Radni okvir za procjenu i unapređenje kulture informacijske sigurnosti

Arbanas, Krunoslav

Sveučilište u Zagrebu

Fakultet organizacije i informatike

Krunoslav Arbanas

RADNI OKVIR ZA PROCJENU I UNAPREĐENJE KULTURE INFORMACIJSKE SIGURNOSTI

DOKTORSKA DISERTACIJA

Varaždin, 2021

Sveučilište u Zagrebu

Fakultet organizacije i informatike

Krunoslav Arbanas

RADNI OKVIR ZA PROCJENU I UNAPREĐENJE KULTURE INFORMACIJSKE SIGURNOSTI

DOKTORSKA DISERTACIJA

Mentori:

Prof. dr. sc. Mario Spremić
Doc. dr. sc. Nikolina Žajdela Hrustek

Varaždin, 2021.

University of Zagreb

Faculty of Organization and Informatics

Krunoslav Arbanas

INFORMATION SECURITY CULTURE EVALUATION AND IMPROVEMENT FRAMEWORK

DOCTORAL THESIS

Supervisors:

Prof. Mario Spremić, Ph. D.
Asst. Prof. Nikolina Žajdela Hrustek, Ph.D.

Varaždin, 2021

PODACI O DOKTORSKOJ DISERTACIJI

I. AUTOR

Ime i prezime	Krunoslav Arbanas
Datum i mjesto rođenja	06. svibnja 1983., Požega
Naziv fakulteta i datum diplomiranja na VII/I stupnju	Fakultet organizacije i informatike, 18. srpnja 2007.
Sadašnje zaposlenje	Hrvatska energetska regulatorna agencija

II. DOKTORSKA DISERTACIJA

Naslov	Radni okvir za procjenu i unapređenje kulture informacijske sigurnosti
Broj stranica, slika, tablica, grafikona, priloga, bibliografskih podataka	234 stranica, 22 slike, 57 tablica, 9 grafikona, 6 priloga, 351 bibliografski podatak
Znanstveno područje i polje iz kojeg je postignut doktorat znanosti	Društvene znanosti, Informacijske i komunikacijske znanosti
Mentori ili voditelji rada	Prof. dr. sc. Mario Spremić Doc. dr. sc. Nikolina Žajdela Hrustek
Fakultet na kojem je obranjen doktorski rad	Fakultet organizacije i informatike
Oznaka i redni broj rada	158

III. OCJENA I OBRANA

Datum sjednice Fakultetskog vijeća na kojoj je prihvaćena tema	26. svibnja 2019.
Datum predaje rada	11. srpnja 2020.
Datum sjednice Fakultetskog vijeća na kojoj je prihvaćena pozitivna ocjena rada	10. prosinca 2020.
Sastav povjerenstva koje je rad ocijenilo	Prof. dr. sc. Valentina Kirinić Doc. dr. sc. Petra Grd Prof. dr. sc. Marin Golub
Datum obrane	07. siječnja 2021.
Sastav Povjerenstva pred kojim je rad obranjen	Prof. dr. sc. Valentina Kirinić Doc. dr. sc. Petra Grd Prof. dr. sc. Marin Golub
Datum promocije	

... mojim roditeljima

... u znak zahvale za podršku i razumijevanje

Zahvale

Na početku ove disertacije mogu samo reći hvala dragom Bogu što je nakon 8 godina, 5 pravilnika o doktorskom studiju, 3 prezentacije na doktorskim radionicama i više stotina pročitanih članaka, konačno došao kraj i ovoj avanturi…

U prvom redu želio bih se zahvaliti na pomoći i savjetima svojim mentorima, prof. dr. sc. Mariju Spremiću i posebno doc. dr. sc. Nikolini Žajdela Hrustek, bez koje ne bi bilo ove disertacije. Puno hvala!

Isto tako, hvala svim profesorima i asistentima s kojima sam tijekom ovih 8 godina ostvario kontakt povodom traženja znanstvenog doprinosa u temama koje sam predlagao.

Također, posebno se želim zahvaliti doc. dr. sc. Katarini Pažur Aničić, Blanki Zubalj i Renati Đurić na nesebičnoj pomoći oko znanstvenog odnosno stručnog dijela provedenog istraživanja.

Hvala svim eksperticama i ekspertima koji su pristali sudjelovati u istraživanju, kao i svim sudionicima istraživanja koji su odvojili svoje dragocjeno vrijeme i (u potpunosti) ispunili anketni upitnik, a posebno veliko hvala ide onima koji su, nakon što su ispunili upitnik, zagnjavili i svoje kolege da ispune i oni.

U konačnici, hvala svima onima koji su na bilo koji način doprinijeli nastanku ove disertacije.

Sažetak

Već duži niz godina istraživanja iz domene informacijske sigurnosti ističu kako su upravo informacije ključni resurs svake organizacije koje je, sukladno tome, potrebno primjereno štititi. Međutim, ono što se promijenilo u odnosu na prije dvadesetak godina je činjenica da zaštita informacija temeljena na samo tehničkim mjerama zaštite više nije dovoljna, a informacijska sigurnost više ne predstavlja tehnički nego upravljački problem. Novija istraživanja pokazuju kako je za primjereno upravljanje informacijskom sigurnošću potrebno, uz davno prepoznate tehničke mjere, uzeti u obzir i ne-tehničke mjere s posebnim naglaskom na ljudski čimbenik. Međutim, iako su ljudi u literaturi prepoznati kao kritične prijetnje u zaštiti informacijske imovine, oni ujedno mogu postati i rješenje problema. Mjerama kao što su, između ostalog, definiranje sigurnosnih politika i procedura ili održavanje radionica podizanja svijesti o informacijskoj sigurnosti uspostavlja se dobra kultura informacijske sigurnosti koja može značajno doprinijeti zaštiti informacijske imovine na način da ljude, kao prepoznati problem informacijske sigurnosti, pretvori u rješenje tog problema. Način za postizanje toga je uspostava primjerene kulture informacijske sigurnosti kao načina zaštite informacija što dovodi do potrebe identifikacije elemenata koji doprinose uspostavi kulture informacijske sigurnosti.

Glavni doprinosi istraživanja opisanog u ovoj disertaciji su sistematizacija znanja iz područja kulture informacijske sigurnosti, identifikacija ključnih čimbenika koji čine kulturu informacijske sigurnosti, razvijen i validiran mjerni instrument za procjenu kulture informacijske sigurnosti temeljen na dosadašnjim istraživanjima i provedenom empirijskom istraživanju te u konačnici, razvijen i validiran okvir za procjenu i unapređenje kulture informacijske sigurnosti koji kulturu informacijske sigurnosti ne promatra u samo jednom aspektu (primjerice ponašanje zaposlenika) već u obzir uzima njenu organizacijsku, sociološku i tehničku komponentu. Validacija mjernog instrumenta i radnog okvira za procjenu i unapređenje kulture informacijske sigurnosti provedena je putem provjere pouzdanosti te sadržajne i konstruktne valjanosti teorijskih koncepata pomoću znanstvenih metoda (evaluacija eksperata, metoda sortiranja karata, faktorska analiza) i pokazatelja (Fleiss Kappa, omjer pogodaka, omjer sadržajne valjanosti, Cronbachov alfa i dr.).

Ključne riječi: *informacijska sigurnost, kultura, sigurnosna kultura, kultura informacijske sigurnosti, radni okvir, čimbenici, faktorska analiza, mjerni instrument, validacija*

Extended abstract

For many years, information security researchers have identified information as the key resource of any organization that needs to be adequately protected. However, what has changed in the past twenty years is the fact that information protection based on purely technical measures is no longer sufficient, since information security is no longer technical but managerial problem. Recent research shows that, with well-known technical measures, for an appropriate information security management it is necessary to take into account non-technical measures also, with a special emphasis on the human factor. However, although literature recognize people as the weakest link in the security chain, they can also become a solution of the problem. A good way to achieve this is to establish an appropriate information security culture as a way of protecting information, which leads to the need of identifying elements that contribute to the establishment of an information security culture in organization.

The research described in this thesis contained several phases based on the use of qualitative and quantitative scientific methods. The first phase referred to the identification of key factors of information security culture in the organizational context, the second phase consisted of activities for conceptual framework development, the third phase was about the development and testing of a measuring instrument, and the final, fourth phase referred to the analysis of empirical research data as well as correlation analysis of information security culture and information security measures implementation in the organization. During the first phase, key factors of information security culture in the organizational context were identified by using scientific methods of review, analysis and synthesis of available relevant research in the field of information security culture. During the second phase, an information security culture evaluation and improvement conceptual framework, in form of defined categories and components of each category based on the results of the first phase of research, was developed.

The most extensive, third phase, consisted of the development and testing of a measuring instrument which was in the form of a survey questionnaire. The creation of the questionnaire particles was based on a literature search in the information security culture field, after which the particles used so far were used to describe and measure the identified factors influencing the information security culture. In other words, particle creation was based on the results obtained in the first phase of the research. In this section, a convenient (available) sample of 12 experts was contacted to participate in the validation of the content and construct validity of extracted particles. In the context of this research, the term “experts” means certified

professionals in the field of information security or information systems auditing. Content validation included the calculation of the Content Validity Ratio (CVR) and the Averaged value of relative importance. The next steps included the measurement scale development and measurement instrument testing. In this part of the research, the Q-sort (card sorting) method was used and it was based on the experts' involvement in particle assessment, where experts were to classify particles into separate categories with respect to similarities and differences among particles. If the experts consistently classified the particles into appropriate constructs, it was considered that the convergent validity of a certain construct was achieved, as well as the discriminant validity in relation to other constructs. For those particles for which experts did not reach consensus, they were excluded from further analysis. Two measurement methods were used to assess the reliability of the sorting procedure: the Fleiss Kappa coefficient, as a measure of agreement between more than two experts, and the Hit Ratio, as an indicator of how many variables were placed in the target group by experts. Scales that have a high percentage of "correct" classifications can be said to have a high degree of construct validity and a high potential for good reliability. All the measuring instrument particles were measured using a five-degree Likert-type semantic ordinal scale. In order to determine the relevance of the measuring instrument, it contained several questions about objective indicators of the implemented information security measures in the organization (for example, occurrences of incidents or awareness campaigns via e-mails alerting employees to various security threats).

For the purpose of measuring instrument validation in terms of internal consistency and conceptual framework validation, it was planned to form a sample of organizations that make operators of essential services in the context of critical national infrastructure in the Republic of Croatia. Then, after the sample would be formed, the survey questionnaire would be sent to employees of these organizations, who are users of the information system. However, due to the impossibility of determining the entire population of the operators of essential services, from which a random sample was to be formed, due to the sensitivity of information about which organizations they are, the author of this study was forced to use the non-probabilistic Snowball method to determine participants in the empirical part of this study. For this reason, as a basis for determining the required minimum sample size or number of subjects, a literature-supported measure of at least three times more subjects than there are particles in the measuring instrument, was taken. The empirical research was conducted on the basis of voluntary and anonymous participation without collecting any personal data.

The final, fourth phase included the analysis of the collected data after the conducted empirical research as well as the analysis of the correlation between information security culture and implemented information security measures in the organization. At the very beginning, a descriptive statistical analysis was used, which goal was to examine summary descriptions of the distributions of quantitative variables and to validate the instrument in terms of reliability of the obtained data. To assess the reliability of the measuring instrument, the Cronbach's α (alpha) coefficient was used, as a measure of internal consistency, which determines the extent to which research results can be repeated over time or through different groups of subjects. In order to further verify the validity and reliability of the measuring instrument, an exploratory factor analysis was performed on the data obtained by empirical research, which reduced the total number of factors to 8 factors distributed within 3 higher-level categories. It is important to emphasize that the information security culture evaluation and improvement framework is based on a validated measuring instrument and shares its structure. This means that the measuring instrument consists of manifest variables (particles) that describe the first-level latent variables (factors) and the second-level latent variables (categories) that are described by these factors. The mentioned factors and categories from the measuring instrument are integral parts of the information security culture evaluation and improvement framework, which in its initial structure consisted of 13 factors divided into 3 higher-level categories (organizational measures, sociological factors and technical measures).

Based on the question of objective indicators of implemented information security measures in the organization, which were the part of the measuring instrument, correlation analysis was used to verify and prove the positive relatively weak correlation between information security culture and implemented information security measures. Thus, in addition to the validation of the measuring instrument as the basis for the framework development, the information security culture evaluation and improvement framework was successfully validated. Finally, after theoretical and empirical validation of the measuring instrument and framework, first through the expert opinion method, and then by factor analysis, the final structure of the measuring instrument and the information security culture evaluation and improvement framework was obtained. It consisted of 3 second-level latent variables (categories), 8 first-level latent variables (factors) and 46 manifest variables (particles) that directly measure first-level latent variables.

One of the main identified research limitations is the inability to create a representative sample of organizations that are the operators of essential services as well as employees or participants in the research due to the inability to determine the size of the entire population. The

organizations that are operators of essential services have been selected for the proposed framework and measurement instrument validation because they are increasingly the targets of various forms of information security incidents and are an important element in terms of national critical infrastructure. Additional recognized limitations are the limited ability to generalize results due to the use of non-probabilistic sampling method, relatively small number of experts who participated in the content and construct validation of the measuring instrument, poor motivation of potential participants and inevitable possible subjectivity during the relevant literature review.

This thesis is divided into 7 chapters, where the **first chapter**, which is the introductory part, briefly elaborates the importance of the research topic from which the 3 research goals to be achieved by this research arose, as well as the formulation of 2 hypotheses that this research seeks to confirm or discard. The **second chapter** provides a general view of information security, its evolution through history and the basic components that make information security. The **third chapter** deals with an extensive topic of information security management in which the emphasis is on information security as corporate governance part as well as management-level, and no longer only the technical-level problem. Also, this chapter emphasizes the need for a holistic approach to information security management. This chapter also addresses the challenges of information security as well as the elements of information security management and provides a brief overview of relevant laws and norms in the field of information security with emphasis on the importance of the so-called critical national infrastructure. The **fourth chapter** provides a detailed overview of information security culture, from the definition of the term, through its importance and relationship with organizational culture to documenting the acquired knowledge about key factors and existing models and frameworks of information security culture from relevant literature. The **fifth chapter** is reserved for the research methodology, which describes step by step the scientific methods and indicators that will be used in meeting the set research goals. The **sixth chapter** extensively presents the results of the research obtained through the methodology described in the previous chapter, while the **seventh**, last chapter, summarizes the research results in the context of research goals and hypotheses, underlining the contributions and limitations of this research.

Keywords: *information security, culture, security culture, information security culture, framework, factors, factor analysis, measuring instrument, validation*

SADRŽAJ

POPIS SLIKA

POPIS TABLICA

POPIS GRAFIKONA

1. UVOD

Informacijska sigurnost već je nekoliko desetljeća u fokusu kako stručne, tako i znanstvene zajednice zbog prepoznate činjenice da su informacije ključni resurs svake organizacije. Samim time, sigurnost i zaštita takvih informacija trebala bi biti imperativ u svim organizacijama, neovisno o sektoru iz kojeg organizacija dolazi. Međutim, nerijetko se događa da se informacijska sigurnost smatra nepotrebnim troškom te samo smeta zaposlenicima u bržem i učinkovitijem obavljanju njihovih svakodnevnih aktivnosti.

Krajem 90-ih godina prošlog stoljeća napadi na informacijske sustave evoluirali su od upotrebe trojanskih konja i virusa na sofisticirane napade poput distribuiranih napada na dostupnost, ugradnju malicioznog koda u poruke elektroničke pošte ili različitih oblika malicioznog softvera namijenjenom iznudi i ucjeni. Ulaskom u 21. stoljeće napadi nisu više samo rezultat napadačevih želja pokazivanja svog znanja, već imaju za cilj ostvarivanje financijske koristi. Ujedno se promijenila i paradigma napada te se može reći da se više ne napada stroj odnosno sustav nego korisnik odnosno čovjek [1]. Rezultat toga je određeni pomak u sigurnosnim protumjerama, od čisto tehničkih mjera zaštite što se pokazalo nedovoljnim [2] do proaktivnog strateškog pristupa koji uključuje i druge elemente informacijske sigurnosti, posebno one s organizacijskog ili sociološkog aspekta budući da ni najbolja sigurnosna tehnologija ne može zaustaviti napad socijalnim inženjeringom [1]. Jedan od prvih, a ujedno i najvećih izazova s kojim se susreću rukovoditelji informacijske sigurnosti, je uspješno balansiranje između potrebe zaštite informacijske imovine s jedne strane i omogućavanja operativnog poslovanja s druge, budući da prevelika zaštita putem striktnih kontrola može dovesti do sprječavanja poslovne učinkovitosti dok labave kontrole mogu stvoriti neprihvatljive rizike za informacijsku imovinu [3]. Suvremeni pogled na informacijsku sigurnost nalaže kako učinkovita strategija informacijske sigurnosti mora biti uravnotežena, odnosno da, prilikom dizajniranja i implementiranja sigurnosnih rješenja, treba naglasiti važnost tehnologije, ali i sociološko-organizacijski kontekst unutar organizacije [3], a informacijsku sigurnost promatrati kao poslovno odnosno upravljačko pitanje, a ne samo tehničko [3], [2]. Također, iako je ljudski faktor u literaturi prepoznat kao kritična prijetnja informacijskoj sigurnosti odnosno ključni čimbenik (ne)uspjeha upravljanja informacijskom sigurnošću u organizacijama [4], on istovremeno može postati i rješenje problema, a dobar način za postizanje toga je uspostava primjerene kulture informacijske sigurnosti.

U konačnici, ako činjenicu da kultura informacijske sigurnosti može ili pridonijeti zaštiti informacija ili stvoriti rizik, stavimo u kontekst današnjeg izrazito dinamičnog poslovnog okruženja u kojem se gotovo svakodnevno otkrivaju nove prijetnje sigurnosti informacija, postaje još izraženija potreba za razvojem kvalitetnog okvira za procjenu i unapređenje kulture informacijske sigurnosti što čini opravdan razlog i motivaciju za ovo istraživanje čiji je glavni cilj upravo razvoj i validacija takvog okvira.

Doktorska disertacija podijeljena je u 7 poglavlja gdje se u **prvom poglavlju**, koje čini uvodni dio, sumira izgled disertacije po poglavljima te ukratko elaborira važnost teme istraživanja iz koje su proizašla 3 cilja istraživanja koja se žele postići ovim istraživanjem kao i formulacija 2 hipoteze koje se ovim istraživanjem žele potvrditi ili odbaciti.

Drugo poglavlje donosi općeniti pogled na informacijsku sigurnost, njen razvoj kroz povijest i osnovne sastavnice koje čine informacijsku sigurnost.

Treće poglavlje obrađuje opširnu temu upravljanja informacijskom sigurnošću u kojem je dan naglasak na informacijsku sigurnost kao dio korporativnog upravljanja odnosno problema upravljačke, a ne više samo tehničke razine, kao i potrebe holističkog pristupa upravljanja informacijskom sigurnošću. Ovo poglavlje dotiče se također izazova informacijske sigurnosti kao i elemenata upravljanja informacijskom sigurnošću te pruža kratki osvrt na relevantne zakone i norme iz domene informacijske sigurnosti s naglaskom na važnost tzv. kritične nacionalne infrastrukture.

U **četvrtom poglavlju** detaljno se daje pregled kulture informacijske sigurnosti, od same definicije tog pojma, preko njene važnosti i odnosa s organizacijskom kulturom do dokumentiranja stečenih spoznaja o ključnim čimbenicima i postojećim modelima i radnim okvirima kulture informacijske sigurnosti iz relevantne literature.

Peto poglavlje rezervirano je za metodologiju istraživanja u kojem su po koracima opisane znanstvene metode i pokazatelji koji će se koristiti prilikom ispunjavanja postavljenih ciljeva istraživanja.

U **šestom poglavlju** opširno su navedeni rezultati provedenog istraživanja dobiveni putem metodologije opisane u prethodnom poglavlju, dok **sedmo**, ujedno i posljednje poglavlje, sumira rezultate istraživanja u kontekstu postavljenih ciljeva i hipoteza istraživanja, uz navođenje doprinosa i ograničenja ovog istraživanja.

1.1. Definiranje problema istraživanja

Istraživači već neko vrijeme naglašavaju kako se u borbi za postizanje sigurnosti više ne može oslanjati samo na tehnološke kontrole i mjere zaštite [4] već je potrebno uzeti u obzir i netehničke mjere s posebnim naglaskom na ljudski faktor [5], [6], [7], [8]. Budući da je cilj zaštite informacija često u određenoj mjeri u svojevrsnom sukobu s uobičajenim poslovnim ciljevima maksimiziranja produktivnosti i smanjenja troškova, potrebno je izgraditi stav u organizaciji da informacijska sigurnost postane prirodni dio dnevne rutine svih zaposlenika [8] pazeći pritom da uspostavljene sigurnosne kontrole nisu pretjerane već razmjerne mogućim rizicima [9].

Sukladno tome, zaključak je kako je za primjerenu razinu informacijske sigurnosti u organizacijama potreban holistički, višedimenzionalni pristup [9], [4]. Tako Panguluri i suradnici [10] takav pristup uspoređuju s tronošcem gdje su tehničke mjere poput enkripcije, vatrozida, antivirusnog softvera i sl. bitan element zaštite informacijske imovine, ali su ipak samo jedna 'noga' spomenutog tronošca te nisu dovoljne bez druge dvije 'noge' koje čine ljudi i procesi. Yildrim [4] kao tri komponente takvog holističkog pristupa vidi tehnologiju, ljude i edukaciju, a AlHogail i Mirza [11] ljude, organizaciju i tehnologiju.

Pojam kulture informacijske sigurnosti pojavio se krajem 1990-ih godina u svrhu promicanja sigurnog ponašanja zaposlenika u organizacijama budući da se ljudi često u literaturi nazivaju „najslabijom karikom u sigurnosnom lancu" [12], [13] jer, namjerno ili iz nemara, predstavljaju najveću prijetnju informacijskoj sigurnosti organizacije [13], [14]. Postoji mnoštvo definicija kulture informacijske sigurnosti od kojih je jedna od najjednostavnijih da je to „način na koji se stvari obavljaju u organizaciji radi zaštite informacijske imovine" [15]. Da Veiga [16] s druge strane proširuje tu definiciju te tvrdi kako kultura informacijske sigurnosti predstavlja "stavove, pretpostavke, uvjerenja, vrijednosti i znanje koje zaposlenici/dionici koriste u interakciji s organizacijskim sustavima i postupcima u bilo kojem trenutku gdje interakcija rezultira prihvatljivim ili neprihvatljivim ponašanjem koje se očituje u artefaktima i kreacijama koje postaju dijelom načina na koji se stvari obavljaju u organizaciji kako bi se zaštitila informacijska imovina.".

Kao što je vidljivo iz navedenih definicija, velik naglasak je stavljen na zaposlenike, što je razumljivo zbog činjenice da se jednim od glavnih uzroka incidenata informacijske sigurnosti smatraju sadašnji i bivši zaposlenici [17], a ne manjkava tehnologija [18]. Tome u prilog govori i istraživanje koje je proveo EY [19] koje je pokazalo da je postotak ispitanika koji su prepoznali

nemarne ili neosviještene zaposlenike kao izvor sigurnosnih ranjivosti, 2017.g. porastao na 60% u odnosu na dvije godine ranije kad je taj postotak bio 44%. Također, 64% ispitanika prepoznalo je zlonamjerni softver (engl. *Malware*) i lažno predstavljanje radi stjecanja osjetljivih informacija (engl. *Phishing*) kao izvore sigurnosnih prijetnji organizacijama, u odnosu na 44% za zlonamjerni softver odnosno 43% za lažno predstavljanje, dvije godine ranije.

Kao što vidimo, istraživanja vezana uz informacijsku sigurnost dosljedno ukazuju na to da zaposlenici predstavljaju najveću prijetnju informacijskoj sigurnosti te su time zapravo kritični faktor u procesu upravljanja informacijskom sigurnošću. Međutim, iako zaposlenici na taj način predstavljaju dio problema informacijske sigurnosti, oni su ujedno i dio rješenja [13] budući da se putem edukacije, osposobljavanja i podizanja svijesti o informacijskoj sigurnosti povećava razina sigurnosti u organizaciji. Drugim riječima, uspostavom kulture informacijske sigurnosti u kojoj je sigurnost odgovornost svih zaposlenika smanjuje se vjerojatnost pojave incidentnih situacija, no valjana kultura informacijske sigurnosti ne može se uspostaviti bez formalno dokumentiranih politika i procedura [10]. S druge strane, dosljedna podrška rukovodstva bitna je za stvaranje podržavajuće okoline u organizaciji [5] kako bi se dobila uključenost svih zaposlenika u zahtjevima informacijske sigurnosti njegujući na taj način kulturu informacijske sigurnosti [10] obzirom da kultura informacijske sigurnosti u organizaciji može ili pridonijeti zaštiti informacija ili stvoriti rizik [16].

1.2. Ciljevi i hipoteze istraživanja

Na temelju identificiranog istraživačkog problema, postavljeni su sljedeći ciljevi koji se žele postići te hipoteze koje se žele testirati ovim istraživanjem.

Ciljevi istraživanja su sljedeći:

(1) Identificirati čimbenike koji čine kulturu informacijske sigurnosti,
(2) Razviti mjerni instrument za procjenu kulture informacijske sigurnosti koji sadrži ključne čimbenike koji su vezani uz kulturu informacijske sigurnosti unutar organizacije te provesti validaciju mjernog instrumenta putem empirijskog istraživanja,
(3) Razviti i validirati okvir za procjenu i unapređenje kulture informacijske sigurnosti.

Hipoteze istraživanja su sljedeće:

H1: Organizacijske mjere i sociološki čimbenici zajedno s tehničkim mjerama ključne su kategorije u procjeni i unapređenju kulture informacijske sigurnosti u organizaciji.

H2: Razina kulture informacijske sigurnosti pozitivno je povezana s primjenom implementiranih mjera informacijske sigurnosti u organizaciji na način da veća razina kulture informacijske sigurnosti predstavlja veću primjenu implementiranih mjera informacijske sigurnosti.

2. INFORMACIJSKA SIGURNOST

U današnje vrijeme kada informacije predstavljaju najvrjedniju imovinu koju organizacija ima, a posjedovanje određene, relevantne i točne informacije može napraviti ogromnu razliku u učinkovitosti organizacije [20], pitanje sigurnosti informacija nešto je s čime se u nekom obliku suočavaju sve organizacije u svim sektorima [21].

Kako su računala postala sve više i više sveprisutna, tako su organizacije postale ovisne o informacijskim sustavima za svoje svakodnevne operacije i strateške svrhe čime pojačavaju potrebu za informacijskom sigurnošću [22] čija je funkcija važnija nego ikad za očuvanje korporativne vrijednosti zbog činjenice da, dok su se u prošlosti obrađivale informacije o poslovanju, danas informacije *jesu* posao [23].

Opseg informacijske sigurnosti mijenja se kako se tehnologija mijenja. Kako se računarstvo razvilo od mainframe računala, preko osobnih računala i mobilnih uređaja, do oblaka i Interneta stvari (engl. *Internet of Things - IoT*), svima je na neki način postala potrebna informacijska sigurnost te ju je potrebno osigurati na način da ona postaje prirodna faza u svakodnevnim aktivnostima organizacije [20].

Uz kontinuirani razvoj informacijske tehnologije i sveobuhvatne popularizacije Interneta, informacijska sigurnost proširena je na politiku, gospodarstvo, društvo i ostala polja [24].

2.1. Pojam informacijske sigurnosti

Sami počeci informacijske sigurnosti odnosno točnije, njezine preteče, računalne sigurnosti sežu u 60-e godine prošlog stoljeća gdje su najranija spominjanja ovog pojma uglavnom iz vladine i vojne perspektive, pri čemu se računalna sigurnost prije svega odnosila na mjere koje su poduzimali administratori i programeri za zaštitu tih vojnih sustava [25].

Pojam *informacijska sigurnost* u sebi već sadrži objašnjenje na čemu je naglasak i što je to što se treba zaštiti, međutim, ono što je potrebno razjasniti prije same formalne definicije tog pojma je što je to zapravo *informacija* i kako se ona razlikuje od *podatka*, ako se uopće razlikuje, zbog čega se u nastavku nalazi kratko objašnjenje ovih pojmova.

2.1.1. Podatak

Hrvatska enciklopedija, mrežno izdanje [26] definira podatak kao „*poznatu ili pretpostavljenu činjenicu na osnovi koje se oblikuje informacija*".

Ackoff [27] navodi kako su podaci „*simboli koji predstavljaju svojstva objekata i događaja*" dok ih Vacca [23] definira kao „*prikaz činjenica, pojmova ili uputa pogodnih za komunikaciju, tumačenje ili obradu"*.

Podaci uključuju sirove brojeve i riječi [28] odnosno mogu biti bilo koja neobrađena činjenica koja se koristi za donošenje odluka [29]. Na primjer, niz znakova „2012" može predstavljati godinu, datum rođenja, PIN za mobitel ili bankovnu karticu, numerički dio registarske oznake automobila ili nešto drugo, te bez konteksta predstavlja samo sirovu činjenicu.

Na temelju predstavljenih definicija možemo zaključiti kako ti nizovi alfanumeričkih znakova koji predstavljaju podatak, sami po sebi nemaju neko značenje ukoliko ih se ne stavi u kontekst, što drugim riječima znači kako je podatak preduvjet za stvaranje informacije.

2.1.2. Informacija

Hrvatska enciklopedija, mrežno izdanje [26] definira informaciju kao „*skup podataka s pripisanim značenjem, osnovni element komunikacije koji, primljen u određenoj situaciji, povećava čovjekovo znanje*".

Whitman i Mattord [28] navode kako informaciju čine „*podaci koji su organizirani, strukturirani i predstavljeni kako bi se pružio dodatni uvid u njihov kontekst, vrijednost i korisnost*", a Ackoff kako se informacije sastoje od „*obrađenih podataka gdje je obrada usmjerena na povećanje njegove korisnosti*" [27].

Slijedom navedenog, može se reći kako su informacije podaci koji imaju značenje u određenom kontekstu i koriste se za prijenos koncepta koji ima vrijednost za osobu u određenim okolnostima [30], odnosno to su „*podaci koji su obrađeni u oblik koji ima značaj za primatelja i koji ima stvarnu ili uočenu vrijednost u trenutnim ili budućim radnjama ili odlukama"* [29].

Drugim riječima, obrađeni podaci postaju informacije [31], na način da informacije unose jasnoću u podatke, tako da se na temelju njih može djelovati [29].

2.1.3. Informacijska sigurnost

Međunarodna organizacija za standardizaciju (engl. *International Organization for Standardization - ISO*) definira informacijsku sigurnost kao „*očuvanje povjerljivosti, integriteta i dostupnosti informacija*" [32], a američki Nacionalni Institut za standarde i tehnologiju (engl. *National Institute of Standards and Technology – NIST*) kao „*zaštitu*

informacija i informacijskih sustava od neovlaštenog pristupa, upotrebe, otkrivanja, ometanja, izmjene ili uništavanja radi pružanja povjerljivosti, integriteta i dostupnosti" [33].

Dakle, informacijska sigurnost uključuje zaštitu organizacijske imovine od poremećaja poslovanja, modificiranja osjetljivih podataka ili otkrivanja vlasničkih podataka gdje se ta zaštita spomenutih podataka obično opisuje kao „*održavanje povjerljivosti, integriteta i dostupnosti imovine, operacija i informacija organizacije*" [23] i to „*bilo u pohrani, obradi ili prijenosu, primjenom politike, edukacije, obuke i podizanja svijesti te tehnologije*" [28]. Upravo ta organizacijska imovina, koja se u informacijskoj sigurnosti naziva i informacijskom imovinom, predstavlja fokus informacijske sigurnosti i predstavlja informacije i izvore informacija koje imaju vrijednost za organizaciju kao i sustave koji pohranjuju, obrađuju i prenose informacije [28].

Kao što vidimo, postoje brojne definicije informacijske sigurnosti, međutim, ono što je zajedničko svima njima je naglasak na očuvanju osnovne tri kategorije informacija kad je u pitanju sigurnost, a to su povjerljivost, integritet i dostupnost, te iako se često naglašava povjerljivost informacija, dok su integritet i dostupnost informacija potisnuti, sva tri svojstva moraju biti u ravnoteži [34] budući da isticanje samo jednog na štetu drugih može dovesti do smanjene učinkovitosti i produktivnosti bilo koje organizacije [35].

2.1.3.1. Povjerljivost

Povjerljivost (engl. *Confidentiality*) je jedno od tri osnovna svojstva sigurnosti informacije i pojam je koji prvo pada na pamet kad se spomene sigurnost.

Međunarodna organizacija za standardizaciju (ISO) [32] definira povjerljivost kao "*svojstvo da informacija nije dostupna ili otkrivena neovlaštenim pojedincima, entitetima ili procesima*" što znači da, ako se želi sačuvati povjerljivost informacija, potrebno ih je čuvati u tajnosti na način da ne smiju biti dostupne svima onima tko im želi pristupiti [36].

Informacije imaju povjerljivost kada su zaštićene od otkrivanja ili izlaganja neovlaštenim pojedincima ili sustavima [28] osiguravajući da se te informacije dijele samo među ovlaštenim korisnicima. [37]. Čim neovlašteni pojedinci ili sustavi imaju uvid u osjetljive informacije, povjerljivost je narušena. Uobičajeni izrazi za gubitak povjerljivosti uključuju proboj podataka, krađu podataka, izlaganje, curenje i piratstvo [38]. Ostali primjeri kršenja povjerljivosti uključuju zaposlenika koji uklanja dokument iz arhive koji sadrži osjetljive informacije bez

upotrebe uređaja za uništavanje papira (engl. *Shredder*) ili hakera koji se uspješno probija u internu bazu organizacije i krade osjetljive podatke o njenim klijentima, kao što su imena, adrese i brojevi kreditnih kartica [28].

2.1.3.2. Integritet

Integritet (engl. *Integrity*) informacije predstavlja „*svojstvo zaštite točnosti i cjelovitosti*" [32] i važan je zbog činjenice da informacije igraju glavnu ulogu u procesu donošenja odluka, a ako informacije nisu točne ili potpune, pogrešne odluke mogu dovesti do neželjenih situacija koje bi se u protivnom mogle spriječiti [36].

Informacije su korisne i pouzdane samo ako su točne i valjane [39] odnosno nisu izmijenjene mimo namjera stvaratelja informacije [35] te se za takve informacije onda može reći kako imaju integritet [39].

Održavanje integriteta osigurava da neovlaštene osobe ili procesi ne mijenjaju informacije, ovlaštene osobe ili procesi ne vrše neovlaštene izmjene podataka, a informacije su interno i eksterno konzistentne [25]. Uobičajeni izrazi za gubitak integriteta uključuju korupciju podataka, uništavanje, modificiranje, subverziju i neovlašteno mijenjanje [38].

Do oštećenja cjelovitosti može doći prilikom pohrane ili prijenosa informacija. Mnogi su računalni virusi i crvi dizajnirani s izričitom svrhom oštećivanja informacija. Iz tog razloga, ključna metoda za otkrivanje virusa ili crva je traženje promjena u integritetu datoteke, primjerice veličini datoteke. Druga ključna metoda osiguravanja integriteta informacija je izračunavanje vrijednosti sažetka (engl. *Hash*) datoteka koja je za bilo koju kombinaciju bitova jedinstvena. Oštećenje datoteka nije nužno rezultat vanjskih snaga, poput hakera, već oštećenje može biti uzrokovano i šumom u mediju za prijenos zbog činjenice da odašiljanje podataka sklopovljem s niskim naponom može promijeniti i oštetiti podatke [28].

Cjelovitost informacija je stup informacijske sigurnosti i zbog toga je potrebna za postojanje zdravog procesa upravljanja sigurnošću. Međutim, priznato je da 100% integriteta informacija trenutno nije moguće postići zbog različitih ograničenja i stoga je prihvaćen revizijski koncept *razumne sigurnosti*. To je u skladu s konceptom da se stopostotna informacijska sigurnost ne može dostići i predodžbom da je cilj *odgovarajuća sigurnost* primjenom odgovarajućih protumjera [31].

2.1.3.3. Dostupnost

Dostupnost (engl. *Availability*) je treće ključno svojstvo informacije koje podrazumijeva omogućavanje korisnicima da dobiju pravovremene informacije, odnosno to je „*svojstvo raspoloživosti i upotrebljivosti na zahtjev ovlaštenog entiteta*" [32].

Da bi organizacija sačuvala dostupnost svoje informacijske imovine, mora osigurati da su takvi resursi dostupni za upotrebu ovlaštenim osobama u pravo vrijeme. Osiguravanje dostupnosti informacija je izuzetno važno, jer bez pravovremenih informacija organizacija ne bi bila u stanju nastaviti normalno funkcioniranje [36].

Uobičajeni uvjeti za gubitak raspoloživosti uključuju gubitak kontinuiteta poslovanja, uništavanje ili gubitak podataka, prekid rada i uskraćivanje usluge [38], gdje je napad uskraćivanjem usluge (engl. *Denial of Service – DoS*) jedan od najčešćih načina na koji je ugrožena dostupnost informacija.

2.1.3.4. Ostala svojstva sigurne informacije

Osim povjerljivosti, integriteta i dostupnosti, ponekad se u samu definiciju informacijske sigurnosti dodaju i druga svojstva, kao što su autentičnost, krajnja odgovornost, neporecivost ili pouzdanost.

Autentičnost (engl. *Authenticity*) je „*osobina da je entitet ono što tvrdi da jest*" [32] odnosno može se smatrati varijantom integriteta u kojoj resursi i usluge moraju dokazati svoje podrijetlo, a korisnici moraju dokazati kontrolu određenog identiteta [23] i odnosi se na legitimitet podataka [37].

Krajnja odgovornost (engl. *Accountability*) je također varijanta integriteta, u kojoj je cilj jamčiti da se radnje u sustavu uvijek bilježe bez gubitaka i povezane su s provjerenim identitetom korisnika [28], [23] odnosno mogu se pratiti do odgovorne osobe [37].

Neporecivost (engl. *Non-repudiation*) je „*sposobnost dokazivanja pojave određenog događaja ili radnje i njihovog podrijetla*" [32] na način da korisnici ne mogu poreći da su odgovorni za radnje koje su izvršili na sustavu [23]. Zajedno s integritetom čini temelj sustava koji ne samo da jamči da je ono što je primljeno i poslano, nego može i dokazati da ga je pošiljatelj stvarno poslao što znači da se kasnije ne može tvrditi da je nešto krivotvoreno ili izmišljeno [25].

U konačnici, pouzdanost (engl. *Reliability*), kao posljednje dodatno svojstvo, predstavlja „*svojstvo konzistentnih namjeravanih ponašanja i rezultata*" [32].

2.2. Razvoj informacijske sigurnosti kroz povijest

Jedan od prvih dokumentiranih sigurnosnih problema dogodio se početkom 1960-ih, kada je administrator sustava radio na datoteci MOTD (engl. *Message of the day* - poruka dana), dok je drugi administrator uređivao datoteku s lozinkom. Softverski propust pomiješao je dvije datoteke, a na svaku izlaznu datoteku ispisala se cijela datoteka lozinke [40].

Povijesno gledano, postoji mnogo načina opisivanja razvoja informacijske sigurnosti tijekom posljednjih desetljeća, a jedan od načina mapiranja ovog razvoja je analiza razvoja po fazama koje označavaju specifične trendove [41].

Tako Krakar i suradnici [42] prepoznaju pet faza dosadašnjeg razvoja koncepata informacijske sigurnosti. U prvoj fazi fokus je na IT sigurnosti, odnosno tehničkim aspektima sigurnosti, u drugoj fazi fokus je na sigurnosti podataka u kojoj IT sigurnost postaje dio upravljanja funkcijom IT-a dok se u trećoj fazi pojavljuje fokus na sigurnosti informacija uslijed širenja područja i standardizacije dijelova IT sigurnosti. Četvrtu fazu karakteriziraju sustavi informacijske sigurnosti gdje se fokus sigurnosti širi na cjelokupnu informacijsku imovinu dok petu, završnu fazu, čini korporativna informacijska sigurnost čije su značajke primjena koncepata korporativnog upravljanja sigurnošću informacija s najvišim rukovodstvom kao nositeljem tih aktivnosti [42].

S druge strane von Solms [43] također prepoznaje pet faza razvoja informacijske sigurnosti, odnosno valova, kako ih on naziva, ali su ponešto drugačije raspoređeni nego one kako ih navode Krakar i suradnici. Tako von Solms razlikuje tehnički val, upravljački val, institucijski val, val korporativnog upravljanja informacijskom sigurnošću i val kibernetičke sigurnosti. Dodatno, von Solms napominje kako se mora shvatiti da tih pet valova nisu 'blokovi' koji su započeli i završili u određenom trenutku već predstavljaju nova kretanja koja su započela u određenom razdoblju i stavljala novi naglasak na aspekte povezane sa sigurnošću informacija tijekom zadnjih 30 do 40 godina i stoga ih treba smatrati paralelno postojanima jednih s drugima [43].

Svaki od tih pet valova opisan je u nastavku.

2.2.1. Prvi val – tehnički val

Prvi val razvoja informacijske sigurnosti, do otprilike početka 1980-ih godina, može se smatrati 'Tehničkim valom', koji se uglavnom karakterizira vrlo tehničkim pristupom sigurnosti informacija odnosno mehanizmima kao što su kontrolne pristupne liste, korisničke identifikacijske oznake i lozinke [44], gdje je informacijsku sigurnost, budući da se radi o tehničkom pitanju, najbolje prepustiti tehničkim stručnjacima [45]. Točnije, u ovom razdoblju zapravo se radilo o *računalnoj sigurnosti* gdje je taj termin određivao potrebu da se fizička lokacija računalne tehnologije osigura od vanjskih prijetnji koje su se prvenstveno odnosile na fizičku krađu opreme, špijunažu protiv proizvoda i sabotažu [28].

1940-e do 1950-ih godina obilježile su svitanje računarstva, kada su nastala računala prve generacije, nakon čega je uslijedila era mainframe računala kada je samo nekolicini operatera bilo dopušteno koristiti ta računala. Ključno pitanje sigurnosti tijekom ove ere bilo je osiguravanje da samo ovlašteni računalni operater (jedan korisnik - jedno računalo) ima pristup i da fizičko računalo ne ukradu ili oštete vanjski napadači. Fizička sigurnost bila je osnovno načelo na kojem se temeljila sva sigurnost računalnih sustava. Mainframe računala bila su izolirane samostalne jedinice, a računalne mreže tada još nisu postojale. Za prijenos programa i podataka između računala koristili su se teklići ili fizička pošta, a jedina prijetnja koja se odnosila na prijenos informacija bila je ta što se mediji za pohranu mogu izgubiti ili ukrasti [1].

Kasne 1960-e do početka 1970-ih godina označava početak glupih terminala. Ovime je omogućeno korisnicima (više korisnika - jedno računalo) pristup i korištenje udaljenih podataka. Ova je inovacija uvela novi rizik za udaljene podatke jer je sad postojala mogućnost pristupa podacima od strane neovlaštene osobe ili osobe izvan organizacije. Budući da se jednostavna fizička sigurnost nije mogla nositi s tim novim rizikom, početkom 1970-ih identifikacija i provjera autentičnosti (autentikacija) postali su aktivni koncepti. Osoba zadužena za sigurnost pregledala bi fizički pristup terminalima prije nego što je korisnik mogao započeti postupak identifikacije i provjere autentičnosti. Budući da je bilo malo terminala bilo je lako pratiti sve prijavljene korisnike i njihove aktivnosti. Međutim, budući da nisu postojale sigurnosne politike koje bi nametnule upotrebu jakih lozinki, probijanje lozinki u to je vrijeme predstavljalo veliku prijetnju dok je dodatni problem bilo dijeljenje lozinke [1].

U tadašnje doba, koncept zapošljavanja predanog IT službenika za sigurnost gotovo se nije čuo već su, umjesto toga, najvještiji arhitekti sustava, administratori i programeri bili mobilizirani u krizi i morali se nositi s onim što im je stavljeno pred njih kao izazov. Do kraja 1990-ih, još

uvijek nisu postojale dobro definirane uloge u ne-tehničkim poslovima nego je umjesto toga funkcija informacijske sigurnosti bila učvršćena za druge uloge, poput voditelja IT odjela, administratora sustava, mrežnog administratora pa čak i voditelja kvalitete [25].

Doba glupih terminala naslijedilo je razdoblje mini računala. Uvođenje mini računala označilo je početak računalnih mreža i sustava za više korisnika koji su promijenili pravila igre. S padom cijena modema i terminala povećao se i broj ljudi s računalnim znanjem. Uvedene su kontrole pristupa kako bi se spriječilo međusobno ometanje radnog prostora između korisnika. Iznad povjerljivosti pojavila se briga za integritet podataka [1].

2.2.2. Drugi val – upravljački val

Drugi val, od početka ranih osamdesetih do sredine devedesetih godina prošlog stoljeća, može se promatrati kao 'Upravljački val', karakteriziran rastućom spoznajom i uključivanjem rukovodstva u važnost sigurnosti, nadopunjavajući Tehnički val [44], budući da se dogodila spoznaja kako sigurnost ima snažnu dimenziju upravljanja i da su aspekti poput politika i procedura ili uključenost rukovodstva vrlo važni [45]. Ovaj pomak od tehnologije prema cjelovitijem gledištu poslovanja preusmjerila je računalnu sigurnost na *informacijsku sigurnost* [25].

1980-te su obilježile uvođenje osobnih računala i odjednom je svaki korisnik imao svoje računalo, čime se povećao broj ljudi s računalnim znanjem [1], a činjenica da se informacije ne pohranjuju na jednom središnjem dobro zaštićenom računalu, već se distribuiraju na mnoštvo stolnih računala povezanih računalnim mrežama, stvorila je ozbiljne sigurnosne rizike koje je trebalo riješiti. Opseg informacijske sigurnosti dodatno se proširio, sigurnost informacija postala je stvar koja je privukla pažnju uprave te su imenovani i voditelji informacijske sigurnosti kao dedicirane osobe za informacijsku sigurnost koji su započeli s kreiranjem politika i procedura informacijske sigurnosti [43].

U ovom desetljeću pojavili su se operacijski sustav Microsoft Windows i lokalne mreže (LAN), a ovo je desetljeće obilježio i porast računalnih virusa koji su se širili uporabom disketa. Krajem osamdesetih također se uvodi antivirusni softver [1].

2.2.3. Treći val – institucijski val

Krajem devedesetih godina 20.-og stoljeća započeo je treći val, koji se naziva 'institucijski val', a koji je trajao do oko 2005.g. te ga karakteriziraju aspekti poput dobrih praksi za upravljanje

sigurnošću informacija, međunarodnih certifikata za informacijsku sigurnost, njegovanja informacijske sigurnosti kao korporativne kulture te dinamičkog i kontinuiranog mjerenja informacijske sigurnosti [44].

U 1990-ima su dominirali otvoreni sustavi i mobilno računarstvo te je sve više i više osobnih računala bilo spojeno na Internet. Ova inovacija donijela je nove rizike, što bi se i očekivalo jer su otvoreni sustavi također bili otvoreni i za zlouporabu te je hakerska zajednica stvorila slobodno dostupne alate za hakiranje, a samim tim su se napadi računalnih virusa i crva pojačali. Krajem devedesetih napadači su promijenili stil rada iz uporabe crva i virusa do sofisticiranijih napada. Uvođenje distribuiranog uskraćivanja usluge i zlonamjernog koda priloženog poslovnoj e-pošti i web stranicama pomaknulo je fokus na pristupnike (engl. *Gateway*) što je dovelo do uvođenja filtrirajućih vatrozida (engl. *Firewall*). Sigurnost perimetra pojavila se tako da osigurava zid oko mreže i sprečava vanjske napadače. No kako se upotreba Interneta intenzivirala, mrežne granice nestale su i nestala je sigurnost perimetra [1].

Jedan od pokretača u ovom trenutku bila je ideja dobre međunarodne prakse za sigurnost informacija i dolazak međunarodnih standarda (BS 7799). Drugi pokretač bio je sve veći naglasak na informiranosti o sigurnosti informacija i riziku da neuki zaposlenici mogu ugrozit mjere informacijske sigurnosti. Razvijeni su opsežni tečajevi za podizanje svijesti, a zaposlenici su obučavani da informacijska sigurnost postane dio njihove kulture i kulture tvrtke. Tijekom ove faze, tvrtke su također započele izrađivati tehnike za mjerenje statusa i razine usklađenosti s informacijskom sigurnošću te izvještavanje o tom stanju najvišem rukovodstvu [43].

2.2.4. Četvrti val – val korporativnog upravljanja

Četvrti val započeo je oko 2005. godine i naziva se 'Val korporativnog upravljanja informacijskom sigurnošću' gdje su pokretači ovog četvrtog vala usko povezani s razvojem u područjima korporativnog upravljanja i povezanim pravnim i regulatornim područjima budući da je postalo jasno kako je korporativno upravljanje informacijskom sigurnošću više od samog upravljanja sigurnošću informacija [45]. U ovom periodu pojavilo se nekoliko dobrih međunarodnih praksi za dobro korporativno upravljanje, a uloga upravljanja rizicima informacijske tehnologije i korporativnog upravljanja informacijskom tehnologijom bila je istaknuta u mnogima od njih. Očekivano, dobro korporativno upravljanje informacijskom tehnologijom uključivalo je i dobre implementacije informacijske sigurnosti [43]. Financijske informacije tvrtke pohranjivane su i obrađivane na računalima, a ako pohranjivanje i obrada takvih podataka nije pravilno osigurana i zaštićena, može doći do ozbiljnih kompromitacija.

Postao je vrlo jasan rizik počinjenja prijevare i zlouporabe financijskih sredstava manipuliranjem elektroničkim podacima tvrtke pohranjene u njezinim informacijskim sustavima na neovlašteni način, kao i to da je rukovodstvo u konačnici odgovorno za to, zbog čega i dolazi do koncepta korporativnog upravljanja informacijskom sigurnošću. Činjenica da je „korporativno upravljanje informacijskom sigurnošću sastavni dio korporativnog upravljanja" postala je dobro prihvaćena [43].

Za ova četiri dosadašnja vala bitno je spomenuti dva aspekta. Prvo, ova četiri vala u osnovi imaju veze s osiguravanjem podataka i informacija tvrtke za što je odgovornost za to na tvrtki i njezinim zaposlenicima. Glavna svrha je osigurati čuvanje povjerljivosti i cjelovitosti informacija tvrtke u svakom trenutku - s unutarnje strane tvrtke. Zbog toga su tvrtke uvele vrlo dobre sigurnosne mjere, što je značajno otežalo napadačima koji su željeli pristup takvim podacima i informacijama. Drugo, tvrtke su uvodile sve više i više sustava temeljenih na Internetu i webu, što omogućava milijunima klijenata i kupaca da koriste takve sustave i uđu u tzv. kibernetičko doba [43].

Izravni rezultat ova dva aspekta bio je da su kriminalci svoju pozornost sada prenijeli na krajnjeg korisnika. Koristeći Internet kao pristupni medij, s milijunima krajnjih korisnika s niskom razinom osviještenosti i znanja o informacijskoj sigurnosti, kriminalna strana započela je s korištenjem širokog raspona mehanizama napada usmjerenih prema krajnjem korisniku koji se uglavnom temelje na socijalnom inženjeringu [45]. Njihov moto postao je: „ne pokušavajte provaliti u IT sustave tvrtke; moglo bi biti vrlo teško - idite na naivnog krajnjeg korisnika" [43].

2.2.5. Peti val – val kibernetičke sigurnosti

Peti val, koji se naziva 'Val kibernetičke sigurnosti' započeo je oko 2006. godine, a čiji je cilj osiguranje informacijske sigurnosti u kibernetičkom prostoru [43].

Primijeniti bilo koji sustav baziran na Internetu znači predstaviti se ostatku svijeta, pružajući tako mogućnost kibernetičkim kriminalcima da napadnu sustav [43]. Napadači su počeli hakirati zbog financijske dobiti, a ne samo kako bi pokazali svoje sposobnosti. IT infrastruktura postala je raširena u gotovo svim industrijama (poznato kao doba raširenog računarstva (engl. *Pervasive computing*)) gdje je svaka druga riječ sada započinjala s „e-", na primjer, e-trgovina, e-poslovanje, e-uprava itd., jer je sve počelo biti elektronički [1]. Budući da su se pojavili različiti uređaji (osobni digitalni asistenti, pametni telefoni, prijenosna računala, tableti, itd.), postalo je teško jasno definirati računalo. Pojavio se i mobilno računarstvo (Bluetooth i Wi-Fi)

koje je stvari još više zakompliciralo. Online platni sustavi i upotreba kreditnih kartica postali su vrlo popularni i intenzivirale su se web aplikacije. Uslijedile su inovacije i razvoj 21. stoljeća s jakom ovisnošću o IT infrastrukturi. Ovo je otvorilo nova i atraktivna vrata za hakersku zajednicu. Napadači su evoluirali od računalnih entuzijasta do profesionalnih hakera te sazreli od korištenja vještina hakiranja kako bi pokazali da mogu zaobići proces potvrde autentičnosti i doći do tuđih podataka do korištenja tih podataka u krađi brojeva kreditnih i debitnih kartica, poslovnih tajni i osobnih podataka za financijsku dobit. To je rezultiralo prijetnjama informacijske sigurnosti poput ucjenjivačkog softvera (engl. *Ransomware*), socijalnog inženjeringa, napada s ciljem krađe identiteta (engl. *Phishing*) i sl. koji lako mogu ugroziti autentikacijske i autorizacijske vjerodajnice [1].

2.3. Odnos informacijske i kibernetičke sigurnosti

Izraz kibernetička sigurnost (engl. *Cyber security*) često se upotrebljava naizmjenično s pojmom informacijska sigurnost što može dovesti do nejasnoća u razumijevanju na što se točno misli po tim pojmom te radi li se zaista o istoznačnicama.

Međunarodna organizacija za standardizaciju (ISO) definira **kibernetičku sigurnost** kao „*očuvanje povjerljivosti, integriteta i dostupnosti informacija u kibernetičkom prostoru*", gdje je kibernetički prostor „*složeno okruženje koje proizlazi iz interakcije ljudi, softvera i usluga na Internetu pomoću tehnoloških uređaja i povezanih mreža, a koje ne postoji u fizičkom obliku*" [46]. Ako tu definiciju usporedimo s već prije spomenutom definicijom **informacijske sigurnosti** iste organizacije gdje je informacijska sigurnost „*očuvanje povjerljivosti, integriteta i dostupnosti informacija*" [32], možemo vidjeti da su definicije gotovo identične, ali uz jednu bitnu razliku – kibernetički prostor.

U prilog tome da to nisu dva identična pojma govore Von Solms i Van Niekerk [47] koji tvrde da, iako postoji značajno preklapanje između kibernetičke i informacijske sigurnosti, ova dva koncepta nisu u potpunosti istoznačna. Dio koji se preklapa je zaštita informacijske imovine koja se pohranjuje ili prenosi korištenjem informacijske i komunikacijske tehnologije. Dio koji se razlikuje u informacijskoj i kibernetičkoj sigurnosti je činjenica da je fokus informacijske sigurnosti također informacijska imovina koja se pohranjuje ili prenosi bez informacijske i komunikacijske tehnologije, dok je s druge strane fokus kibernetičke sigurnosti također i ne-informacijska imovina koja je osjetljiva na prijetnje putem informacijske i komunikacijske tehnologije.

Nadalje, u njihovom radu se navodi da kibernetička sigurnost nadilazi granice tradicionalne informacijske sigurnosti i uključuje ne samo zaštitu informacijskih resursa, već i ostale imovine, uključujući i samu osobu. U informacijskoj sigurnosti referenca na ljudski faktor se obično odnosi na uloge ljudi u sigurnosnom procesu dok u kibernetičkoj sigurnosti ovaj faktor ima dodatnu dimenziju, ljude kao potencijalne mete kibernetičkih napada ili čak nesvjesne sudionike u takvim napadima [47]. Stoga, u stvarnosti, kibernetička sigurnost uključuje i zaštitu interesa neke osobe, društva ili nacije, uključujući i njihovu informacijsku i ne-informacijsku imovinu koju treba zaštititi od rizika koji se odnose na njihovu interakciju s kibernetičkim prostorom [48]. Dakle, fokus informacijske sigurnosti je zaštita informacija [47] od mogućih štetnih posljedica različitih prijetnji i ranjivosti dok je kibernetička sigurnost usmjerena na zaštitu samog kibernetičkog prostora, kao i zaštita ljudi koji funkcioniraju u kibernetičkom prostoru i bilo koje imovine koja se može dosegnuti putem kibernetičkog prostora [49], [48].

Dodatno, Ried i Van Niekerk [48] tvrde da je temeljna razlika u tome što informacijska sigurnost ima za cilj osigurati kontinuitet poslovanja i ograničiti utjecaj sigurnosnih incidenata, kako bi se umanjila poslovna šteta, čime se naglašava taj fokus informacijske sigurnosti prvenstveno na očuvanje informacija u organizacijskom kontekstu. Međutim, kibernetička sigurnost proteže se daleko izvan granica organizacije, budući da se informacije dijele i koriste u kibernetičkom prostoru. Stoga, iako postoji uska povezanost između informacijske sigurnosti i kibernetičke sigurnosti, postoje aspekti koji spadaju izvan opsega informacijske sigurnosti [50] što su Von Solms i Van Nieker [47] pokazali na primjeru sigurnosnih incidenata.

Oni su krenuli od pretpostavke, da ako je kibernetička sigurnost sinonim za informacijsku sigurnost bilo bi opravdano pretpostaviti da bi se incidenti kibernetičke sigurnosti mogli opisati i u smislu karakteristika koje se koriste za definiranje informacijske sigurnosti. Stoga bi incident kibernetičke sigurnosti također doveo do kršenja povjerljivosti, integriteta ili dostupnosti informacija [47]. Autori dalje navode kako ta pretpostavka vrijedi za većinu prijetnji koje se odnose na kibernetičku sigurnost kojima zaposlenici i/ili organizacija mogu biti izloženi, ali tvrde i kako postoje prijetnje kibernetičke sigurnosti koje nisu dio formalno definiranog opsega informacijske sigurnosti te objašnjavaju nekoliko scenarija koji to potvrđuju [47].

Ti scenariji bave se specifičnim aspektom kibernetičke sigurnosti gdje interesi osobe, društva ili čak nacije, uključujući njihovu imovinu koja se ne zasniva na informacijama, moraju biti zaštićeni od rizika koji proizlaze iz interakcije s kibernetičkim prostorom, a odnose se na

internetsko zlostavljanje (engl. *Cyberbullying*), kućnu automatizaciju (engl. *Home Automation*) i kibernetički terorizam (engl. *Cyberterrorism*) [47].

Kod *internetskog zlostavljanja* ne dolazi do gubitka povjerljivosti, integriteta ili dostupnosti informacija, već je cilj takvih aktivnosti sam korisnik što znači da internetsko zlostavljanje dovodi do izravne štete toj osobi. Povećanu udobnost upravljanja domom putem interneta (*kućna automatizacija*) prati povećan rizik da bi netko mogao dobiti neovlašteni pristup takvim sustavima i nanijeti štetu koja se može kretati od 'psina' poput isključivanja tople vode, do teških zločina poput isključivanja sigurnosnog sustava radi provale u dom, što ne mora nužno utjecati na žrtvine informacije. Kod *kibernetičkog terorizma*, kibernetički teroristi mogu ciljati kritičnu infrastrukturu zemlje putem kibernetičkog prostora što može biti ili neizravno, na primjer utjecajem na dostupnost informacijskih usluga pomoću napada uskraćivanja usluge ili, izravnije, napadom na nacionalnu električnu mrežu. U slučaju napada na takvu kritičnu infrastrukturu, gubitak podrazumijeva ne samo integritet ili dostupnost informacijskih resursa, već i pristup takvim kritičnim uslugama. U ovom slučaju nije u opasnosti ni sama informacija, niti pojedinačni korisnik informacija, već dobrobit društva u cjelini [47].

Dakle, iako su pojmovi informacijska sigurnost i kibernetička sigurnost vrlo slični i oba se odnose na osmišljavanje i provedbu zaštitnih kontrolnih mjera koje će zaposlenike i organizacije štititi od sigurnosnih napada, krađe podataka i incidenata, kibernetička sigurnost se ipak odnosi na specifične, visokosofisticirane metode napada, fokusirajući se zaštitnim mjerama ne samo na organizacije, nego gotovo podjednako i na ljude-pojedince, pokrivajući pri tome organizacijske, tehnološke i društvene aspekte napada i zaštite [51].

Von Solms i von Solms [52] odlaze korak dalje i tvrde kako je kibernetička sigurnost zapravo podskup informacijske sigurnosti jer bez obzira na to koliko je povezanosti omogućio kibernetički prostor, koncepti sigurnosti obuhvaćeni informacijskom sigurnošću još uvijek su primjenjivi na kibernetičku sigurnost. Dvije osnovne promjene u odnosu na prije su da se, zbog povećane povezanosti povećala i potreba zaštite jer smo sada izloženi većem broju imovine odnosno uređaja, opreme, korisnika i sl. [53] gdje takva imovina uključuje apsolutno bilo koga ili bilo što do čega se može doći putem kibernetičkog prostora [47] te da je, zbog povećane povezanosti, kibernetički prostor predstavio nove sigurnosne prijetnje i rizike [53].

U konačnici, De Bruin i Von Solms [53] napominju kako sredstva i načini zaštite od gore spomenute dvije osnovne promjene nisu različiti između kibernetičke i informacijske sigurnosti čime dolaze do zaključka kako kibernetička sigurnost i informacijska sigurnost nisu zasebne

ideje već kibernetička sigurnost primjereno živi unutar informacijske sigurnosti, a sigurnosni principi su isti dok se samo razlikuje način na koji se provode.

3. UPRAVLJANJE INFORMACIJSKOM SIGURNOŠĆU

U današnje vrijeme, informacije su jedan od glavnih resursa modernih organizacija [54], a često i njihova najvrjednija imovina zbog čega su glavna meta namjernih napada [28] te se može izvući zaključak kako se zaštita povjerljivosti, integriteta i dostupnosti informacija ne može preuveličati [55].

Informacijska sigurnost dramatično se promijenila tijekom posljednjih desetljeća te je postala najvažniji aspekt za većinu organizacija [54]. Informacije koje su nekad bile materijal koji pomaže poslovanju, a sad predstavljaju najvažniju imovinu većine tvrtki, ranjivije su nego prije zahvaljujući širenju mreža i povezivanju organizacija širom svijeta [23] zbog čega su izložene sve većem i različitijem broju prijetnji i ranjivosti [56], a samim time i napada na sigurnost [54].

Međutim, informacijska sigurnost ne pokriva samo same informacije već i cjelokupnu infrastrukturu koja olakšava njihovu upotrebu pa tako pokriva hardver, softver, prijetnje, fizičku sigurnost i ljudske čimbenike, gdje svaka od tih komponenata ima svoje osobine [20]. Informacijska sigurnost doprinosi razvoju poslovanja osiguravajući pouzdanost poslovanja te se sve više promatra kao stvaratelj vrijednosti ili pokretač poslovanja u novim poslovnim modelima. Njena dodana vrijednost uključuje pružanje pouzdane i sigurne razmjene, osiguranje sigurnog prijenosa podataka, omogućavanje udaljenog zaštićenog pristupa, osiguravanje dostupnosti usluga, kao i mogućnost eksternalizacije procesa na kontroliran i siguran način [57].

Različite organizacije trebaju različite razine sigurnosti, ali iako sigurnosni zahtjevi za određenu organizaciju možda nisu toliko visoki kao sigurnosni zahtjevi drugih organizacija i dalje će biti važno postizanje optimalne sigurnosti za određenu situaciju te organizacije [58] imajući u vidu poslovne ciljeve i poslovne zahtjeve organizacije prilikom implementacije sigurnosnih mjera [35]. No, iako je informacijska sigurnost prepoznati problem, često se događa da organizacije imaju malo ili nimalo razumijevanja što učiniti ili kako [55] te se nerijetko događa da tijekom izgradnje informatizacije mnoge organizacije, uslijed nedostatka vremena, ljudi ili novca obavljaju aktivnosti rukovodeći se mišlju „prvo posao, onda sigurnost” [24].

Važno je naglasiti da ne postoji „srebrni metak” za učinkovitu informacijsku sigurnost jer danas niti jedan samostalni mehanizam ili tehnologija više nisu dovoljni za postizanje uspjeha. Umjesto toga, učinkovita sigurnost informacija može se postići holističkim pristupom koji primjenjuje više mehanizama za usklađivanje organizacijskih i sociooloških čimbenika unutar organizacije u kombinaciji s tehnološkim kompetencijama [2], [3].

3.1. Informacijska sigurnosti kao problem upravljanja

Iako se zadnjih godina situacija počela mijenjati, bila je uobičajena praksa smatrati informacijsku sigurnost tehnološkim problemom s tehnološkim rješenjem [20] pod jurisdikcijom IT odjela, odvojeno od glavnog poslovanja [59], [15].

Danas, informacijska sigurnost više nije čisto tehničko pitanje te zahtijeva uključivanje višeg rukovodstva u uspostavu politika, procedura, organizacijskih struktura i zaposlenika za poboljšanje informacijske sigurnosti [60] čime postaje važno upravljačko pitanje budući da je njena svrha stvaranje sigurnog informacijskog okruženja [30]. Mnogi autori [8], [58], [2], [61], [60] suglasni su oko toga kako je informacijska sigurnost prvenstveno problem upravljanja i poslovanja te ju treba tretirati kao poslovnu sigurnost, a ne tehnički problem [62].

Von Solms i Von Solms [61] još su prije više od 15 godina identificirali deset bitnih aspekata koji će, ako se ne uzmu u obzir prilikom planiranja upravljanja informacijskom sigurnošću, sigurno prouzrokovati neuspjeh ili barem ozbiljne nedostatke u upravljanju informacijskom sigurnošću. Od tih deset aspekata prva tri su: 1) neshvaćanje da je informacijska sigurnost odgovornost korporativnog upravljanja, 2) ne shvaćanje da je informacijska sigurnost poslovno, a ne tehničko pitanje te 3) ne shvaćanje činjenice da je upravljanje informacijskom sigurnošću višedimenzionalna disciplina [61].

3.2. Informacijska sigurnost kao dio korporativnog upravljanja

Upravljanje informacijskom sigurnošću je kontinuirani, strukturirani i sustavni sigurnosni pristup upravljanju i zaštiti informacija organizacije od ugrožavanja od strane neodgovornih pojedinaca [63], a informacijska sigurnost treba biti integrirana u korporativno upravljanje organizacije [36], [57].

Tome u prilog govori i činjenica da će se, ako misija i strategija organizacije nisu definirane, organizacija i dalje boriti za sigurnost svojih podataka, a zaposlenici neće shvatiti ozbiljno svoju odgovornost i neće slijediti i poštivati smjernice vezane za informacijsku sigurnost. Drugim riječima, srž informacijske sigurnosti mora dolaziti s vrha organizacije kako bi se potaknuo ozbiljan stav zaposlenika i očekivanja da će se pridržavati pravila i propisa vezanih uz informacijsku sigurnost [20]. Sigurnosna strategija organizacije mora uravnotežiti informacijsku sigurnost s omogućavanjem poslovanja te osigurati usklađenost s unutarnjim i

vanjskim zahtjevima vezanim uz informacijsku sigurnost [3] za što je potrebno dedicirati dovoljan budžet [20].

Razlika između upravljanja informacijskom sigurnošću (engl. *Information Security Management*) i korporativnog upravljanja informacijskom sigurnošću (engl. *Information Security Governance*) nije baš uvijek u potpunosti jasna, no može se reći kako upravljanje obuhvaća provedbu i nadzor sigurnosnog programa, dok korporativno upravljanje daje strateške smjernice i osigurava njihovo pravilno izvršavanje, odnosno općenito govoreći, korporativno upravljanje uključuje odlučivanje, dok upravljanje osigurava implementaciju kontrola [57]. To znači da je korporativno upravljanje informacijskom sigurnošću primjena principa korporativnog upravljanja na funkciju informacijske sigurnosti gdje ti principi uključuju odgovornost izvršnog rukovodstva da osigura strateški smjer, osigura postizanje ciljeva, nadgleda da se rizicima upravlja na odgovarajući način i da potvrđuje odgovorno korištenje resursa [28]. Osnovna ideja korporativnog upravljanja informatikom i posljedično, informacijskom sigurnošću, je da se donošenje poslovnih odluka vezanih za upravljanje informacijskim sustavima i informacijskom sigurnošću više ne može prepustiti samo profesionalnim informatičarima, već važnu ulogu pri tome treba imati najviša razina rukovodstva [64].

Prema Volchkovu [57] učinkovito korporativno upravljanje informacijskom sigurnošću ima sljedeće karakteristike: *uključena je cijela tvrtka*, što znači da je poznata imovina koja mora biti zaštićena i određena je razina sigurnosti, a sigurnosne mjere podržavaju poslovanje; *definirane su odgovornosti*, što znači da su uprava i rukovodstvo uključeni u proces odlučivanja u sigurnosnom programu, a vlasnici informacija identificirani i aktivni; *razina zaštite ovisi o apetitu za rizik*, što znači da je definirana prihvatljiva razina rizika i uspostavljeno proaktivno upravljanje rizicima vezano za sve aktivnosti organizacije; *sigurnošću se aktivno upravlja*, što, između ostalog, podrazumijeva da se sigurnosni program nadzire, revidira i prilagođava potrebama organizacije [57].

3.3. Holistički pristup upravljanju informacijskom sigurnošću

Povijesno gledano, problemi informacijske sigurnosti redovito su se proučavali u tehnološkom kontekstu [2], pa su tako organizacije pratile tehnički usredotočenu strategiju informacijske sigurnosti koja naglašava primarnu ulogu tehnologije u oblikovanju učinkovitih sigurnosnih rješenja [3] gdje je takav model upravljanja informacijskom sigurnošću bio reaktivan i rijetko

usklađen s poslovnim potrebama [65]. Međutim, sadašnje gledište je da učinkovita strategija informacijske sigurnosti mora biti uravnotežena, naglašavajući važnost tehnologije, ali i sociološko-organizacijski kontekst organizacije, a sve veće sigurnosne potrebe proširile su pozornost istraživača na istraživanje uloge rukovodstva u upravljanju informacijskom sigurnošću [2].

Istraživači se slažu kako tehnologija ne može pružiti cjelovito rješenje te se sigurnost informacija ne može više osigurati korištenjem samo tehnoloških rješenja i kontrola [66], [67], [68], [8], [57], [69] budući da je sigurnost i „tehnički problem", ali i „problem ljudi" [6], [70].

Iz toga proizlazi da organizacije koje žele preživjeti u narednim godinama moraju razviti cjelovit i sveobuhvatan pristup informacijskoj sigurnosti [2], prihvaćajući i ljudsku i tehničku dimenziju [71], odnosno koristiti holistički pristup informacijskoj sigurnosti [65], uzimajući u obzir sve njene dimenzije [72], a posebno tehničke, upravljače i ljudske aspekte [69], [73].

U novijoj literaturi postoji konsenzus oko toga da je potrebno posvetiti jednaku pažnju tehničkim i ne-tehničkim aspektima informacijske sigurnosti te brojni autori ističu važnost integracije tehničkih i upravljačkih aktivnosti. Iako nisu u potpunosti usuglašeni oko naziva dimenzija koje čine informacijsku sigurnost, kao što prikazuje Tablica 3.1., istraživači uglavnom govore o tri ključne kategorije odnosno dimenzije koje čine trokut *ljudi-procesi-tehnologija.*

Upravo uzimanje u obzir više dimenzija informacijske sigurnosti putem holističkog pristupa stvara temelj slojevite ili dubinske obrane (engl. *Defense-in-depth*) koja pruža najopsežniju zaštitu [84], [28], [85]. Slojevita se obrana temelji na činjenici da oslanjanjem na jednu jedinstvenu kontrolu (ili vrstu kontrole) organizacija može postati izložena rizicima koji tom kontrolom nisu pokriveni [71] te bi trebalo primijeniti nekoliko komplementarnih pristupa kako bi se poboljšala sigurnost i interakcija ljudi s informacijskim sustavima [86].

Napadaču jedan obrambeni mehanizam može biti relativno lak za zaobići pa je osnovna ideja iza strategije dubinske obrane usporiti napadača što je više moguće s više slojeva obrane [84] kako bi se povećao trošak napadača u vidu dodatnog vremena, truda ili opreme koje mora uložiti [23]. Usporavanjem napadača, organizacija bi povećala šanse za otkrivanje i reagiranje na napad u tijeku, a povećani troškovi za napadača mogli bi ga odvratiti od nekih njegovih pokušaja napada ako procijeni da troškovi nadmašuju moguću korist od uspješnog napada [10]. Dubinska obrana treba uključivati ljude, tehnologiju i procese [23] pa će tako organizacija

postaviti kritičnu opremu za obradu poslovnih informacija u sigurno područje, osigurati prilagođenu zaštitu za potvrđene rizike, izgraditi odgovarajuće sigurnosne barijere i kontrolu pristupa, smanjiti neovlašteni pristup, konfigurirati antivirusni sustav, uspostaviti proces redovnih instalacija zakrpi na poslužiteljima, propisati uloge i odgovornosti, kao i pravila ponašanja te upoznati sve zaposlenike s važećim pravilima ponašanja putem edukacija i radionica podizanja svijesti o informacijskoj sigurnosti [24].

Tablica 3.1. Dimenzije informacijske sigurnosti

Rbr.	Dimenzije informacijske sigurnosti	Reference
1.	Tehnološki kontekst; organizacijski aspekt; kontekst okoline	[37]
2.	Tehnologija; ljudska svijest i kvalifikacije	[74]
3.	Tehničke kontrole; ljudske kontrole	[6]
4.	Tehnički čimbenici; organizacijski čimbenici; individualni čimbenici	[75]
5.	Tehničke kontrole; proceduralne kontrole; ljudi koji koriste kontrole	[76]
6.	Ljudi; organizacija; proces	[63]
7.	Tehnički resursi; socio-organizacijski resursi	[77]
8.	Tehnički aspekti; upravljački aspekti; ljudski aspekti	[69]
9.	Ljudska pitanja; procesna pitanja; tehnološka pitanja	[78]
10.	Ljudi; procesi; tehnologija	[79]; [41]
11.	Organizacijski procesi: tehnologija; način na koji zaposlenici obrađuju informacije	[80]
12.	Ljudi; edukacija; tehnologija	[4]
13.	Ljudska dimenzija; tehnička dimenzija	[71]
14.	Tehnički aspekti; organizacijski aspekti; ljudski aspekti; društveni aspekti	[54]
15.	Organizacijski čimbenici; individualni čimbenici; tehnički čimbenici	[75]
16.	Tehnologija; ljudi; organizacija	[81]
17.	Ljudski faktori; organizacijski aspekti; tehnološke kontrole	[82]
18.	Upravljanje; tehnologija; korisnici	[73]
19.	Ljudi; politike; tehnologija	[35]
20.	Tehnički aspekti; ljudski aspekti; socijalni aspekti; organizacijski aspekti	[83]

Izvor: *vlastiti prikaz*

Uz pritisak visokih troškova implementacije i održavanja, organizacije trebaju razlikovati kontrole koje su im potrebne od onih manje važnih [87] na način da odabrane kontrole mogu kontrirati specifičnim prijetnjama i na taj način smanjiti pridružene rizike [88]. Lopes i Oliveira [54] ističu kako su poduzete mjere u najvećem omjeru one kontrole povezane s fizičkom sigurnošću, a slijede mjere povezane s logičkim kontrolama te naposljetku one povezane s

ljudskim aspektom organizacije, koje su zapravo te koje predstavljaju najveći nedostatak brige od strane organizacije i njenih čelnika.

Van Niekerk i Von Solms [88] kategoriziraju sigurnosne kontrole kao fizičke, tehničke i operativne kontrole dok Campbell [25] koristi izraz „proceduralne" umjesto „operativne" kontrole. Fizičke kontrole bave se fizičkim aspektom sigurnosti, na primjer bravom na vratima, sigurnosnim ormarima i zaštitarima ili sustavima fizičke detekcije provale, poput alarmnih sustava i video nadzora [25]. Tehničke kontrole predstavljaju tradicionalne mjere sigurnosti koje se mogu očekivati u korporacijskoj tehnologiji, poput vatrozida, antivirusnog sustava ili sustava za skeniranje ranjivosti [25]. Operativne kontrole su sve kontrole koje u nekom obliku upravljaju ponašanjem ljudi [88], što su zapravo i proceduralne kontrole prema Campbellu, koje obično imaju oblik politika i procedura koje definiraju kako se zaposlenici trebaju ponašati [25]. Ponekad se fizičke i tehničke sigurnosne kontrole stavljaju u zajedničku skupinu tehničkih kontrola za razliku od operativnih (proceduralnih) koje se stavljaju u skupinu ne-tehničkih kontrola.

3.4. Izazovi informacijske sigurnosti

Proces uspostave učinkovitog upravljanja informacijskom sigurnošću u organizaciji neminovno dolazi do brojnih izazova. Od gledanja na sigurnost kao na mjesto troška i funkciju koja je manje vrijedna od ostalih korporativnih funkcija koje donose profit [23] te se ne smatra poslovnim pokretačem niti izvorom konkurentske prednosti [89], preko zabluda o informacijskoj sigurnosti, poput onih da je sigurnost čisto tehničko pitanje i da se može postići bez uključivanja korisnika ili da se tijek informacija može u potpunosti kontrolirati [90] pa sve do neoptimalnog ulaganja u informacijsku sigurnost [91] koje, uslijed neočekivanog povrata izaziva nezadovoljstvo rukovodstva te nerealnog optimizma [92] prilikom procjene rizika ili upravljanja sigurnosnim incidentima.

Dodatne izazove predstavljaju stalno mijenjajuće prijetnje poput raznih vrsta zlonamjernog softvera, nove vrste napada putem socijalnog inženjeringa, ponašanje zaposlenika uslijed neznanja ili jednostavno nebrige, nedostatak podrške višeg rukovodstva, neznatna tehnička oprema, tehnološke greške u hardveru i softveru ili nepostojanje internih smjernica i standarda, nedostatak znanja, osposobljavanja i edukacija iz domene informacijske sigurnosti te nedostatak financijskih sredstava posvećenih upravljanju informacijskom sigurnošću [93] gdje su ti izazovi posebno izraženi kod malih i srednjih poduzeća [94].

Područje informacijske tehnologije, a tako i informacijske sigurnosti, jedno je od najbrže mijenjajućih i razvijajućih područja što znači da se organizacije konstantno moraju nositi s novim izazovima uslijed novih prijetnji koje možda do prije nekoliko godina nisu obuhvaćali u svojim procjenama rizika i odgovorima na sigurnosne incidente. Tu su primjerice sigurnosni izazovi povezani s Internetom stvari (engl. *Internet of Things*), društvenim medijima, kognitivnim računarstvom, pametnim automobilima, pametnim gradovima i drugim novim primjenama informacijske tehnologije koje donose nove mogućnosti, zajedno s novom prijetnjom [85].

3.4.1. Sigurnost naspram funkcionalnosti

Sigurnost je po svojoj prirodi neugodna, a što su sigurnosni mehanizmi robusniji, proces postaje neugodniji. Tako zaposlenici, koji moraju obavljati svoj posao za koji su plaćeni, žele odmah početi raditi, bez dodatnih komplikacija, kao što je enkripcija diska ili dvofaktorska provjera autentičnosti zbog čega često smatraju kako je sigurnost uglavnom dosadna, iritantna smetnja inače pristupačnom svijetu komunikacije bez smetnji [23].

Sigurnost se često smatra štetnom za poslovne ciljeve jer sustav čini manje korisnim [95] budući da se većina sigurnosnih mehanizama, od složenih lozinki do višefaktorske provjere autentičnosti smatra preprekama do produktivnosti [23]. Stoga se može tvrditi da je cilj osiguranja informacija u određenoj mjeri u sukobu s normalnim poslovnim ciljevima maksimiziranja produktivnosti [96] i smanjenja troškova [95]. Informacijska sigurnost mora postati dio uspješnosti posla, a ne biti u sukobu s obavljanjem posla [97], međutim informacijska sigurnost se ne može ostvariti bez njenog prihvaćanja u svakodnevnom radu [98].

Da bi informacijska sigurnost bila prihvaćena u svakodnevnom radu sigurnosne kontrole moraju biti smislene i što manje nametljive [99] odnosno potrebno je odrediti ravnotežu između omogućavanja poslovanja i osiguranja informacijske imovine [3], [100]. Sigurnosne kontrole temelje se na kliznoj ljestvici gdje je jedan kraj potpuna sigurnost i potpuna neugodnost, a drugi je potpuna nesigurnost i potpuna jednostavnost korištenja zbog čega je bilo koju sigurnosnu kontrolu potrebno pozicionirati na ljestvici tako da razina sigurnosti i jednostavnost uporabe odgovaraju prihvatljivoj razini rizika za organizaciju [23] budući da prekomjerna zaštita kroz strogu kontrolu može spriječiti funkcionalnost poslovanja, dok labave kontrole mogu stvoriti neprihvatljive rizike za informacijsku imovinu [3].

Iako informacijska sigurnost može izravno ometati ili biti u sukobu s drugim organizacijskim vrijednostima, poput otvorenosti, učinkovitosti i privatnosti, realizacija ciljeva povezanih s drugim vrijednostima može također izravno ovisiti o sigurnosti informacija [101] zbog čega se informacijska sigurnosti ne bi trebala zanemariti u svakodnevnom radu već biti sastavni dio svih aktivnosti [35].

3.4.2. Ulaganja u informacijsku sigurnost

Ulaskom u 21. stoljeće područje ekonomije sigurnosti se proširilo i njezin se fokus kreće prema razvoju matematičkog modela za optimizaciju troškova sigurnosti [102] budući da se, u idealnom slučaju, odluke o ulaganju ograničenih resursa u nove ili dodatne postupke i tehnologije za koje se očekuje da će unaprijediti sigurnost informacija temelje na kvantitativnim analizama [103]. Međutim, sigurnost je teško kvantificirati budući da odsutnost aktivnosti ne govori je li nedostatak uspješnih napada rezultat dobre sigurnosti ili samo pitanje sreće te se organizacije mogu samo nadati da će ulaganje u informacijsku sigurnost odgoditi trenutak kad će organizacija podleći napadu budući da ne postoji savršena sigurnost [103].

Zakonodavni pritisci i sigurnosni proboji tjeraju organizacije da pribjegnu ulaganju u informacijsku sigurnost [104], a istraživanja i izvješća o sigurnosti informacijskih sustava upućuju na to da upravljanje i zaštita informacijske imovine brzo postaje kritična briga za organizacije jer nastaju veliki troškovi u pokušaju zaštite tih resursa [105] budući da u postizanju visoke razine sigurnosti organizacija mora biti u mogućnosti uložiti znatnu količinu novca kako bi uspješno i učinkovito zaštitila svoju imovinu [59] odnosno zadržala napadača izvan svog sustava [102].

No, s druge strane, ekonomska perspektiva prepoznaje da, iako je ulaganje u informacijsku sigurnost dobro, veća razina sigurnosti ne vrijedi uvijek više [106] što znači da vrijednost informacija mora opravdati troškove zaštite [107], a organizacije trebaju putem načela „umjerene zaštite" odabrati odgovarajuće sigurnosne tehnologije i proizvode na temelju razmatranja troškova i povrata ulaganja [24].

Gordon i Loeb [106] tvrde kako za određeni potencijalni gubitak organizacija ne smije nužno usmjeriti svoje investicije na informacije s najvišom ranjivošću budući da su iznimno ranjivi skupovi informacija možda neuobičajeno skupi za zaštitu te bi organizaciji bilo bolje koncentrirati svoje napore na skupove informacija sa srednjim ranjivostima. To znači da je mala ili nikakva informacijska sigurnost ekonomski opravdana za iznimno visoke, kao i za iznimno

niske razine ranjivosti, dok bi se organizacija trebala fokusirati na ulaganja u zaštitu informacija koje imaju srednju razinu ranjivosti na sigurnosne proboje [106].

Budući da informacijski sustav ne može biti potpuno siguran bez obzira na to koliko ulaganja je uloženo [91], a optimalni izdaci za zaštitu određenih skupova informacija ne povećavaju se uvijek s povećanjem ranjivosti informacija [106], optimalno ulaganje ne smije prelaziti očekivani gubitak za profitnu organizaciju [91].

Štoviše, Ye i Feng [91] navode kako je optimalno ulaganje u informacijsku sigurnost manje od polovice očekivanog gubitka bez ulaganja u sigurnost i to čak i ako se vjerojatnost prijetnje povećava s ranjivošću sustava.

U konačnici, organizacija koja se suočava s odlukom o troškovima sigurnosti trebala bi najprije razmotriti potrebu potrošnje, a tek tada odrediti koliko i na što potrošiti jer je u protivnom vjerojatni rezultat neučinkovita potrošnja [108] poput primjerice pretjeranog ulaganja u tehničke mjere zaštite kao što su vatrozidi, složeni kriptografski sustavi i sustavi za prevenciju i detekciju sigurnosnih proboja da bi se na kraju dogodio sigurnosni proboj uslijed nedostatka ulaganja u obuku i podizanje svijesti zaposlenika o informacijskoj sigurnosti [71].

3.4.3. Upravljanje rizicima

Velika većina današnjih organizacija snažno se oslanja na informacijske sustave koji pohranjuju osjetljive podatke potrebne za učinkovito poslovanje organizacije, uključujući financijske podatke, informacije o korisnicima i zapise o proizvodima zbog čega je neophodno upravljati rizicima povezanim s gubitkom važnih informacija.

Ideja upravljanja rizicima je da se moraju prepoznati, klasificirati i procijeniti prijetnje svih vrsta kako bi se izračunao njihov potencijal štete [23] u odnosu na ranjivost informacijske imovine organizacije koja je prošla proces identifikacije, klasifikacije i određivanja prioriteta [28] te provelo primjereno tretiranje prepoznatog rizika [29]. Međunarodna organizacija za standardizaciju [32] definira rizik kao „*mogućnost štetnih posljedica za organizaciju ukoliko prijetnje iskoriste ranjivosti informacijske imovine*", prijetnju kao „*potencijalni uzrok neželjenog događaja koji može rezultirati štetom za sustav ili organizaciju*", a ranjivost kao „*slabost imovine ili kontrole koju može iskoristiti jedna ili više prijetnji*". Prijetnja može biti izazvana namjernim ili nenamjernim radnjama, kao i prirodnim nepogodama, poput poplava,

požara i zemljotresa, koje se ne mogu kontrolirati [29], a da bi se nešto moglo smatrati prijetnjom, ne mora se nužno dogoditi incident ili sigurnosni proboj [25].

Prilikom same procjene rizika potrebno je čim objektivnije sagledati situaciju i ne upasti u zamku tzv. nerealnog optimizma ili optimistične pristranosti koja predstavlja podcjenjivanje vjerojatnosti doživljavanja negativnih događaja budući da, u mnogim negativnim situacijama ljudi pokazuju sklonost vjerovanju da su manje rizični od ostalih i tom optimističnom pristranošću tumače dvosmislene informacije ili nesigurne situacije u, za sebe, povoljnom smjeru [92].

Tako rezultati analize koju su proveli Rhee i suradnici [92] pokazuju da postoji optimistična pristranost rukovoditelja IT-a u pogledu upravljanja sigurnošću i da je opseg pristranosti veći s društvenom distancom od cilja usporedbe, što znači da rukovoditelji IT-a smatraju kako je njihov rizik podjednako velik kao rizik njihovih poslovnih partnera, ali značajno manji od rizika drugih prosječnih organizacija. Nadalje, otkriva se da je percepcija mogućnosti kontroliranja sigurnosnih rizika faktor koji utječe na optimističnu pristranost [92].

Također, Feng i Wang [109] ispitali su povezanost apetita za rizikom rukovoditelja IT-a s incidentima kršenja informacijske sigurnosti. Rezultati su pokazali da je razina averzije prema riziku od strane rukovoditelja IT-a negativno povezana s vjerojatnošću da će doći do sigurnosnih incidenata, a ova povezanost jača je ako je glavni izvršni direktor tvrtke također protivnik rizika. U dodatnim analizama pokazano je da odnos između averzije prema riziku od strane rukovoditelja IT-a i sigurnosnih incidenata ovisi o vrsti kršenja i strateškom položaju tvrtke, a moderira ga moć rukovoditelja IT-a [109].

Postoji više metodologija za procjenu rizika, kao što su *NIST SP800-30 - Risk Management Guide for Information Technology Systems, CRAMM - CCTA Risk Analysis and Management Method, OCTAVE - Operationally Critical Threat, Asset, and Vulnerability Evaluation, ISO/IEC 27005 - Information Security Risk Management, MEHARI - Risk analysis and treatment guide* i druge [39], [42], no sve se generalno slažu u koracima koje je potrebno provesti prilikom procjene rizika. Nakon identifikacije primjenjivih prijetnji i ranjivosti, potrebno je procijeniti razinu rizika i tretirati procijenjene rizike jednom od četiri moguće opcije za tretiranje rizika, koje uključuju prihvaćanje, smanjivanje, prijenos ili izbjegavanje rizika [29], sukladno organizacijskom apetitu za rizikom (engl. *Risk Appetite*) koji predstavlja

količinu i prirodu rizika koje su organizacije spremne prihvatiti dok ocjenjuju kompromise između savršene sigurnosti i neograničene pristupačnosti [28].

Upravo apetitom za rizikom uprava organizacije, čija je krajnja odgovornost za sigurnosne rizike [57], naglašava koji su rizik spremni preuzeti za organizaciju i na taj način određuju koje bi kontrole informacijske sigurnosti trebalo primijeniti da bi se smanjio rizik. Kim i Solomon [39] ističu kako postoje dva ključna načela upravljanja rizikom, a to su: 1) ne trošite više na zaštitu imovine nego što ona vrijedi, što potvrđuju i Whitman i Mattord [28] i 2) protumjera bez odgovarajućeg rizika rješenje je koje traži problem - teško je opravdati njene troškove [39]. Drugim riječima, to znači da će nekad trošak nekih sigurnosnih kontrola premašivati njihovu korist u smanjenju potencijalnog rizika čime će se uprava organizacije odlučiti za opciju prihvaćanja nekih od rizika, nakon primjene troškovno opravdanih kontrola.

3.4.4. Upravljanje incidentima informacijske sigurnosti

Kako raste vrijednost informacijskih sustava i važnost informacija koje štite, tako raste i važnost njihove zaštite. Nažalost, mnoge su organizacije pronašle stvarnu vrijednost učinkovite sigurnosti tek nakon što su doživjele negativne posljedice povezane s povredama sigurnosti [110] gdje je većina povreda sigurnosti rezultat pretpostavki na temelju razmišljanja 'to se neće baš meni dogoditi' [71] odnosno tzv. nerealnog optimizma [92]. Primjer toga je slučaj Sony Computer Entertainment gdje su osobni podaci 100 milijuna ljudi procurili s njihove web stranice za igraće konzole PS3 zbog korištenja starih softverskih inačica, što je hakerskim grupama olakšalo napad na njih putem tzv. napada ubacivanja SQL kôda (engl. *SQL injection*). Odgovornost rukovodstva Sony-a bila je osigurati da se organizacija pravilno bavi ranjivostima koje su izravno izvedene iz informacijskih sustava i organizacijskih nedostataka koje uzrokuju njeni zaposlenici, ali su zakazali [81].

Neki od najvećih sigurnosnih proboja u ranijoj povijesti, kako ih navodi web stranica CSO Online [111] koja pruža vijesti, analize i istraživanja vezana uz sigurnosti i upravljanje rizicima, su sigurnosni proboji koji su pogodili Yahoo, Marriott International, Adult Friend Finder i Equifax.

Yahoo je u rujnu 2016. objavio da je 2014. godine bio žrtva onoga što se smatra najvećim probojem podataka u povijesti. Napadači, za koje je tvrtka vjerovala da su „akteri sponzorirani od strane država", kompromitirali su stvarna imena, adrese e-pošte, datume rođenja i telefonske brojeve 500 milijuna korisnika, a Yahoo je tvrdio da je većina kompromitiranih lozinki bila u

sažetcima (engl. *Hash*). Zatim je u prosincu 2016. Yahoo otkrio još jedan proboj iz 2013. godine od strane drugog napadača koji je kompromitirao imena, datume rođenja, adrese e-pošte i lozinke te sigurnosna pitanja i odgovore za milijardu korisničkih računa. Yahoo je revidirao tu procjenu kompromitiranih korisničkih računa u listopadu 2017. godine kako bi uključio svih svojih 3 milijarde korisničkih računa [111].

Marriott International objavio je u studenom 2018. godine da su napadači ukrali podatke o približno 500 milijuna korisnika. Proboj se u početku dogodilo na sustavima koji podržavaju hotelski brand Starwood počevši 2014. godine. Napadači su ostali u sustavu nakon što je Marriott kupio Starwood 2016. godine i nisu otkriveni do rujna 2018. godine, a uspjeli su uzeti kombinaciju kontaktnih podataka, broja putovnice, brojeva važnih gostiju, putnih podataka i drugih osobnih podataka [111].

Mreža FriendFinder, koja uključuje neobavezna druženja i web stranice sa sadržajem za odrasle poput Adult Friend Finder, imala je sigurnosni proboj sredinom listopada 2016. godine u kojem su ukradeni podaci iz šest baza podataka koji su uključivali imena, adrese e-pošte i lozinke pohranjene tijekom perioda od 20 godina, čime je kompromitirano 412,2 milijuna korisničkih računa [111].

Equifax, jedan od najvećih kreditnih biroa u SAD-u, izjavio je 7. rujna 2017. da je ranjivost aplikacije na jednoj od njihovih web stranica dovela do proboja podataka. Prekršaj je otkriven 29. srpnja, ali tvrtka navodi kako je vjerojatno započela sredinom svibnja. Proboj je kompromitirao osobne podatke (uključujući brojeve socijalnog osiguranja, datume rođenja, adrese, a u nekim slučajevima i brojeve vozačkih dozvola) 143 milijuna klijenata te podatke o kreditnim karticama 209.000 klijenata. Taj je broj povećan na 147,9 milijuna u listopadu 2017. godine [111].

Kao što je vidljivo iz navedenih primjera, izazov čuvanja informacija i pridružene informacijske imovine sigurnima nikad nije bio veći, ne samo zbog broja napada, koji su posljednjih godina eksponencijalno porasli, unatoč činjenici da se milijarde dolara godišnje troše na sigurnosnu obranu, već i zbog poteškoća u obrani od tih napada. Te poteškoće uključuju: brzinu napada, veću sofisticiranost napada, jednostavnost napadačkih alata (ne zahtijevaju više puno tehničkih znanja za upotrebu), brže otkrivanje ranjivosti, kašnjenje u provedbi sigurnosnih zakrpa, distribuirani napadi, zbunjenost korisnika [84]. Istraživanje koje je proveo Deloitte 2019.

godine [112] navodi kako je 57% organizacija zadnje sigurnosne incidente ili proboje doživjelo u posljednje dvije godine.

Organizacije troše milijarde dolara razvijajući slojevitu obranu protiv napadača i implementiraju rješenja kao što su antivirusni sustavi, sustavi za otkrivanje i/ili sprečavanje proboja i druga tehnička rješenja za zaštitu informacija [113], zanemarujući činjenicu da će uporni napadači na kraju dobiti pristup bez obzira kakva zaštita bila [114] budući da danas loši dečki ne pokušavaju probiti vatrozid, već ga zaobilaze [113]. Uz primjenu ovih sofisticiranih rješenja, napadači se sada okreću ciljanim napadima usredotočenim na prijevaru korisnika da klikne na internetsku poveznicu ili otvori privitak, kao što je detaljnije opisano u potpoglavlju *3.4.6. Socijalni inženjering*.

Incidenti vezani uz informacijsku tehnologiju i informacijski sustav utječu na poslovanje i, kao što mnogi primjeri pokazuju, također mogu imati ozbiljne poslovne utjecaje, a osiguravanje kontinuiranih IT operacija jedno je od osnovnih odgovornosti upravljanja informacijskom sigurnošću unutar organizacije [115]. Tako je ucjenjivački softver (engl. *Ransomware*) WannaCry, kao jedan od najutjecajnijih i najraširenijih zlonamjernih programa u 2017. godini koji je pogodio više od 150 zemalja širom svijeta [116], pokazao koliko je bitna redovita izrada sigurnosne kopije podataka kako se ne bi dogodilo da organizacija uslijed napada ucjenjivačkog softvera koji kriptira podatke, nepovratno izgubi ključne poslovne informacije.

Istraživanja pokazuju kako većina organizacija mjesecima ne zna da je napadnuta pa je tako prosječno vrijeme za prepoznavanje sigurnosnih proboja u 2019. godini bilo 206 dana, a prosječno vrijeme obuzdavanja proboja 73 dana, odnosno ukupno 279 dana od otkrivanja do rješavanja što predstavlja porast od 4,9% u odnosu na 266 dana životnog ciklusa sigurnosnog proboja u 2018. godini [117]. Najdulje razdoblje koje je napadač bio prisutan u sustavu prije nego što je otkriven sigurnosni proboj je čak 9 godina [118].

Izvori sigurnosnih incidenata ugrubo se mogu podijeliti na **prirodne prijetnje**, koje obuhvaćaju potrese, požare, erupcije vulkana, tsunamije i ostale elementarne nepogode, **prijetnje uzrokovane ljudskim djelovanjem**, u kojima je čovjek glavni akter svojim djelovanjem, bilo namjernim ili nenamjernim te **tehničke prijetnje**, koje uključuju pad infrastrukture, kvar dijela računalnog sustava, greške u sustavu i sl. [119].

Unatoč ovom rasponu izvora sigurnosnih incidenata, u gotovo svakom incidentu informacijske sigurnosti uzrok je bio ljudski čimbenik [114], [97], [120], bilo da se radi o namjernim

radnjama, kao što su krađa, vandalizam, sabotaža i špijunaža [113] ili, češće, nenamjernim ljudskim pogreškama zbog neiskustva, nepravilne obuke [28] ili nedostatka znanja i svijesti o informacijskoj sigurnosti [97]. Globalno istraživanje informacijske sigurnosti koje je proveo EY 2018./2019. godine navodi kako 34% organizacija vide nepažljive/neosviještene zaposlenike kao najveću ranjivost [121] koji ujedno predstavljaju jedan od aktera prijetnji od kojeg se najteže obraniti [122].

Prema izvješću EU Agencije za kibernetičku sigurnost (ENISA) za 2019. godinu, u zadnje tri godine prvo mjesto, kao glavna prijetnja, drži zlonamjerni softver [123]. Istraživanje koje su proveli IBM Security i Ponemon Institute [117] navodi kako je od 2014. godine udio sigurnosnih proboja uzrokovanih zlonamjernim napadima porastao za 21%, rastući s 42% proboja u 2014. godini na 51% proboja u 2019. godini. Iako su zlonamjerni proboji najčešći, nenamjerni proboji zbog ljudskih pogrešaka i propusta na sustavu i dalje su osnovni uzrok gotovo polovice (49%) proboja podataka analiziranih u izvješću. 51% incidenata uključivalo je zlonamjerni ili kriminalni napad, 25% uključivalo je probleme u sustavu, uključujući IT i poslovne procese, a 24% je bilo zbog ljudske greške uslijed nepažnje [117].

Suprotno općenitom shvaćanju da su organizacije uglavnom osjetljive na vanjske prijetnje, većinu slučajeva sigurnosnih proboja zapravo čine zaposlenici [124], [75], [41] jer su oni agenti prijetnji koji su najbliži informacijama [28] te kao takvi čine unutarnje prijetnje (engl. *Insider Threats*) informacijskoj sigurnosti organizacije.

Dakle, unutarnje prijetnje proizlaze od bilo kojeg zaposlenika organizacije, neovisno o radnom mjestu i statusu, koji koristi ranjivosti u sustavima, procesima i aplikacijama i to, ili radi osobne koristi putem raznih oblika prijevara, krađa informacija i druge imovine ili uključivanjem u nepromišljeno ponašanje (ako nije namjera nanijeti štetu), zlonamjernu štetu i/ili sabotažu (ako se namjerava nanijeti štetu) na korporativnoj, operativnoj ili IT razini [125].

Svaka osoba u organizaciji, od predsjednika Uprave, preko voditelja IT odjela do zaštitara ili čistačice, potencijalni je kandidat za unutarnju prijetnju ako ima motivaciju iskoristiti prednost bivanja dijelom organizacije i radom unutar nje. Zavist, ljutnja ili nezadovoljstvo nepravednim postupanjem može biti motiv zaposleniku za sabotažu IT sustava, uništavanje informacijske imovine organizacije, blaćenje organizacije ili šefa, krađu iz organizacije ili poduzimanje drugih radnji kako bi se nadoknadilo njihovo nezadovoljstvo [125].

Pace [126] ističe kako je ključna stavka u borbi protiv realizacije unutarnje prijetnje nezadovoljnog zaposlenika bliska suradnja između dva ključna odjela za ovo pitanje – odjela za ljudske resurse i IT odjela. Naime, da bi nezadovoljni zaposlenik mogao izvršiti kibernetički napad na svoju organizaciju, on mora imati tri stvari - sredstva, motiv i priliku. Bavljenje aspektom *motiva* čvrsto pripada odjelu za ljudske resurse koje treba bolje razumjeti zašto ljudi čine ove zločine i paziti na ponašanja koja bi ih mogla pokrenuti. S druge strane, sredstva i prilike potpuno pripadaju IT odjelu koji će trebati uspostaviti snažniji sustav upravljanja pristupom koji ljudima onemogućuje odlazak tamo gdje im nije dopušteno ići i isključuje ih iz sustava kad napuste organizaciju. Zadaća IT odjela je uspostaviti odgovarajuće sigurnosne kontrole, a posao odjela za ljudske resurse uvesti odgovarajuće procese i postupke i stvoriti pravu kulturu u pogledu sigurnosne usklađenosti zaposlenika [126] budući da samo značajne promjene u kulturi informacijske sigurnosti mogu umanjiti broj doživljenih kršenja sigurnosti [127].

3.4.5. Zlonamjerni softver

Zlonamjerni softver (engl. *Malware*) predstavlja softver koji ulazi u računalni sustav bez vlasnikova znanja ili pristanka i uključuje širok izbor štetnog ili neugodnog softvera. Osnovni ciljevi zlonamjernog softvera uključuju zarazu računala i skrivanje prisutnosti zlonamjernog softvera [84].

U globalnom istraživanju o informacijskoj sigurnosti iz 2019. godine koju je proveo EY [121], zlonamjerni softver predstavlja drugu po redu najveću sigurnosnu prijetnju organizacijama dok ga ENISA već treću godinu zaredom svrstava na prvo mjesto

3.4.5.1. Neželjena pošta (engl. Spam)

Neželjena pošta (engl. *Spam*) je zloupotreba sustava elektroničkih poruka za neselektivno slanje neželjenih skupnih poruka, od kojih mnoge sadrže podvale ili drugi nepoželjni sadržaj, poput poveznica do web stranica kojima je cilj krađa osobnih i povjerljivih informacija (Vacca, 2017). Napadači obično šalju ogroman broj poruka koristeći softver koji automatski stvara račune koji će se koristiti za slanje neželjene pošte. Općenito, *spam* je ozbiljan problem i ne postoje učinkovite protumjere za zaštitu od neželjene pošte [83].

Campbell [25] naglašava kako neželjena pošta predstavlja brojne prijetnje iz različitih perspektiva. Prvenstveno, ona zakrčuje informacijske sustave neželjenim porukama, što troši propusnost i resurse sustava s čime se današnji sustavi mogu nositi. Međutim, prava šteta dolazi

od sadržaja poruke budući da većina neželjenih poruka pokušava navesti primatelja da klikne na poveznicu ili otvori privitak koji ima zlonamjerni sadržaj što čini neželjenu poštu medijem za zarazu od bilo koje druge vrste zlonamjernog softvera [25].

3.4.5.2. Špijunski softver (engl. Spyware)

Špijunski softver (engl. *Spyware*) je opći pojam koji se koristi za opisivanje softvera koji narušava privatnost korisnika [84], odnosno svaku tehnologiju koja pomaže u prikupljanju podataka o ljudima ili organizacijama bez njihovog znanja [28].

Špijunski softver implementiran je na način koji narušava korisnikovu kontrolu nad upotrebom resursa sustava, uključujući programe koji su instalirani na korisničkom računalu, zatim prikupljanjem, korištenjem i distribucijom osobnih ili na drugi način osjetljivih podataka te u konačnici, materijalnim promjenama koje utječu na korisničko iskustvo, privatnost ili sigurnost sustava [84].

Općenito, špijunski softver nije dizajniran da našteti korisničkom računalu već mu je svrha pratiti navike pretraživanja, prikupljati osobne podatke, instalirati softver, preusmjeravati web preglednik, mijenjati postavke uređaja, usporavati uređaj i prikazivati skočne oglase [83]. Špijunski softver ponekad dolazi iz zlonamjernih izvora tako da zarazi uređaje obmanjujući korisnike, na primjer, klikom na poveznicu ili gumb na skočnom prozoru [83], a ponekad se isporučuje kao skrivena komponenta besplatnih (engl. *Freeware*) ili djelomično besplatnih (engl. *Shareware*) programa koje korisnici preuzimaju s Interneta ili izravnom razmjenom datoteka [39].

Jedan oblik špijunskog softvera koristi se za praćenje web stranica koje posjećuju kupci na Internetu kako bi se internetska reklama mogla prilagoditi njihovim navikama surfanja. Drugi oblik je analogan prisluškivanju, samo što je ciljni uređaj računalo. Softver bilježi aktivnosti korisnika, uključujući unesene lozinke i pritiske tipki, e-poštu, razgovore u chatu, instant messenger, sva posjećena web mjesta i snimke zaslona računala [128].

3.4.5.3. Oglašivački softver (engl. Adware)

Oglašivački softver (engl. *Adware*) sličan je špijunskom softveru, ali ne prenosi osobne podatke [39] već u svrhu zarade prikazuje neželjene oglase koji smetaju korisnicima i čine ih nezadovoljnima dok surfaju Internetom [83].

Ovaj zlonamjerni softver namijenjen pružanju neželjenog marketinga i oglašavanja uključuje skočne prozore i bannere na korisnikovom ekranu [28], utječe na produktivnost i može se kombinirati s aktivnim pozadinskim aktivnostima, kao što je kôd za otmicu početnih web stranica te prikuplja i prati informacije o aplikaciji, web stranici i internetskim aktivnostima [39].

3.4.5.4. Ucjenjivački softver (engl. Ransomware)

Ucjenjivački softver (engl. *Ransomware*) je vrsta zlonamjernog softvera koji je posebno dizajniran za prepoznavanje i enkripciju vrijednih podataka u sustavu žrtve kako bi se iznudilo plaćanje za ključ potreban za dekripciju podataka [28] uz prijetnju da će u suprotnom izbrisati ili javno objaviti podatke [83].

Ucjenjivački softver, iako iznimno popularan od strane napadača u zadnjih nekoliko godina, nije novost. Prvi ucjenjivački softver u povijesti pojavio se 1989. godine, a zvao se AIDS Trojan (bio je poznat i pod nazivom PC Cyborg virus). Razvio ga je Joseph Popp koji je softver proširio putem 20.000 zaraženih disketa koje je poslao sudionicima konferencije o AIDS-u koju je organizirala Svjetska zdravstvena organizacija (WHO). Disketa je sadržavala interaktivni upitnik koji je poslužio za pokretanje zlonamjernog kôda za kriptiranje korisničkih podataka nakon otprilike 90 ponovnih pokretanja zaraženog računala, nakon čega bi se pojavila poruka u kojoj se tražilo slanje otkupnine u iznosu od 189 dolara na poštanski pretinac u Panami. Nije prošlo dugo nakon čega su razvijeni alati za dešifriranje korisničkih podataka [129].

Ucjenjivački softver se najčešće instalira nakon što korisnik otvori zlonamjerni privitak e-pošte ili klikne na poveznicu do zlonamjerne web stranice koja se nalazi u e-pošti čiji je cilj krađa identiteta. Jednom kada se zlonamjerni kôd izvrši na korisnikovom računalu, putem Interneta javlja se napadaču s osobnim podacima koji se odnose na uređaj korisnika koji je možda poslan s njegove IP adrese, korisničkog imena ili drugih korisničkih podataka kako bi stvorio poseban ključ za šifriranje koji je svojstven tom sustavu. Tip enkripcije koji koristi moderni ucjenjivački softver zasnovan je na jakom javnom ključu, što znači da ne postoji poznata metoda njegovog vraćanja, a budući da su ključevi posebno izrađeni po mjeri za svako zaraženo računalo, ne postoji način da se probije kôd ili grubom silom razbije enkripcija pa je jedini način izlaska iz ove situacije ili oporavak podataka iz sigurnosne kopije (ako imate sreće pa ju imate) ili plaćanje otkupnine [25].

3.4.5.5. Virusi (engl. Viruses)

Virus (engl. *Virus*) je vrsta zlonamjernog softvera koji se priključuje ili kopira na ostale izvršne programe [39], a kad se aktivira, reproducira se i širi u ostale sustave pomoću više komunikacijskih načina (npr. virus može poslati svoje kopije svim kontaktima iz aplikacije za slanje e-pošte zaraženog računala) [28].

Računalni virus djeluje na sličan način kao i biološki virus što znači da bi preživio, potreban mu je prenositelj odnosno „domaćin" koji u slučaju računalnog virusa predstavlja neka programska datoteka ili dokument [39]. Virus se potajno veže za jednog od tih legitimnih prenositelja i zatim izvršava svoj zlonamjerni kôd kad se otvori taj dokument ili pokrene programska datoteka [84] dok se replicira i unutar domaćina i u druge domaćine na različite načine [25]. Ti prijenosnici su obično originalne datoteke poput sistemskih datoteka [35].

Pored kôda kojim se pomaže u širenju na druge objekte, virus često ima kôd za obavljanje drugih funkcija čime mogu uzrokovati mnogo različitih gubitaka, uključujući, ali ne ograničavajući se na gubitak osjetljivih informacija i upropaštavanje računalnih resursa [83]. Na primjer, virus može izbrisati ili prepisati datoteke, prikazati podatke na zaslonu računala, uzrokovati da se računalo više puta ruši, napraviti višestruke kopije i potrošiti sav slobodni prostor na tvrdom disku, formatirati tvrdi disk, smanjiti sigurnosne postavke i dopustiti uljezima udaljeni pristup računalu ili pokušati komunicirati s drugim računalima putem bilo kojeg aktivnog mrežnog sučelja [84].

Virus obično ima ograničen skup funkcija i njegov kreator nema daljnje interakcije s njim jednom kad se pusti [23]. Prvi zabilježeni virus bio je virus *Creeper*, kojeg je napisao istraživač Bob Thomas 1971. godine. *Creeper* se kopirao na druga umrežena računala prikazujući poruku "Ja sam gmizavac [creeper], uhvati me ako možeš!" [39].

3.4.5.6. Crvi (engl. Worms)

Crv (engl. *Worm*) je vrsta zlonamjernog softvera koji se samostalno umnožava i širi mrežnim konekcijama, e-porukama, zaraženim web stranicama i instant porukama obično bez ljudske interakcije. Većina crva iskorištava poznatu ranjivost u sustavima i kompromitira one koji nisu pravilno zakrpani [23].

Iako se često miješaju s virusima, crvi su različiti. Za razliku od virusa koji se mora priključiti na programsku datoteku ili dokument i širiti se putujući pomoću prenositelja, crv može putovati

samostalno [28]. Druga je razlika u tome što virus treba od korisnika izvršenje određene akcije poput pokretanja programske datoteke ili otvaranja privitka e-pošte za pokretanje zaraze, dok crv ne zahtijeva nikakvu korisničku radnju da bi započeo svoje izvršavanje [84]. Što se tiče štete, oba mogu stvoriti havariju. Neki od popularnih crva su: Melissa, ILOVEYOU ili Stuxnet [35].

Prvi crv za koji je prijavljeno širenje „u divljini" bio je crv Morris kojeg je napisao Robert Tappan Morris 1988. godine, a koji je napao ranjivost prepisivanja spremnika (engl. *Buffer overflow*) [39].

3.4.5.7. Trojanski konji (engl. Trojan Horses; Trojans)

Trojanski konj ili kraće **trojanac** (engl. *Trojan Horse* or *Trojan*) je zlonamjerni program koji se maskira kao legitimni, koristan program koji u međuvremenu obavlja zlonamjerne funkcije u pozadini [23], a ime je dobio po drvenom trojanskom konju u čuvenoj bitci između Grka i njihovog napada na grad Troju [25].

Trojanski konj, poput računalnog virusa, ne može se širiti ako se ne aktivira, što znači da se oslanja na čovjeka da ga aktivira, obično putem trika gdje se korisniku najčešće nudi neki računalni program za određenu svrhu, a zapravo, kad korisnik pokrene program, trojanski konj izvršava zlonamjernu svrhu za koju je osmišljen (ili može obavljati i oglašavane i zlonamjerne aktivnosti). Na primjer, korisnik može preuzeti ono što se oglašava kao besplatan kalendar, ali kada se pokrene, uz instaliranje kalendara, on pretražuje sustav za brojevima kreditnih kartica i lozinkama, povezuje se putem mreže s udaljenim sustavom, a zatim prenosi te informacije [84].

Iako se, za razliku od virusa i crva, Trojanci ne razmnožavaju inficiranjem drugih datoteka, već umjesto toga, rade i izvršavaju se neovisno na korisnikovom računalu [25], mogu poslužiti kao vrata za drugu samoumnožavajuće zlonamjerne aplikacije radi zaraze žrtvinog uređaja izvođenjem zlonamjernih radnji poput otvaranja sigurnosne rupe u uređaju žrtve [83].

Prvi poznati računalni trojanski konj bio je *Animal*, objavljen 1974. godine. *Animal* se prerušio u jednostavnu kviz igru u kojoj će korisnik misliti na životinju, a program će postavljati pitanja kako bi pokušao pogoditi životinju. Međutim, uz postavljanje pitanja, program se kopirao u svaku mapu kojoj je korisnik imao pravo pisanja [39]. Neki primjeri popularnih Trojana su *Flame*, *Banker*, *Zeus* ili *Beast* [35].

3.4.5.8. Stražnji ulaz (engl. Backdoor)

Stražnji ulaz (engl. *Backdoor*) je zlonamjerni softver koji zaobilazi standardne sigurnosne kontrole kako bi poskrivećki omogućio pristup napadaču. Stražnji ulazi rijetko imaju mogućnost samoumnožavanja, a napadač ih ručno instalira nakon što kompromitira sustav kako bi olakšao budući pristup ili putem drugih samostalno širećih zlonamjernih softvera. [23]

Stražnji ulaz i trojanski konj imaju nekoliko zajedničkih stvari. Oba dolaze s dva dijela softvera, klijentskim i poslužiteljskim. Poslužiteljski dio je dio koji će 'udaljeni administrator' (zapravo napadač) upotrijebiti za zarazu žrtvinog računala, a klijentski dio koji će napadač koristiti za nadgledanje računala žrtve. Oba programa omogućuju potpuni pristup žrtvinim datotekama što znači da napadač može kopirati, premjestiti, preimenovati, izbrisati pa čak i promijeniti bilo koju datoteku ili mapu na žrtvinom računalu [23].

3.4.5.9. Logičke bombe (engl. Logic Bombs)

Logička bomba (engl. *Logic Bomb*) je računalni program ili dio programa koji izvršava neku zlonamjernu funkciju kad otkrije određene uvjete [39] odnosno nalazi se u stanju mirovanja dok ga ne pokrene određeni logički događaj, poput određenog datuma u kalendaru sustava ili ranga osobe u organizaciji koja je iz nekog razloga degradirana [84].

Logičke bombe u mnogočemu su slične stražnjim ulazima (engl. *Backdoors*). Kao kategorija zlonamjernog softvera, glavni atribut koji razlikuje logičku bombu od bilo koje druge vrste jest taj što logička bomba miruje na računalnom sustavu dok se ne ispuni određeni uvjet gdje, nakon što se taj uvjet ispuni, zlonamjerni softver ponovno oživljava obavljajući sve zlonamjerne aktivnosti koje je njegov autor namjeravao [25]. Te zlonamjerne aktivnosti mogu uzrokovati trenutnu štetu ili pokrenuti niz događaja koji uzrokuju štetu tijekom dužeg razdoblja [39].

Mnoge logičke bombe potječu od samih zaposlenika unutar organizacije [39] pa tako npr. logička bomba može biti postavljena od strane zaposlenika u sustav za obračun plaća gdje bi program mogao biti osmišljen tako da će, ukoliko se ime zaposlenika ukloni s platne liste (što znači da je dao otkaz ili je otpušten), nakon tri mjeseca logička bomba oštetiti čitav računovodstveni sustav organizacije [84].

3.4.5.9. Zombiji i mreže botova (engl. Zombies and Botnets)

Izraz „**mreža botova**” (engl. *Botnet*) obično se koristi za skup kompromitiranih računala koji se nazivaju **botovi ili zombiji**, a na kojima se izvodi određeni softver, obično instaliran putem

crva ili trojanskih konja [23] koji će omogućiti da se zaraženo računalo stavi pod udaljenu kontrolu napadača [84]. Nakon što je računalo zaraženo, ono se pridružilo određenom IRC (engl. *Internet Relay Chat*) kanalu na IRC poslužitelju i čeka upute, omogućujući napadaču udaljenu kontrolu zombi računala. Jednom kada su pod nadzorom glavnog računala koje upravlja ostalima, botneti se mogu koristiti u različite zlonamjerne svrhe, kao na primjer širenje zlonamjernog softvera i širenje mreže botova, manipulaciju online anketa ili napade uskraćivanjem usluge [84].

3.4.5.10. Alati za prikrivanje prisutnosti napadača (engl. Rootkit)

Alat za prikrivanje prisutnosti napadača (engl. *Rootkit*) je zlonamjerna skrivena aplikacija koja je osmišljena za pružanje neovlaštenog pristupa uređajima ili drugoj aplikaciji [83] odnosno skup softverskih alata koje napadač koristi da bi provalio u računalo, stekao posebne privilegije za obavljanje neovlaštenih funkcija, a zatim sakrio sve tragove svog postojanja [84].

Rootkit se sastoji od riječi *root* (hrv. *korijen*) koji predstavlja administratorski račun na Unix/Linux operacijskim sustavima i *kit* (hrv. *oprema*) koji se odnosi na implementaciju samog alata [83]. U skoro svim slučajevima, cilj *rootkita* nije izravno oštetiti računalo kao što to čini virus već je, umjesto toga, njegova funkcija skrivanje prisutnosti drugih vrsta zlonamjernog softvera, poput trojanskih konja, virusa ili crva [84] na način da mijenja ili zamjenjuje jedan ili više postojećih programa kako bi sakrio tragove napada [39].

Iako *rootkiti* obično mijenjaju dijelove operacijskog sustava kako bi sakrili tragove svoje prisutnosti, oni mogu postojati na bilo kojoj razini - od uputa za pokretanje računala do aplikacija koje se izvode u operacijskom sustavu. Jednom instalirani, *rootkiti* pružaju napadačima lak pristup kompromitiranim računalima za pokretanje dodatnih napada [39], a dodatna otežavajuća okolnost je da je *rootkite* vrlo teško otkriti, a još teže ukloniti [25]. Naime, budući da *rootkiti* koriste tehnike skrivanja, mogu se izvoditi kao proces u sustavu, ali se ne pojavljuju u upravitelju zadataka na Windows računalu. Također, ako se pogleda datotečni sustav, *rootkit* kôd je skriven jer se može zaštititi korištenjem pristupnih kontrolnih listi tako da korisnici do njega zapravo i ne mogu doći [25].

3.4.6. Socijalni inženjering i s njim povezani napadi

Socijalni inženjering (engl. *Social Engeneering*) je svaki čin u kojem napadači pokušavaju korisnika navesti da izvrši neku radnju, stavljajući tako ljudski element u petlju sigurnosnog proboja i koristeći čovjeka kao oružje [39]. To je zapravo proces korištenja društvenih vještina

kojom jedna osoba uvjerava drugu da joj da informacije koje želi [86] odnosno umjetnost manipuliranja ljudima u izvođenju radnji ili razotkrivanju informacija [23] kao što su pristupne vjerodajnice ili druge vrijedne informacije [28].

Budući da je socijalni inženjering napad na/kroz ljudsku prirodu, napadači iskorištavaju neke od karakteristika ljudskog ponašanja, kao što su spremnost za pomoći, spremnost za povjerovati, poštivanje autoriteta ili strah da bi prikupili informacije koje kasnije mogu koristiti za pokretanje napada [35]. Naime, ljudska bića su po prirodi korisna i žele pomoći ljudima u nevolji ili u teškim situacijama te instinktivno vjeruju drugima. Također, ljudska bića sklona su poštivanju naredbi svojih nadređenih ili osoba s autoritetom u svojoj organizaciji te se po prirodi plaše posljedica nepridržavanja pravila organizacije, posebno gubitka posla [35].

Pomoću tehnika socijalnog inženjeringa napadač će najvjerojatnije odabrati metu koju može prevariti odnosno za koju vjeruje da je ranjiva na prijedloge, što će se često naći u niže plaćenim redovima organizacije. Iz tog razloga, organizacije bi trebale poticati kulturu informacijske sigurnosti u cijelom poslovanju kako bi se osiguralo da svi zaposlenici u svakom trenutku imaju sigurnost u vidu te, kad vide nešto što izgleda ili se čini pogrešnim ili naiđu na neko neobično ili sumnjivo ponašanje, umjesto da slijede prirodne ljudske osobine ignoriranja, treba ih ohrabriti da to ispitaju i prijave. Na svim razinama, zaposlenike treba podsjećati da je u redu reći 'ne' ili pitati nadređenog radije nego riskirati kršenje sigurnosti [25].

Socijalni se inženjering može odvijati osobno (napadač koji se pretvara da je dostavljač paketa), telefonom (osoba koja se pretvara da je zaposlenik Odjela za IT ili korisnik koji treba pomoć) i putem interneta (putem nekog oblika krađe identiteta). Za napad se obično koriste sljedeće metode: napad s ciljem krađe identiteta (engl. *Phishing*), priprema uvjerljive lažne priče (engl. *Pretexing*), namamljivanje (engl. *Baiting*), praćenje u stopu (engl. *Tailgating*), virenje preko ramena (engl. *Shoulder surfing*) ili kopanje po smeću (engl. *Dumpster diving*) [35].

3.4.6.1. Napad s ciljem krađe identiteta (engl. Phishing)

Napad s ciljem krađe identiteta (engl. *Phishing*) je oblik socijalnog inženjeringa u kojem napadač prikazuje ono što se čini legitimnom komunikacijom (najčešće e-poštom), ali sadrži skriveni ili ugrađeni kôd koji odgovor preusmjerava na web stranicu treće strane u pokušaju da izvuče osobne ili povjerljive informacije [28] poput lozinki, brojeva kreditnih kartica i računa [86] koje će napadač iskoristiti za krađu identiteta [35].

Prema globalnom istraživanju o informacijskoj sigurnosti koje je proveo EY [121], najveća prijetnja organizacijama predstavlja napad s ciljem krađe identiteta (engl. *Phishing*), što ne treba čuditi budući da je napad s ciljem krađe identiteta toliko snažno iskorišten da više od 90% zaraza zlonamjernim softverom i 72% sigurnosnih proboja podataka u organizacijama potječu od njega [123].

Ova vrsta napada, koja ne zahtijeva nikakve tehničke sposobnosti i nerijetko je uspješna [84], obično se koristi za početak sigurnosnog proboja gdje napadači šalju na desetke tisuća poruka e-pošte kako bi pokušali namamiti nekoliko neopreznih korisnika da kliknu na poveznicu za preuzimanje nekog zlonamjernog softvera ili otvaranje zlonamjernog privitka [25] ili poveznice koja vodi na lažnu stranicu koja zahtijeva vjerodajnice za prijavu. Ako korisnik dostavi te vjerodajnice, napadač korisnikove vjerodajnice može upotrijebiti za pristup stvarnoj stranici.

Napad s ciljem krađe identiteta ima dvije podvrste, a to su usmjereni napad s ciljem krađe identiteta (engl. *Spear Phishing*) i glasovni napad s ciljem krađe identiteta (engl. *Vishing*).

Dok uobičajeni napadi s ciljem krađe identiteta ciljaju što veći broj primatelja, **usmjereni napad s ciljem krađe identitet**a (engl. *Spear phishing*) šalje poruku maloj grupi ljudi ili čak jednoj osobi gdje se čini da je poruka od poslodavca, kolege ili drugog legitimnog pošiljatelja [28] budući da napadač koristi stvarna imena i informacije prikupljene s društvenih mreža ili drugih skladišta otvorenog kôda kako bi pokušaj krađe identiteta bio vjerodostojniji [25]. Ako je osoba na koju se odnosi usmjereni napad s ciljem krađe identiteta na rukovodećem položaju, kao što su izvršni direktor, glavni izvršni direktor i svatko s financijskom odgovornošću koji ima mogućnost odobravanja plaćanja velikih računa [25], takav napad naziva se i **pecanje velike ribe** (engl. *Whaling*) [39].

Glasovni napad s ciljem krađe identiteta (engl. *Vishing – Voice phishing*) predstavlja izvođenje napada s ciljem krađe identiteta telefonskim putem radi dobivanja osobnih podataka koristeći verbalnu prisilu i uvjeravanje žrtve odnosno slatkorječivost napadača [39]. Kod ovakve vrste napada, obično se upućuje poziv na žrtvin telefon umjesto da se e-mailom pošalje poveznica te joj se ostavlja poruka da nazove određeni broj gdje se čini da su ovi pozivi stigli od legitimnih organizacija poput banaka ili financijskih institucija. Ti se pozivi obično pokreću automatiziranim sredstvima gdje će žrtva, kad nazove broj naveden u snimljenoj poruci, biti preusmjerena na sustav za glasovni odgovor koji će ju dalje navoditi na odavanje informacija kao u slučaju uobičajenih napada s ciljem krađe podataka budući da je i namjera napadača ista

kao i kod uobičajenih napada, a to je krađa identiteta i korištenje prikupljenih podataka za daljnje napade [35].

3.4.6.2. Priprema uvjerljive lažne priče (engl. Pretexing)

Priprema uvjerljive lažne priče (engl. *Pretexing*) potječe od engleske riječi koja znači *izlika* ili *izgovor*, a uključuje upotrebu pametno osmišljenih dobro izrađenih laži s lošom namjerom prikupljanja podataka o pojedincu ili organizaciji za pokretanje napada. Takvi napadi temelje se na informacijama koje su napadaču već dostupne ili na višestrukim, postupnim napadima koji traju dok se ne postigne planirani cilj [35].

3.4.6.3. Namamljivanje (engl. Baiting)

Namamljivanje (engl. *Baiting*) je vrsta napada gdje se umjesto e-pošte koriste fizički pogoni poput CD-a, DVD-a ili USB pogona koji na sebi sadrže zlonamjerni softver. Namjera napada je zlonamjerno zaraziti računala koja ih koriste, a zatim i mrežu, pružajući napadaču pristup svim informacijama na računalu i mreži [35].

3.4.6.4. Praćenje u stopu (engl. Tailgating) ili šlepanje (engl. Piggybacking)

Praćenje u stopu (engl. *Tailgating*), ponekad poznato i kao **šlepanje** (engl. *Piggybacking*), predstavlja postupak dobivanja neovlaštenog ulaska u objekt pomnim praćenjem druge osobe kroz ulaz i korištenjem vjerodajnica ovlaštene osobe za zaobilaženje kontrolne točke [28] što znači da napadač slijedi legitimnog korisnika kroz provjerene autenticirane ulaze poput onih kojima je pristup dopušten pristupnim karticama ili otiscima prstiju [35].

3.4.6.5. Virenje preko ramena (engl. Shoulder surfing)

Virenje preko ramena (engl. *Shoulder surfing*) je izravno, prikriveno promatranje pojedinačnih informacija ili korištenja sustava [28] odnosno čin gledanja osobe koja tipka na tipkovnici računala radi otkrivanja i krađe lozinke ili drugih korisničkih podataka [128] budući da se informacije poput lozinki i PIN-ova lako ugrožavaju, kao i povjerljivi obrasci koji mogu biti otvoreni na korisničkom zaslonu dok osoba prima telefonski poziv [25].

3.4.6.6. Kopanje po smeću (engl. Dumpster diving)

Kopanje po smeću (engl. *Dumpster diving*) predstavlja informacijski napad koji uključuje pretraživanje kontejnera sa smećem ciljane organizacije i recikliranje osjetljivih podataka [28] ili privatnih podataka za krađu identiteta pronađenih na neuništenim komadima papira [39].

Pronađene informacije koje su odbačene od strane organizacije ili same po sebi imaju vrijednost ili predstavljaju alat za napad u socijalnom inženjeringu, poput internih brojeva telefona ili naziva radnih mjesta [128].

3.5. Elementi upravljanja informacijskom sigurnošću

Od trenutka kad je informacijska sigurnost prepoznata kao poslovno, a ne isključivo tehničko pitanje, uloga rukovodstva u informacijskoj sigurnosti postaje sve važnija i privlači pozornost istraživača [2], budući da, bez razumijevanja koji elementi čine upravljanje informacijskom sigurnošću uspješnim, organizacijama je teško precizno i dosljedno navesti prednosti koje pruža upravljanje informacijskom sigurnošću, kao ni osigurati optimalno korištenje, ionako ograničenih, resursa [130].

Tako literatura navodi podršku rukovodstva kao jednim od elemenata o kojem može značajno ovisiti uspjeh ili neuspjeh upravljanja informacijskom sigurnošću u organizaciji [2], [20], [30], [55], [79], [131]. Nadalje, ključnu ulogu u upravljanju informacijskom sigurnošću ima i razvoj i implementacija učinkovite politike informacijske sigurnosti [2], [20], [132], [30], [55], [130], [131], kao i integracija tehničkih i upravljačkih aktivnosti za uspješnu politiku informacijske sigurnosti [2].

Drugi upravljački aspekti o kojima se raspravlja u literaturi su ljudski čimbenik, svijest o informacijskoj sigurnosti, edukacija i obuka o usklađenosti [2], [20], [30], [55], [132] gdje, uz sve navedeno i organizacijska struktura predstavlja važan element u upravljanju informacijskom sigurnošću [83].

3.5.1. Podrška rukovodstva

Upravljanje informacijskom sigurnošću najbolje je započeti odozgo prema dolje, gdje uprava i više rukovodstvo predstavljaju ključnu komponentu za uspješnu provedbu inicijativa vezanih uz informacijsku sigurnost [28], [115], [133]. Bez podrške rukovodstva bilo kakve inicijative vjerojatno će doživjeti neuspjeh, a ta podrška bit će uskraćena ako rukovodstvo ne vidi važnost informacijske sigurnosti odnosno činjenicu da ona podržava ključne poslovne aktivnosti organizacije [20].

Barton i suradnici [94] istraživali su motiviranost rukovodstva za pružanje podrške sigurnosti, podijelivši podršku rukovodstva na dva konstrukta – uvjerenja rukovodstva i sudjelovanje rukovodstva. Rezultati su pokazali da uvjerenja rukovodstva u informacijsku sigurnost dovodi

do veće asimilacije sigurnosti u organizacijama povećanjem sudjelovanja rukovodstva u upravljanju informacijskom sigurnošću, podržavajući dugotrajan argument da je podrška rukovodstva ključna za uspješnu sigurnost [94].

Rukovodstvo može podržati informacijsku sigurnost kao važnu funkciju na razini cijele organizacije na mnoge načine [105], [5] uključujući ljudske i materijalne resurse potrebne za implementaciju pojedinih sigurnosnih kontrola [29], [10], aktivno sudjelovanje u razvoju politike informacijske sigurnosti putem definiranja svojih očekivanja od zaposlenika [134], [135], poticanje održavanja sigurnosnih edukacija, obuka i radionica podizanja svijesti [124], [136], [87] te promociju prihvaćanja i naglašavanja važnosti sigurnosti ostalim zaposlenicima unutar organizacije [136], [97], [137]. Ukratko, rukovodstvo mora aktivno podupirati sigurnosne napore na svim razinama [87].

Empirijski je utvrđeno da što je veća podrška rukovodstva, to je učinkovitija informacijska sigurnost u organizacijama, jer se više sredstava troši kako bi se izbjegli sigurnosni incidenti [87], a organizacije s jačom podrškom rukovodstva sklonije su primjeni preventivnih mjera zaštite nego organizacije sa slabijom podrškom rukovodstva [134]. Primjer organizacija sa slabijom podrškom, u smislu vremena i novca, su australska mala i srednja poduzeća, koja, uslijed nedovoljne podrške vlasnika tih poduzeća zbog nedovoljne svijesti o njenoj važnosti [138], zauzimaju reaktivan, a ne proaktivan stav prema informacijskoj sigurnosti [139].

Da bi proces upravljanja informacijskom sigurnošću uspio, a sigurnosne politike imale smisla [140], rukovodstvo mora učiniti više od pukog odobrenja sigurnosne politike ili radionica podizanja svijesti što znači da mora osobnim primjerom pokazati posvećenost informacijskoj sigurnosti [128] na način da neće smatrati kako su oni iznad odredbi sigurnosne politike i kako se te odredbe ne odnose na njih [137].

Jednom kad se osigura podrška i predanost na razini rukovodstva, lakše je osigurati predanost ostalih zaposlenika [29], [141]. Bez podrške i uključenosti višeg rukovodstva, stvaranje, osposobljavanje i provođenje sigurnosnih politika organizacije u pravilu se ne shvaća ozbiljno [37], [98], a ako rukovodstvo rijetko ili nikada vrednuje usklađenost, zaposlenici najvjerojatnije neće poštivati te politike [137].

3.5.2. Organizacija informacijske sigurnosti

Ključna odluka u organiziranju informacijske sigurnosti je gdje smjestiti funkciju informacijske sigurnosti unutar organizacije [28], za što ne postoji ispravan ili pogrešan odgovor. Međutim, ono što je važno jest osigurati da netko bude ovlašten za donošenje sigurnosnih odluka i odgovornost za njihovo izvršavanje [25]. Dodjeljivanje funkcija pojedincima u velikoj mjeri ovisi o veličini organizacije, njenim specifičnostima i povezanim rizicima [57] pa tako u malim i srednjim poduzećima nedostaje osoba dedicirana za nadzor i upravljanje informacijskom sigurnošću [24] dok velike organizacije, pogotovo iz financijskog sektora [25], u pravilu imaju imenovanog voditelja informacijske sigurnosti (engl. *Chief Information Security Officer – CISO*) ili srodnu funkciju ili čak cijeli odjel zadužen za informacijsku sigurnost.

Postoji nekoliko valjanih izbora za pozicioniranje funkcije informacijske sigurnosti unutar organizacije, a tradicionalno najčešća opcija uključuje postavljanje informacijske sigurnosti unutar IT-a ili funkcije fizičke sigurnosti (ako postoji), međutim organizacije koje tragaju za racionalnim kompromisom trebale bi postaviti funkciju informacijske sigurnosti tamo gdje ona može uravnotežiti potrebu za provođenjem sigurnosne politike organizacije i potrebe pružanja kvalitetne usluge cijeloj organizaciji [28]. To znači da se voditelj informacijske sigurnosti može nalaziti unutar ili izvan IT odjela i može, ali ne mora voditi tim sigurnosnih stručnjaka s odgovornošću za neke ili sve sigurnosne funkcije [57].

U slučaju da je funkcija informacijske sigurnosti smještena unutar odjela za IT, voditelj informacijske sigurnosti izvještava voditelja IT-a (engl. *Chief Information Officer – CIO*) ili osobu zaduženu za informacijsku sigurnost na razini uprave (ako postoji) gdje takva struktura podrazumijeva da su ciljevi voditelja informacijske sigurnosti i voditelja IT-a usklađeni što nije uvijek slučaj [28]. Po svojoj prirodi upravljanje informacijskom sigurnošću ponekad može biti u suprotnosti s ciljevima i zadacima odjela za IT u cjelini, budući da voditelj IT-a, kao izvršni direktor zadužen za tehnologiju organizacije teži učinkovitosti u dostupnosti, obradi i pristupu informacijama u tvrtki, a sve što ograničava pristup ili usporava obradu informacija može ometati njegove ciljeve [28].

S druge strane, funkcija voditelja informacijske sigurnosti sličnija je funkciji unutarnjeg revizora u tome što voditelj informacijske sigurnosti usmjerava odjel za IT na provjeru podataka u prijenosu i pohrani kako bi otkrio sumnjivi promet i pregledao sustave radi otkrivanja grešaka i sigurnosnih nedostataka u tehnologiji, softveru te aktivnostima i procesima zaposlenika [28]. Time dolazimo do jednog od prije spomenutih izazova upravljanja informacijskom sigurnošću

– sigurnosti naspram funkcionalnosti. Dodatno, ako voditelj informacijske sigurnosti izvještava voditelja IT-a, vjerojatnije je da će voditelj informacijske sigurnosti biti lojalniji i odaniji voditelju IT-a koji kontrolira IT proračun unutar kojeg se nalaze i predviđena sredstva za informacijsku sigurnost, te ujedno biti i manje sklon objavljivanju svih nedostataka u informacijskoj sigurnosti koji bi mogli ugroziti njegov položaj kao voditelja informacijske sigurnosti ili prikazati voditelja IT-a u negativnom svjetlu [142].

Upravo zbog toga što se ciljevi i zadaci voditelja IT-a i voditelja informacijske sigurnosti uglavnom međusobno suprotstavljaju, noviji trend mnogih organizacija je odvajanje funkcije informacijske sigurnosti od IT odjela [28] gdje voditelj informacijske sigurnosti može izravno izvještavati glavnog izvršnog direktora (engl. *Chief Executive Officer – CEO*) s nadležnošću za sve aspekte sigurnosti (ljude, procese i tehnologiju) [25]. Na ovaj način, voditelj informacijske sigurnosti djeluje kao agent glavnog izvršnog direktora upravljajući sigurnošću informacijskih resursa, uspostavljajući strategiju, standarde i politike informacijske sigurnosti, vodeći se zakonodavnom i industrijskom vizijom usklađenosti organizacije, kao i stvaranjem sigurne poslovne vrijednosti utemeljene na IT-u [142].

Iako je primijećen nedostatak konsenzusa o strukturi izvješćivanja voditelja informacijske sigurnosti u dostupnim istraživanjima, postoji trend ka strukturi izvještavanja više razine [142] čemu u prilog govori i globalno istraživanje o informacijskoj sigurnosti koje je 2019. godine proveo Deloitte [112] na uzorku od 500 izvršnih rukovoditelja (engl. *C-level executives*). Rezultati pokazuju kako je 43% ispitanih voditelja informacijske sigurnosti izjavilo kako o stanju informacijske sigurnosti izvještava izravno glavnog izvršnog direktora što je konzistentno s tvrdnjama cjelokupne populacije ispitanika iz istog istraživanja, od kojih se 32% izjasnilo kako u njihovim organizacijama voditelj informacijske sigurnosti odgovara glavnom izvršnom direktoru, a 19% da odgovara voditelju IT-a [112]. Međutim, ono što je indikativno i pokazuje kako, unatoč svim naporima, informacijska/kibernetička sigurnost još uvijek nije u potpunosti prepoznata kao strateško pitanje, je podatak iz najnovijeg globalnog istraživanja informacijske sigurnosti kojeg je proveo EY [143], koji kaže kako šest od deset ispitanih organizacija nema osobu zaduženu za sigurnost na razini uprave ili izvršnog rukovodstva.

3.5.2.1. Uloge i odgovornosti

Ako bi se pitalo zaposlenike, većina bi rekla da su za sigurnost informacija organizacije odgovorni zaposlenici IT-a [113], međutim informacijska sigurnost trebala bi biti odgovornost svih u organizaciji, od uprave i glavnog izvršnog direktora pa sve do niže razine rukovodstva i

samih zaposlenika [125]. Također jedna od najvećih grešaka koju organizacije mogu učiniti je pretpostavka da je sigurnost problem koji može riješiti voditelj IT-a ili voditelj informacijske sigurnosti, koji će kao stručnjak jednostavno znati što treba učiniti, pronaći najjeftiniji način za napraviti to i uvjeriti se da sustavi rade [23].

Na vrhu bi uprava trebala postaviti cjelokupnu politiku i smjer informacijske sigurnosti u organizaciji te osigurati odgovarajuće resurse za provedbu informacijske sigurnosti, nakon čega bi više rukovodstvo trebalo pružiti dodatnu podršku i smjernice za provođenje uputa uprave, a zauzvrat, različite poslovne jedinice trebaju se baviti informacijskom sigurnošću u sklopu svakodnevnih radnih zadataka i aktivnosti [125] što pokazuje kako su odgovornosti različitih područja sigurnosti raširene u cijeloj tvrtki [57]. Tako na primjer, kontrolu i upotrebu informacija u organizaciji obavljaju vlasnici informacija, koji su odgovorni za sigurnost i upotrebu određenog skupa informacija, skrbnici informacija, koji su odgovorni za pohranu, održavanje i zaštitu informacija te korisnici podataka, koji rade s informacijama za obavljanje svojih svakodnevnih poslova i podržavaju misiju organizacije [28].

Drugim riječima, odgovor na pitanje s početka ovog potpoglavlja tko je odgovoran za sigurnost informacija trebao bi biti - svi su odgovorni [29] gdje je bitno naglasiti da, ukoliko se informacijska sigurnost smatra odgovornošću samo IT odjela, zaposlenici mogu previdjeti svoju ulogu u informacijskoj sigurnosti [144]. Kako se ta uloga ne bi previdjela, uloge i odgovornosti svih zaposlenika ili skupina zaposlenika treba dokumentirati u odgovarajućim politikama i procedurama, gdje procesi utvrđeni politikama i procedurama trebaju pokrivati sve što je potrebno za sigurno i pouzdano korištenje, nadzor i održavanje informacijskog sustava i informacija u njemu [10]. Isto tako, pojedinci s dobro definiranim ulogama i odgovornostima proaktivniji su u smislu poduzimanja smjera informacijske sigurnosti, a jasnoća uloga i odgovornosti te prikladnost sankcija naglašene su kao važni čimbenici koji bi mogli utjecati na promjenu namjera zaposlenika po pitanju usklađenosti s politikom informacijske sigurnosti [37].

Više rukovodstvo organizacije ima važnu ulogu u zaštiti informacijske imovine u organizaciji te treba biti svjesno rizika koji prihvaćaju za organizaciju kroz svoje odluke ili svoje ne donošenje odluka [23], a, između ostalog, odgovorno je za nadgledanje, omogućavanje i podržavanje strukturiranja funkcije informatičke tehnologije i informacijske sigurnosti radi zaštite svoje informacijske imovine odnosno informacija i podataka, hardvera, softvera, procedura, mreža i ljudi [28]. Dio njihovih uloga i odgovornosti su i osiguranje dovoljnih

resursa za provođene sigurnosnih edukacija, obuka i radionica podizanja svijesti, kao i uključivanje i poticanje kulture informacijske sigurnosti unutar organizacije, utvrđivanje ispravnih politika upravljanja informacijskom sigurnošću [23] te uspostava i podrška učinkovitog procesa upravljanja rizicima [28].

Voditelj informacijske sigurnosti je funkcija čija se uloga posljednjih godina znatno promijenila, od voditelja tima za dodjelu prava korisnika u IT odjelima s tehničkim profilom u 1990-im godinama do današnjeg vođenja multidisciplinarnih timova zaduženih za osiguranje poslovnih procesa i donošenje dodane vrijednosti [57]. Voditelj informacijske sigurnosti prvenstveno je odgovoran za pripremu, održavanje i komuniciranje politika i procedura informacijske sigurnosti unutar organizacije [29], ali njegove uloge i odgovornosti obuhvaćaju vrlo širok spektar aktivnosti, u rasponu od osiguranja operacija do komunikacije, osiguranja svijesti, upravljanja sigurnosnim rizicima, upravljanja cjelokupnim procesom i izvješćivanjem o stanju sigurnosti [57]. Voditelj informacijske sigurnosti, uz potrebnu stručnost u informacijskoj sigurnosti [145], mora također znati više i o poslovnim funkcijama kao što su računovodstvo, financije, marketing, operacije, ljudski resursi, organizacijsko ponašanje i upravljanje projektima [146], budući da djeluje kao poveznica između svih područja poslovanja u kojima se brine o sigurnosti [25]. Voditelj informacijske sigurnosti trebao bi, s jedne stane, rukovodstvu i upravi pružiti informacije o sigurnosnim razvojima, rizicima i mogućim postupcima djelovanja u skladu s načelima upravljanja rizikom, a s druge strane, zaposlenicima pružiti jasnu, razumljivu i otvorenu komunikaciju, pokazujući da je sigurnost unutar organizacije dio „načina na koji radimo" [145].

IT odjel osigurava funkcionalnost i sigurnost informacijskih sustava te, na temelju svoje ekspertize po pitanju tehnologije i softverskih alata, preporučuje tehničke mjere koje su učinkovite, jednostavne i korisne za podržavanje sigurnog ponašanja bez opterećenja. Jedna od glavnih kompetencija u IT odjelu trebala bi biti i stručnost po pitanju informacijske sigurnosti što može poslužiti kao dobra podloga za procjenu rizika i pomoć višem rukovodstvu u donošenju odluka po pitanju učinkovitih sigurnosnih kontrola [145]

Odjel za ljudske resurse predstavlja sponu između rukovodstva i zaposlenika i nadzire sve prakse suočavanja sa zaposlenicima, poput podizanja svijesti, obuke i komunikacije. Također pruža uvid u ponašanje zaposlenika i njihove različite uloge te zna kako ugraditi nove prakse u već ustaljene procese. Odjel za ljudske resurse može osigurati da svi prođu istu obuku te može nadgledati sve evaluacije, poticajne sheme ili disciplinske mjere [145].

Odjel za pravne poslove treba osigurati da sve nove prakse doprinose potpunom usklađivanju organizacije s nacionalnim i međunarodnim zakonodavstvom, uključujući i zaštitu informacija. Također, ako bilo koja od praksi informacijske sigurnosti uključuje praćenje ponašanja zaposlenika, odjel za pravne poslove može utvrditi spada li takvo nadgledanje u granice zakona [145].

3.5.2.2. Kompetencije

Krakar i suradnici [42] navode kako termin *kompetencije* predstavlja „*skup znanja i vještina te sposobnosti njihovog korištenja s pripadajućim odgovornostima*" gdje je znanje dio kompetencija kojeg čine stečene i povezane informacije, dok su vještine naučena ponašanja kako obaviti neki posao. Stjecanje i razvoj znanja i vještina vezanih uz informacijsku sigurnost moguće je putem formalnog obrazovanja na sveučilišnim i stručnim studijima ili putem stjecanja stručnih certifikata. Stručni certifikati, do prije nekoliko godina, bili su nešto što je bilo dobro, ali ne i nužno imati prilikom zapošljavanja dok danas već skoro pa postaje pravilo da je uvjet zapošljavanja, uz određeno iskustvo u predmetnom području i posjedovanje certifikata koji potvrđuje to iskustvo, budući da, stručni certifikati, osim iskustva i znanja u pojedinom području, zbog potrebe ponovnog certificiranja svakih nekoliko godina pokazuju i predanost profesionalnom razvoju i stručnom usavršavanju [147]. Iako certifikati nisu savršeni, njihovo dobivanje standardni je način na koji će profesionalci informacijske sigurnosti poboljšati svoje sigurnosno obrazovanje i usavršavanje gdje certifikati pokazuju da je osoba uložila vrijeme, trud i novac u dodatno učenje o sigurnosti [39].

Mnogo je certifikata ponuđenih unutar okvira informacijske sigurnosti koji određuju razvoj, procese, politike i kriterije procjene sigurnosnog sustava [56], no oni se općenito mogu podijeliti na dvije osnovne vrste: certifikate vezane za pojedinog dobavljača (engl. *Vendor-specific*) i certifikate neovisne o dobavljaču (engl. *Vendor-neutral*) [39]. Glavna razlika između ove dvije vrste su teme uključene u svaki od njih, što znači da, dok certifikati neovisni o dobavljaču pružaju sveobuhvatnije pokrivanje u pogledu informacijske sigurnosti te stavljaju veći naglasak na upravljačke vještine, certifikati specifični za pojedine dobavljače nude specifično znanje o područjima koja su potrebna u skladu s okvirima i uređajima dobavljača [56].

Stručni certifikati neovisni o dobavljaču (engl. *Vendor-neutral*) obuhvaćaju koncepte i teme općenite prirode te se ne usredotočuju na određeni proizvod ili liniju proizvoda, a sam certifikat predstavlja službenu izjavu kojom se potvrđuje činjenica da je osoba zadovoljila specifične

uvjete posla gdje ti uvjeti često uključuju posjedovanje određene razine iskustva, završetak edukacije položen ispit [39].

Postoji nekoliko međunarodno prepoznatih organizacija koje pružaju usluge edukacije i stjecanja stručnih certifikata, ne nužno samo iz područja informacijske sigurnosti, od kojih su najpoznatije **ISACA** (Information Systems Audit and Control Association) čiji su najpoznatiji certifikati CISA (Certified Information Systems Auditor) i CISM (Certified information security manager)[1], **(ISC)²** (International Information System Security Certification Consortium), čiji je najpoznatiji certifikat CISSP (Certified Information Systems Security Professional)[2], **GIAC** (Global Information Assurance Certification) čiji su najpoznatiji certifikati GSEC (GIAC Security Essentials) i GSE (GIAC Security Expert)[3] te **CompTIA** (Computing Technology Industry Association) čiji je najpoznatiji certifikat Security+[4].

Stručni certifikati vezani za pojedinog dobavljača (engl. *Vendor-specific*) pomažu identificiranju profesionalaca koji posjeduju detaljno znanje o proizvodima pojedinog dobavljača pa tako postoje certifikati vezani uz Cisco Systems, Check Point, IBM, Oracle, Symantec i druge [39].

Kako bi definirali ključne vještine potrebne za funkciju voditelja informacijske sigurnosti, Haqaf i Koyuncu [56] proveli su istraživanje u kojem su, na temelju okvira informacijske sigurnosti, definirali 43 vještine koje su rasporedili u pet kategorija: *tehničke vještine*, *vještine upravljanja projektima / procesima*, *vještine upravljanja rizicima*, *poslovne vještine* i *temeljne vještine informacijske sigurnosti* koje su eksperti iz područja informacijske sigurnosti potom trebali rangirati po važnosti. Nakon tri kruga panela eksperata, eksperti su se složili oko 16 konačnih vještina bitnih za upravljanje informacijskom sigurnošću u kojima je svih pet predloženih kategorija bilo zastupljeno s barem jednom vještinom. Temeljne vještine informacijske sigurnosti zauzimaju najveći postotak na popisu s vrijednošću od 43,75%, a slijede vještine upravljanja projektima / procesima i vještine upravljanja rizikom s 18,75%, tehničke vještine s 12,50% i poslovne vještine sa 6,25%. Iako su temeljne vještine informacijske sigurnosti bile najzastupljenije, „dizajniranje sigurnosnih informacijskih sustava" kao najbolje rangirana vještina iz te kategorije, bila je tek na trećem mjestu dok su prve dvije ključne vještine „razumijevanje pitanja informacijske sigurnosti iz perspektive rukovodstva" (vještina

[1] https://www.isaca.org/credentialing/certifications
[2] https://www.isc2.org/Certifications
[3] https://www.giac.org/certifications/get-certified/roadmap
[4] https://www.comptia.org/certifications/security

upravljanja projektima/procesima) te „prepoznavanje najbolje prakse informacijske sigurnosti za upravljanje rizicima" (vještina upravljanja rizicima) što ukazuje na važnost vještina upravljanja projektima i upravljanja rizicima za osnaživanje kompetencija voditelja informacijske sigurnosti [56].

Budući da upravljanje informacijskom sigurnošću ima svojevrstan sukob zbog tehničkog stručnjaka s upravljačkom ulogom [56] gdje voditelji informacijske sigurnosti trebaju dobro razumjeti ne samo tehničke već i poslovne aspekte u organizacijama [142] te razgovarati o problemima, razumjeti korisnike i pregovarati o mogućnostima [56] koristeći poslovni, a ne tehnički jezik, obrazovne ustanove trebale bi razvijati kurikulume koji pomažu budućim voditeljima informacijske sigurnosti razviti potrebne i tehničke i poslovne vještine [142]. To je u skladu s istraživanjem koje su proveli Pažur Aničić i suradnici [148] čiji rezultati, na temelju analize sadržaja relevantnih istraživanja, ukazuju na potrebu za holističkim i strateškim pristupom obrazovanju budućih ICT stručnjaka, uključujući podršku razvoju karijere u formalnim procesima visokog obrazovanja.

3.5.3. Politika informacijske sigurnosti

Kvalitetan program upravljanja informacijskom sigurnošću započinje i završava pravilno provedenom politikom informacijske sigurnosti [23] koja pruža formalni smjer i namjeru rukovodstva za zaštitu informacija u organizaciji [149], a istodobno je usklađena s organizacijskim ciljevima [150] te prevodi očekivanja upravljanja sigurnošću u jasne, specifične i mjerljive ciljeve i odgovornosti [151].

Politika informacijske sigurnosti, kao pisani dokument koji utvrđuje pravila i smjernice kako organizacija planira zaštititi svoju informacijsku imovinu [152], [153] i utvrđuje očekivano ponašanje unutar organizacije [28], [154], [155], mora pažljivo uravnotežiti dva ključna elementa, povjerenje i kontrolu, gdje je odgovarajuća razina kontrole određena sigurnosnim potrebama i kulturom organizacije [84]. Primjerice, ako su pravila vezana za složenost lozinke previše striktna može se javiti kontraefekt u vidu zapisivanja lozinki ili dijeljenja lozinki s drugima kako se ne bi morale češće mijenjati [71].

Politike predstavljaju najjeftinije sredstvo kontrole koje je istodobno često najteže provoditi zbog činjenice da ne postoji pristup „jedna veličina odgovara svima" za uspostavljanje sigurnosnih politika jer se svaka organizacija suočava s jedinstvenim skupom prijetnji jedinstvenom skupu informacijske imovine [23]. Međutim, ono što vrijedi za sve organizacije

koje implementiraju sigurnosne politike, bilo svojevoljno ili zbog uvjetovanosti od strane nekog zakonodavnog ili regulatornog tijela [5], jest činjenica da je bez podrške višeg rukovodstva sigurnosna politika osuđena na propast [23], [100].

U kontekstu informacijskih tehnologija i informacijske tehnologije, izraz „politika" ponekad se odnosi na pravilo jedne politike, dok se u drugim slučajevima odnosi na zbirku takvih pravila [23] pa tako postoje upravljačke i tehničke politike [156]. To znači da se na jednoj razini sigurnosna politika može promatrati kao skup izjava rukovodstva koji definira filozofiju organizacije o zaštiti informacija dok se na detaljnijoj i tehničkoj razini sigurnosna politika može smatrati skupom pravila za pristup informacijskom sustavu i razradom kako će se ona provoditi [84]. Budući da je sigurnosna politika toliko sveobuhvatna i često detaljna, većina organizacija odlučuje sigurnosnu politiku razbiti na više podpolitika pa onda razlikujemo opću, vršnu politiku informacijske sigurnosti u obliku kratke pisane izjave koja dolazi od višeg rukovodstva [57], odnosi se na cijelu organizaciju i određuje smjer radnji za zaštitu informacijske imovine [39] i više manjih politika niže razine koje se odnose na pojedino područje upravljanja informacijskom sigurnošću (npr. politika upravljanja pravima pristupa, politika čistog stola, politika upravljanja sigurnosnim incidentima i sl.) [23]. Izraz „sigurnosna politika" općeniti je pojam za sve glavnu politiku i sve podpolitike unutar nje [84].

Budući da sigurnosna politika može značiti različite vrste dokumenata različitim organizacijama, ne postoji jedinstven opis onoga od čega se sastoji pa tako Paananen i suradnici [156] navode kako je njihova analiza otkrila mnogo karakterizacija i funkcija danih sigurnosnoj politici te možemo razlikovati opis i funkciju politike iako mnogi autori kombiniraju pojmove. Ono što sigurnosna politika *jest* (opis) mora primjereno podržavati ono što sigurnosna politika *pruža* (funkcija). Na primjer, nedovoljne upute ne mogu dovesti do sveobuhvatne kontrole nad ljudskim postupcima. Drugim riječima, prilikom definiranja sigurnosne politike moramo se suzdržati od pretpostavke da bi postojanje bilo koje karakteristike politike automatski dovelo do bilo koje njezine funkcije. Na primjer, sâmo postojanje unaprijed definiranih sankcija ne može dovesti do savršene usklađenosti [156].

Prilikom definiranja sigurnosne politike organizacije moraju prepoznati i uključiti elemente važne za kvalitetnu implementaciju sigurnosnu politiku kako bi smanjili rizik razvoja politike koja je slabo osmišljena, nepotpuna, suvišna i nevažna, a koju korisnici neće u potpunosti podržati [157]. Upravljačke politike izvršne razine trebale bi se baviti konceptualnim pitanjima, a ne specifičnostima pa bi tako opća politika informacijske sigurnosti trebala biti što kraća, ne

uključivati tehničke i poslovne detalje koji se redovito mijenjaju već bi se trebala baviti sigurnosnim načelima, a ne detaljima dok politike niže razine mogu biti dinamičnije, specifične i prilično detaljne, uzimajući u obzir trenutne ekonomske, poslovne, tehnološke i druge situacije u obzir [135].

Politika informacijske sigurnosti trebala bi biti podložna promjenama i izmjenama te predmet redovitih periodičkih ažuriranja [152], [28] kako bi uvijek bila aktualna i relevantna te pomogla minimizirati rizik od skupih nezgoda naglašavanjem jasnih uputa o onome što se očekuje kao pravilno ponašanje zaposlenika u pogledu informacijske sigurnosti [100] te koje su sigurnosne politike i prakse obavezne [85]. Također, politika informacijske sigurnosti trebala bi biti jasna, nedvosmislena, laka za shvaćanje i provođenje [152]. To znači da bi politika informacijske sigurnosti trebala biti napisana u neutralnom stilu pisanja bez tehničkog žargona da ih lako razumije ne-tehnički zaposlenik [128] i upotrebom eksplicitnih izjava s jednostavnim rečenicama koje mogu povećati jasnoću politike i smanjiti mogućnost pogrešnog tumačenja te time u konačnici olakšati zaposlenicima pridržavanje navedene sigurnosne politike [158].

Dodatno, rezultati istraživanja koje su proveli Johnston i suradnici [159] pokazuju da suptilno mijenjanje manje od desetak riječi na način na koji je predstavljena sigurnosna poruka bez promjene njezinog sadržaja (npr., korištenjem riječi „naše" umjesto „tvoje/Vaše") ima i značajne i smislene učinke na način na koji zaposlenici razmišljaju i reagiraju na nju [159]. Naposljetku, u politici bi trebalo izričito definirati opseg politike, pravne i regulatorne obveze u smislu definiranja uloga i odgovornosti onih na koje se odnosi i posljedica kršenja njenih uvjeta [152], ali i objasniti zašto je pojedina politika važna jer u protivnom zaposlenici mogu zanemariti neke politike smatrajući ih gubitkom vremena [128].

Ostale komponente povezane sa sigurnosnom politikom uključuju procedure i smjernice kojima se pokušava detaljnije objasniti radnje koje u bilo kojoj situaciji trebaju poduzeti zaposlenici [23].

Procedure predstavljaju logično opisane postupke korak po korak [154] koje zaposlenicima daju detaljne upute kako će se provoditi sigurnosna politika i tko čini što da ispuni zadatke [135]. Procedure se mogu smatrati „receptima" koji daju jasnoću i zajedničko razumijevanje za operacije koje su potrebne za učinkovito podržavanje politike na dosljednoj razini [57]. Na taj način procedure poboljšavaju efikasnost u radu zaposlenika i pomažu u sprječavanju zlouporabe i prijevare budući da zaposlenicima pružaju informacije potrebne za obavljanje

zadataka, a istodobno uvjeravaju rukovodstvo da se zadaci izvršavaju na jedinstven i odobren način [154]. Smjernice, s druge strane, predstavljaju predloženi tijek radnji za korištenje politike, procedura ili standarda, te mogu biti specifične ili fleksibilne u pogledu upotrebe [39]. Primjeri smjernica dobrih praksi uključuju redovito implementiranje sigurnih zakrpi (engl. *Patch*), promjenu unaprijed definiranih lozinki (engl. *Default password*), korištenje robusnih lozinki, zatvaranje nepotrebnih portova, dodjelu prava pristupa samo na temelju poslovne potrebe ili korištenje računa s povlaštenim pravima samo za administrativne poslove [23].

Važno je napomenuti kako definiranjem niza politika organizacije ne osiguravaju da će se svi zaposlenici nužno pridržavati tih pravila [135] jer, čak i u slučaju da sigurnosna politika postoji, potrebno je osigurati da se kontinuirano odvijaju edukacija, obuka i podizanje svijesti o njoj [160], [161], [98] budući da je politika informacijske sigurnosti bez edukacije, obuke i osviještenosti zaposlenika beskorisna [83]. Drugim riječima, sigurnosna politika može biti učinkovita samo ako zaposlenici znaju, razumiju i prihvaćaju potrebne mjere zaštite što dovodi do uvjeta za odgovarajuću osposobljenost i svijest unutar organizacije, kako bi se potaknula odgovarajuća kultura informacijske sigurnosti [21].

3.5.4. Edukacija, obuka, osviještenost

U današnjem okruženju organizacije ne mogu zaštititi povjerljivost, integritet i dostupnost informacija bez osiguravanja da svaka uključena osoba razumije svoje uloge i odgovornosti i ima odgovarajuće znanje o svojoj specifičnoj ulozi u sigurnosnom procesu [162], [163], [160], [164] budući da je posjedovanje dostatnog znanja o informacijskoj sigurnosti preduvjet za obavljanje bilo koje uobičajene aktivnosti na siguran način [95]. Prije nego što se od bilo kojeg zaposlenika zatraži da poštuje uspostavljene sigurnosne politike, zaposlenik prvo mora biti svjestan potrebe i samog procesa [154], [165] iz razloga što, ako zaposlenik ne zna ili ne razumije kako održavati povjerljivost informacija ili kako ih na odgovarajući način zaštititi, organizacija riskira da se jedan od najvrjednijih poslovnih resursa pogrešno obrađuje, na neodgovarajući način upotrebljava ili dobiva od neovlaštene osobe [97].

Činjenica je da, ako se o zahtjevima sigurnosnih politika zaposlenici pravilno i redovito ne obavještavaju i ne educiraju, šanse da se one manifestiraju u njihovom ponašanju su minimalne [135], stoga bi zaposlenike trebalo upoznati s određenim operativnim kontrolama koje ovise o njihovom ponašanju kako bi bile učinkovite. Kako bi se to postiglo, potrebna je određena razina znanja, opsežna svijest o informacijskoj sigurnosti te programi osposobljavanja i edukacije [162] s ciljem oblikovanja namjera zaposlenika u skladu s pravilima sigurnosne politike [166].

Edukacija, obuka i osviještenost ili podizanje svijesti o sigurnosti, koji se često vežu zajedno i nazivaju SETA (engl. *Security Education Training Awareness*) programom, predstavljaju proces kojim svi zaposlenici organizacije imaju priliku poboljšati svoje znanje o informacijskoj sigurnosti u nastojanju da zaštite sebe i organizacijsku imovinu [23] te predstavljaju jednu od najučinkovitijih mjera suprotstavljanja prijetnji ljudskog čimbenika informacijske sigurnosti [86], [9], [167] i važan dio upravljanja informacijskom sigurnošću [168], [169] za koji je potrebno osigurati snažnu podršku rukovodstva kako bi se smanjio pasivan otpor zaposlenika [97], [113].

Budući da su prakse osviještenosti, obuke i edukacije neizbježno povezane [71], razlike između ovih pojmova nisu uvijek u potpunosti jasne i strogo odvojene jer se ponekad naizmjenično koriste u postojećoj literaturi [169], međutim, ipak postoje određena obilježja koja čine razliku kod ova tri mehanizma učenja, kao što prikazuje Tablica 3.2.

Tablica 3.2. Razlika između sigurnosne edukacije, obuke i podizanja svijesti

	Edukacija	**Obuka**	**Podizanje svijesti**
Fokus	Zašto?	Kako?	Što?
Razina	Uvid	Znanje	Informacija
Svrha	Stjecanje razumijevanja i kompetencija	Stjecanje vještina	Podsjećanje na uloge i odgovornosti i aktualne prijetnje i ranjivosti
Metoda učenja	Teoretske instrukcije (seminari, proučavanje literature, istraživanje)	Praktične instrukcije (predavanje, radionice, praktične vježbe)	Mediji (video zapisi, letci, brošure, plakati)
Vremenski okvir učinka	Dugoročni	Srednjoročni	Kratkoročni

Izvor: *prilagođeno prema* [169], [28]

Kao što vidimo, osvješćivanje je obično komponenta „što" edukacijske strategije za utjecanje na ponašanje i praksu, obuka komponenta „kako" implementirati sigurnost i privatnost, dok edukacija čini komponentu „zašto" [97]. Roper i suradnici [170] sažimaju razlike između sigurnosne edukacije, obuke i osvješćivanjem na sljedeći način: ljudi neće raditi ono što ne znaju kako, što se ispravlja obukom; ono čega se ne bi sjetili da trebaju, što se ispravlja podizanjem svijesti; kao ni ono za što smatraju da nema smisla, što se ispravlja edukacijom. Dodatno, isti autori navode kako ljudi neće raditi niti ono za što ne vide razlog, što se u konačnici ispravlja pravilnom motivacijom [170], koja se može sastojati od poticanja i

nagrađivanja poželjnog ponašanja informacijske sigurnosti ili obeshrabrivanja i kažnjavanja nepoželjnog [23] gdje se prednost daje nagrađivanju u odnosu na kažnjavanje [86].

Prvi element SETA programa, **sigurnosna edukacija**, predstavlja specijalizirano dubinsko učenje koje je potrebno za podršku korištenih alata ili kao proces razvoja karijere [154] te je najkorisnija za ljude koji nemaju bogato iskustvo u području informacijske sigurnosti, a mogu imati koristi od formalnih tečajeva kako bi uspostavili osnovno znanje koje mogu nadograđivati [23]. U literaturi je često manji naglasak na edukaciju nego na ostale komponente SETA programa upravo zbog toga što sigurnosna edukacija obuhvaća nastavni plan i program koji je stvoren s ciljem da se pojedinci educiraju u širokom nizu sigurnosnih tema koje će izgraditi niz znanja bitnih za karijeru u informacijskoj sigurnosti [23]. Dok svi zaposlenici trebaju biti sigurnosno obučeni i osviješteni, ne trebaju svi imati stručni certifikat ili formalno obrazovanje iz informacijske sigurnosti [28].

Drugi element SETA programa, **sigurnosna obuka**, predstavlja bilo koje nastojanje kojim se osigurava da je svaki zaposlenik opremljen znanjima, vještinama i sposobnostima vezanim uz informacijsku sigurnost specifičnima za njegove uloge i odgovornosti [169], [97] odnosno, to je proces koji uči vještinu ili upotrebu potrebnog alata [154]. Obuka je ciljani, formalni i interaktivni događaj koji zahtijeva punu pažnju sudionika kako bi imali koristi od nje [23], [97] te je, kao što poslovica kaže „znati, ali ne raditi je isto kao ne znati uopće", na pojedinim sudionicima ovih obuka da ozbiljno shvate poruku i sadržaj tih obuka i primjene ih u svojim aktivnostima [35].

Treći element SETA programa, **sigurnosna osviještenost**, koristi se za poticanje, motiviranje i podsjećanje zaposlenika na ono što se od njih očekuje [154], odnosno predstavlja bilo koje nastojanje usmjeravanja pažnje zaposlenika na informacijsku sigurnost kako bi se osiguralo da svi zaposlenici razumiju i prihvate svoje uloge i odgovornosti u zaštiti organizacijskih informacija, sukladno sigurnosnim politikama [169], [151]. Sigurnosna osviještenost najmanje se koristi kao metoda za prijenos općeg znanja [23], a od velike je važnosti u odvraćanju od namjere zloupotrebe informacijske sigurnosti [171] te osigurava znatno smanjenje šansi pojave ili rizika sigurnosnih ranjivosti i prijetnji. [35]. Sama svijest o informacijskoj sigurnosti može se promatrati kroz tri komponente: ono što zaposlenik zna (znanje), što misli o tome (stav) te što stvarno radi (ponašanje) [76], a kao i obuka, sigurnosna osviještenost namijenjena je svim zaposlenicima, s ciljem njihovog pripremanja na sposobnost projiciranja potencijalnih

sigurnosnih rizika [172], [113], tako da svi održavaju određenu razinu skepse kada se nađu u situaciji koja je neuobičajena [23].

Bez odgovarajućeg znanja, zaposlenici koji se žele ponašati sigurno mogu i dalje primijeniti sigurnosnu kontrolu pogrešno, ali isto tako, zaposlenik koji ima odgovarajuće znanje, ali vjeruje da sigurno ponašanje nije potrebno u njegovoj ulozi u organizaciji i dalje se može ponašati nesigurno. Tako rezultati istraživanja koje su proveli D'Arcy & Hovav [173] sugeriraju kako SETA programi i nadzor, iz perspektive odvraćanja od nepoželjnog ponašanja, manje utječu na zaposlenike koji su napredniji korisnici računala, kao i na zaposlenike koji provode više radnih dana izvan ureda od onih koji su kontinuirano na radnom mjestu u organizaciji. Stoga bi organizacije trebale stvoriti specijalizirane sigurnosne programe za radnike koji provode više radnih dana izvan ureda kako bi shvatili da se organizacijske mjere zaštite primjenjuju jednako bez obzira s koje se strane fizičke granice ureda nalazili [173].

Prilikom provođenja aktivnosti obuke i podizanja svijesti o informacijskoj sigurnosti trebalo bi se voditi načelom da bi informacijska sigurnost trebala biti laka, brza i jednostavna zaposlenicima za razumjeti, umjesto da im predstavlja teret i „još jedan dodatni dosadan zadatak" [167], a takve aktivnosti prilagoditi ciljevima i zahtjevima sigurnosne politike organizacije [174] kao i aktualnim prijetnjama i ranjivostima. Obuka obuhvaća brojne tehnike i pristupe provođenja u rasponu od predavanja licem u licem, koje je aktivna vježba samo za predavača dok je za one koji pohađaju predavanje to pasivna vježba koja nije tako učinkovita kao aktivno učenje pri prenošenju znanja [113], preko obuke temeljene na računalu (engl. *Computer-based Training*), obuke putem video zapisa, seminara putem Interneta (engl. *Webinar*), radionica, vanjskih stručnih predavanja, igranja scenarija i sl. [145], [113]. Svaki pristup ima svoje prednosti i nedostatke, a odluka o tome koje tehnike koristiti većinom se temelji na dostupnosti i troškovima [71].

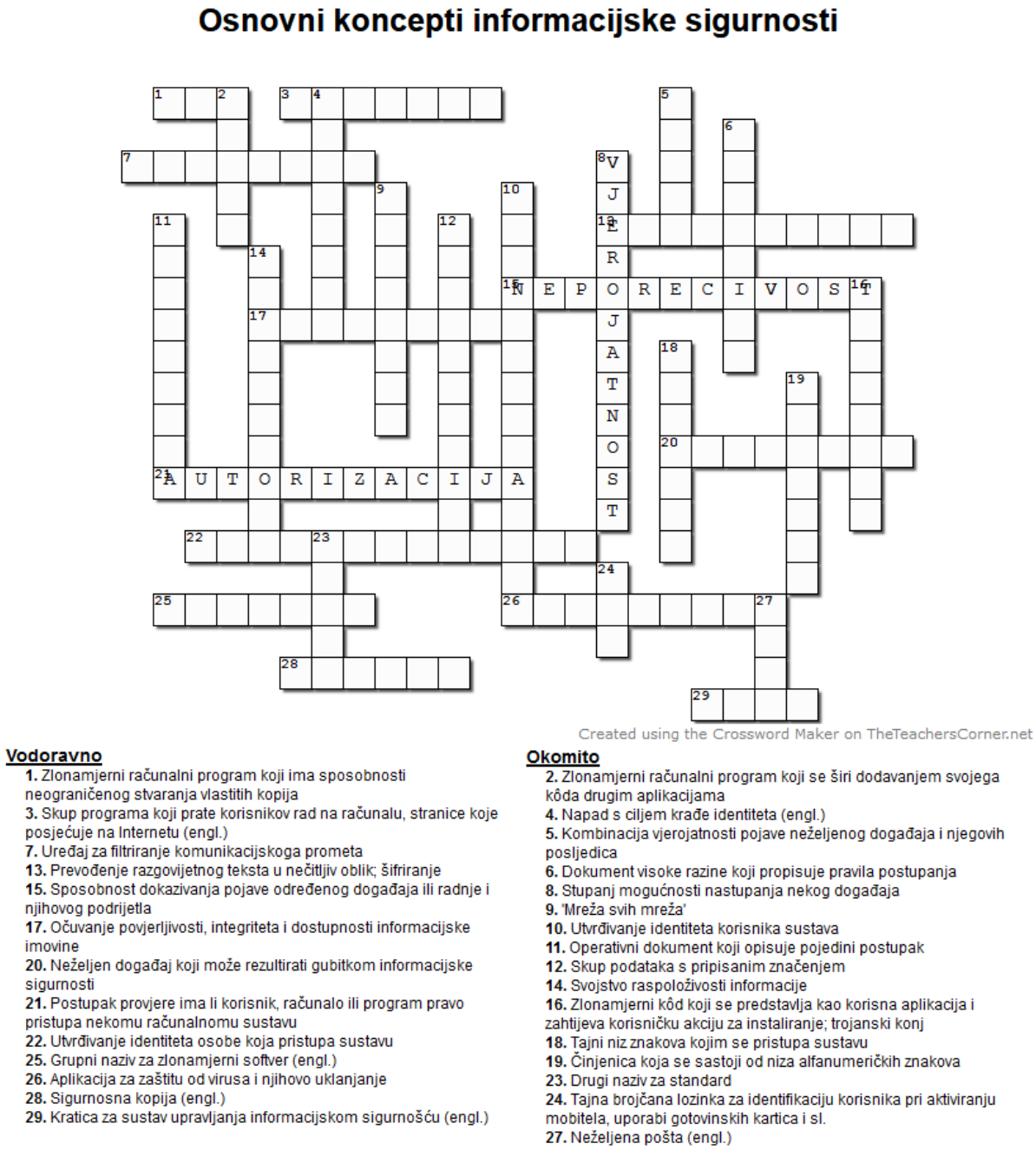
Podizanje svijesti o informacijskoj sigurnosti, uz sve navedene tehnike koje se koriste i za obuku, uključuje i niz dodatnih metoda i tehnika s naglaskom na korištenje vizualnih materijala (kratki, zanimljivi video isječci, animacije, karikature i sl.) i kratke, sažete rečenice umjesto dugačkih, detaljnih, formalno pisanih materija [167] budući da je cilj programa podizanja svijesti prenošenje poruke ljudima [154] zbog čega ne smije biti dosadno [97]. Tehnike i metode podizanja svijesti, između ostalog, uključuju video zapise, animirane elektroničke poruke, SMS-ove, mobilne grupe za chat, društvene mreže, biltene, letke, brošure, plakate (Slika 3.1.), oglasne ploče, kratke podsjetnike, transparente, džepne knjižice o sigurnosti, promotivne

materijale sa sigurnosnim pitanjima, sitnice sa sigurnosnim porukama (šalice, čaše, olovke, upaljače, podloge za miša, privjeske, itd.), edukativna natjecanja, kvizove, križaljke (Slika 3.2.), priče dobre prakse, tablice za savjetima dobrih praksi, odgovore na najčešće postavljena pitanja, interaktivni računalni trening, kao što su video igre, igranje uloga ili simulacije slanja elektroničkih poruka s ciljem krađe identiteta (*Phishing* poruke), korporativna događanja (sigurnosne konferencije, „dan/tjedan/mjesec informacijske sigurnosti", „najsigurniji djelatnik mjeseca", itd.) i sl. [167], [175], [145], [23], [176].

Slika 3.1. Primjeri plakata u svrhu podizanja svijesti o informacijskoj sigurnosti

Izvor: *https://www.globalknowledge.com*[5]

[5] Izravna poveznica: https://www.globalknowledge.com/sv-se/training/courses/topics/security/cybersecurity%20awareness%20month/cybersecurity%20awareness%20month%20posters



Slika 3.2. Primjer tehnike podizanja svijesti o informacijskoj sigurnosti

Izvor: *vlastiti prikaz*[6]

Najučinkovitija obuka i osvješćivanje postiže se kombinacijom različitih tehnika pri čemu se stvara sigurnosna kampanja koja proizvodi propagandu i sadržaj na načine koji su inovativni, privlačni i sveobuhvatni [23]. Međutim, pri tome je potrebno voditi računa o tome da, iako postoji pozitivna korelacija između stupnja bogatstva medija za prezentiranje sadržaja i

[6] Izrađeno pomoću alata Crossword Maker dostupnog na: http://worksheets.theteacherscorner.net/make-your-own/crossword/

poboljšanja razine svijesti o informacijskoj sigurnosti, moguć je i potencijalni negativni učinak prevelikog medijskog bogatstva na uspješnost učenja, kao što su pokazali rezultati istraživanja koje su proveli Shaw i suradnici [172].

Kako bi se poboljšala učinkovitost tehnika podizanja svijesti o informacijskoj sigurnosti, sadržaj informiranja o sigurnosti informacija ne bi se trebao temeljiti na onome što tehnički stručnjaci žele reći ljudima, sadržaju tehničkog standarda ili prevladavajućoj temi najbolje prakse, nego na samoj publici koja nastoji utjecati na prijetnje i štititi informacijsku imovinu [177] zbog čega je potrebno poznavati svoju publiku, a podizanje svijesti učiniti zanimljivijim korištenjem analogija, stvarnih primjera iz prakse, humora i doskočica, vezom s poznatim osobama ili aktualnim zbivanjima iz medija i vijesti, pružanjem praktičnih informacija i sl. [97].

SETA programi mogu drastično umanjiti vjerojatnost kršenja sigurnosti te transformirati ponašanje korisnika i korporativnu kulturu razvijanjem savjesnije i spremnije populacije korisnika [23] gdje su sigurnosne teme i zahtjevi integrirani u normalno poslovno ponašanje, kroz jasne sigurnosne politike i edukaciju zaposlenika o njima [9]. Međutim, važno je napomenuti da sigurnosne politike, čak i ako ih bespogovorno slijede svi zaposlenici, ne jamče da će spriječiti svaki napad socijalnim inženjeringom [128].

Tako su Kearney i Kruger [178] proveli istraživanje vezano uz napade s ciljem krađe identiteta (*Phishing* napadi) i sigurnosnu osviještenost zaposlenika putem testa s dvije različite *phishing* poruke poslane zaposlenicima u dva navrata s ciljem pokušaja utvrđivanja da li se ponašanje zaposlenika imalo pozitivno promijenilo u razdoblju između dva testa. Rezultati prvog testa pokazali su da je od 280 zaposlenika koji su odgovorili na poruku e-pošte, njih 231 (83%) dalo (unijelo na web stranicu) svoja ispravna korisnička imena i lozinke, od čega je njih 23 (10%) to učinilo više puta. Tu je važno napomenuti kako je 159 zaposlenika (69%) koji su dali svoje osobne podatke, već prije prošlo internu sigurnosnu obuku u organizaciji. Rezultati drugog testa, koji je proveden nakon određenog vremenskog razdoblja, a bio isti kao i prvi, osim samog sadržaja elektroničke poruke, bili su neočekivani i pomalo razočaravajući. Naime, iako je niži postotak zaposlenika dao svoja korisnička imena i lozinke (40%), stvarni se broj povećao sa 231 od ukupno 280, na 312 od ukupno 490 zaposlenika koji su odgovorili na lažnu elektroničku poruku. Broj zaposlenika koji su prethodno prošli sigurnosnu obuku, a koji su dali svoje osobne podatke, također je porastao sa 159 na 288, što čini čak 92%. Dodatno, u konačnici je bilo 48 zaposlenika koji su otkrili svoja korisnička imena i lozinke i u prvom i u drugom testu [178].

Rezultati istraživanja kojeg su proveli Eminağaoğlu i suradnici [167] pokazali su pozitivne i učinkovite rezultate nakon provedenih aktivnosti sigurnosne obuke i podizanja svijesti. Između ostalog, upotreba slabih lozinki značajno je i kontinuirano smanjena kod većine zaposlenika, zaposlenici su počeli razvijati kontinuirano poboljšanje osviještenosti i bili su skloniji sigurnije birati i koristiti svoje lozinke, počeli su sudjelovati u kontrolama i mehanizmima informacijske sigurnosti koji su bili uključeni u kampanju podizanja svijesti te se većina zaposlenika počela (iako nevoljko) usklađivati sa sigurnosnim politikama organizacije [167].

Nakon završetka učinkovitog programa sigurnosnog osvješćivanja, mentalni sklop zaposlenika trebao bi biti u mogućnosti napredovati od stanja „*postati svjestan*" preko „*biti svjestan*" do „*ostati svjestan*" sigurnosnih prijetnji [179] što dovodi do sigurnosne kulture unutar organizacije u kojoj se cijene pozitivna sigurnosna ponašanja i potiče stav da sigurnost započinje i završava kod svake osobe koja je uključena u organizacijsku infrastrukturu i aktivnosti [99].

3.5.5. Ljudski čimbenik u informacijskoj sigurnosti

Često se kaže da informacijska sigurnost započinje i završava kod ljudi [81], [180] koji predstavljaju ključni čimbenik (ne)uspjeha upravljanja informacijskom sigurnošću [167], [137], [8], [14], [4], [181], [182] budući da literatura dosljedno prikazuje ljude kao „najslabiju kariku" informacijske sigurnosti [105], [13], [39], [113], [183], [184], [185] [186], [187], [2], [155], [169], [99], [181], [188], [88], [189], [85], [152] stavljajući tako fokus na ljudski čimbenik upravljanja informacijskom sigurnošću umjesto donedavno dominantnih tehničkih čimbenika [190], [12], [79], [8], [191], [86], [192], [153], [68]. Nažalost, svaka je tehnička mjera, bez obzira koliko su dobro osmišljene njene temeljne sigurnosne mogućnosti, sklona eksploataciji ako ljudi koji ju koriste ili upravljaju njome čine propuste u svom djelovanju [25], [71], [167], [79], [193] iz razloga što svaki zaposlenik koji može pristupiti informacijskom sustavu organizacije može postati izvor sigurnosne prijetnje [194].

Ti propusti mogu biti svjesni, poput krađe podataka, uništavanja opreme ili podataka, otkrivanja povjerljivih informacija i sl. i nesvjesni, kao što je postavljanje slabih lozinki, zapisivanje lozinki na papiriće zataknute na računalo, napuštanje računala za vrijeme stanke dok su još prijavljeni na sustav, raspravljanje o povjerljivim informacijama na javnom mjestu i sl. [153], [195], [126], [20]. Za razliku od svjesnih propusta čiji je uzrok određeno zlonamjerno ponašanje, nesvjesni propusti predstavljaju nehotične, nenamjerne ili slučajne radnje koje ugrožavaju informacijsku sigurnost, a čiji uzroci mogu biti razni, uključujući podcjenjivanje

rizika povezanih sa sigurnošću informacija [195], [196], nerazumijevanje uspostavljenih sigurnosnih politika, nedostatak znanja o sigurnosnim praksama ili nemogućnost pravilne primjene svog znanja na svoju radnu ulogu ili okolinu [79].

Upravo ta nesvjesnost o postojanju sigurnosnih praksi ili nerazumijevanje sigurnosne politike može zaposlenike izložiti napadima socijalnog inženjeringa koji pametni napadači koriste za postizanje svojih ciljeva budući da je najlakši način za probijanje u sustav osmisliti put kroz ljudsko sučelje [25] zbog karakteristika i ponašanja ljudi [99]. Ljudi su znatiželjni, žele biti korisni i obaviti dobar posao te žele pružiti dobru korisničku uslugu svojim suradnicima, klijentima i poslovnim partnerima što napadači žele iskoristiti, a jedina poznata obrana od napada metodama socijalnog inženjeringa je učinkovit program edukacije, obuke i ponajviše podizanja svijesti o sigurnosti [113].

Važno je naglasiti kako svijest o informacijskoj sigurnosti, kao temeljni dio učinkovitog upravljanja informacijskom sigurnošću, ipak nije panaceja te kako bi svijest bila učinkovita, treba imati na umu da se, za učinkovito upravljanje sigurnošću, moraju odvijati i druge paralelne aktivnosti [71], koje između ostalog, uključuju primjerenu edukaciju i pravovremenu obuku zaposlenika, pružanje dobre tehničke infrastrukture, jačanje politika i procedura i dodjelu uloga i odgovornosti za informacijsku sigurnost.

Ulaganje u programe edukacije, osposobljavanja i podizanja svijesti o informacijskoj sigurnosti predstavlja pametnu investiciju budući da su pravilno educirani i obučeni zaposlenici jedan od ključnih čimbenika uspjeha u organizacijama bilo koje veličine kako bi se smanjile prijetnje ili zloupotreba informacijske imovine [175], [197]. Zaposlenici moraju biti svjesni informacijske sigurnosti i mogućih sigurnosnih prijetnji [87] jer su oni ti koji će se morati pridržavati sigurnosnih praksi i normi informacijske sigurnosti u organizaciji [20] kako bi mogli donositi dobro informirane odluke o informacijskoj sigurnosti dok svakodnevno obavljaju svoje dužnosti [169] i odgovorni su za pravilno rukovanje najvrjednijom imovinom organizacije [23], [77].

Pravilno obučeni za pridržavanje sigurnosnih politika i prepoznavanje potencijalnih sigurnosnih problema, zaposlenici se od najslabije karike i neprijatelja sigurnosti, pretvaraju u jaku kariku i jedno od najvećih sigurnosnih sredstava [74], [23] u nastojanju da se smanji rizik vezan uz informacijsku sigurnost [77]. Na taj način, zaposlenici koji igraju istaknutu ulogu u stvaranju prijetnji i dio su problema informacijske sigurnosti, istodobno s druge strane postaju

i dio rješenja jer putem edukacije, obuke i podizanja svijesti o informacijskoj sigurnosti igraju ključnu ulogu u zaštiti informacija i sprečavanju sigurnosnih proboja [13], [169], a njihova usklađenost sa sigurnosnim politikama predstavlja značajan pozitivan utjecaj na informacijsku sigurnost unutar organizacije [2].

Umjesto ulaganja u skupi softver ili hardver kako bi se postigla učinkovita razina informacijske sigurnosti, često je korisnije razraditi pažljiv plan edukacije, obuke i osviještenosti koji osigurava da se zaposlenici ponašaju na siguran način, s ciljem promjene navika zaposlenika [20] kako bi ponašanje zaposlenika prema informacijama bilo sigurnosno prihvatljivo i postalo dio svakodnevnog života u organizaciji [160].

Budući da je mijenjanje navika teško, važno je ukloniti prepreke na putu uspostavljanja novih navika koje mogu odvratiti pojedince od ciljeva ili opravdati vraćanju starim navikama [181]. Važno je osigurati prikladnu percepciju sigurnosti zaposlenika na način da svatko pretpostavlja da su sigurnosne aktivnosti dio njegove dnevne radne rutine. Zaposlenici se trebaju osjećati odgovornima za informacijsku sigurnost u organizaciji na što će utjecati stav o tome koje sve dodatne radnje zaposlenik mora poduzeti i smatra li se sigurnost preprekom u njegovim svakodnevnim aktivnostima [198].

Zaposlenici često smatraju sigurnosne prakse smetnjama svojim poslovnim rutinama dajući drugim zadacima viši prioritet nego sigurnosti što može dovesti do namjernih nemarnih radnji u svakodnevnom radu koje su jedan od glavnih uzroka štete za poduzete napore za informacijsku sigurnost unutar organizacije [151]. To znači da, kada je sigurnost neupotrebljiva i glomazna, unaprijed je programiran povratak na stari, učinkovitiji prečac [181], jer zaposlenici mogu odlučiti ne pridržavati se sigurnosnih pravila zbog praktičnosti u svakodnevnim poslovima [66]. Zbog toga organizacije moraju biti proaktivne, razumjeti i riješiti izazove povezane s informacijskom sigurnošću s kojima se zaposlenici svakodnevno susreću osmišljavajući prakse i alate za pomoć zaposlenicima u promjeni njihovih navika [181] na način da sigurnosne funkcije moraju biti smislene i što manje nametljive, a sigurnosne politike razumljive i jednostavne za pronalaženje [99].

Van Niekerk i Solms [162] ističu kako se ljudski čimbenik sastoji od dvije međusobno povezane dimenzije. Prvo, zaposlenici moraju imati dovoljno znanja o informacijskoj sigurnosti kako bi učinkovito provodili i održavali različite kontrole informacijske sigurnosti i drugo, zaposlenici moraju imati ispravan stav prema sigurnosti informacija gdje se nedostatak znanja općenito

može riješiti edukacijom, a stav poticanjem kulture informacijske sigurnosti u organizaciji. Međutim, ako zaposlenici posjeduju odgovarajuće znanje, ali nemaju potreban stav, neće se nužno *ponašati* sigurno, a s druge strane, zaposlenici koji imaju ispravan stav, ali nemaju potrebno znanje, neće se *moći ponašati* sigurno [162] pa su tako stav zaposlenika i nedostatak sigurnosne svijesti najznačajniji doprinos sigurnosnim incidentima [13].

Informacijska sigurnost je problem s kojim se svaki zaposlenik mora suočiti, a sigurnosno ponašanje zaposlenika te čimbenici koji utječu na njega bili su predmet mnogih istraživanja.

Tako su Herath i Rao [199], [66] uzeli u obzir i vanjske i unutarnje motivatore koji mogu potaknuti usklađeno sigurnosno ponašanje te su razmatrali utjecaj kazne (vanjski), društvenih pritisaka (vanjski) i percipirane vrijednosti ili doprinosa (unutarnji) u smislu sigurnosnih mjera. Njihovi rezultati pokazuju da je percepcija zaposlenika o tome jesu li drugi usklađeni s odredbama sigurnosnih politika pokazala da značajno doprinosi namjerama zaposlenika u pridržavanju samih politika [66]. Drugim riječima, ako zaposlenik percipira dosljedno ponašanje svojih kolega koje se podudara s očekivanjima nadređenog, vjerojatnije je da će pratiti što drugi kolege rade [151], [124]. Također, ako zaposlenici primijete kako postoji veća vjerojatnost da će biti uhvaćeni ako krše sigurnosne politike, veća je vjerojatnost da će slijediti sigurnosne politike. Iznenađujuće, ustanovljeno je da ozbiljnost kazne negativno utječe na namjere sigurnosnog ponašanja [199] iako je pronađeno da prethodna literatura o informacijskoj sigurnosti pokazuje proturječne rezultate za djelotvornost sankcija [134], [200]. Rezultati koje su iznijeli Herath i Rao [66] sugeriraju da je postojanje i vidljivost mehanizama otkrivanja možda važnije od težine izrečene kazne.

Rezultati istraživanja koje su proveli Safa i suradnici [201] pokazuju kako percipirana izvjesnost i strogost sankcija značajno utječu na stavove pojedinaca i odvraćaju ih od kršenja informacijske sigurnosti. Dodatno, rezultati analize podataka također su pokazali da subjektivne norme, percipirane kontrole ponašanja i stav utječu na namjere pojedinca i, na kraju, na njihovo ponašanje prema izbjegavanju lošeg ponašanja prema informacijskoj sigurnosti [201].

Velika izvjesnost sankcije šalje signale zaposlenicima o organizacijskim naporima za praćenje, evaluaciji i kažnjavanju nesukladnog ponašanja. Posljedično, povećava se njihova namjera da se ponašaju usklađeno jer su šanse da budu uhvaćeni i kažnjeni velike [67], stoga kazna kao strategija odvraćanja od nepoželjnog ponašanja može rezultirati pozitivnim ishodima [67], a

može uključivati primjenu negativnih posljedica i povlačenjem pozitivnih posljedica [202]. Negativne posljedice uključuju verbalne ukore, novčane kazne, suspenzije i prekid radnog odnosa, dok povlačenje pozitivnih posljedica uključuje uklanjanje privilegija, uskraćivanje povećanja plaća i odgađanje napredovanja. Svrha kazne je zaustaviti ili smanjiti učestalost nepoželjnog ponašanja zaposlenika ili povećati pridržavanje zaposlenika željenih standarda ponašanja organizacije [202].

Kazna je učinkovitija u odvraćanju od nepoželjnog ponašanja ako se kazna odmah izrekne i dosljedno se provodi odmah nakon svakog uočenog nepoželjnog ponašanja, nego ako kazna kasni ili bude nedosljedna. Drugim riječima, ako zaposlenici shvate da se njihovo neusklađeno ponašanje kontinuirano prati i kažnjava odmah i dosljedno, njihova namjera da poštuju sigurnosne politike će se povećati [67].

U isto vrijeme, za promicanje poželjnog ponašanja i poboljšanog radnog učinka, poslodavci često koriste nagrade koje signaliziraju zaposlenicima da njihov rad ili ponašanje ispunjavaju očekivanja organizacije, a može uključivati nematerijalne nagrade (npr. potencijalna promaknuća, nagrada zaposlenik mjeseca) i materijalne nagrade (npr. bonusi i plaćeni dopusti) [67].

Kao što je vidljivo iz prethodno navedenog, sigurnost informacija ovisi o ponašanju zaposlenika koje može pojačati ili oslabiti sigurnost [193] zbog čega istraživači predlažu njegovanje kulture informacijske sigurnosti koja promiče dobro i uklanja loše sigurnosno ponašanje zaposlenika [86], [138] kako bi informacijska sigurnost postala druga priroda za zaposlenike [155], [203] odnosno svačija odgovornost [24].

3.5.6. Usklađenost

Usklađenost s informacijskom sigurnošću odnosi se na učinkovitu primjenu standarda i politika informacijske sigurnosti kako bi se na odgovarajući način zaštitila informacijska imovina organizacije [37], a budući da su zaposlenici istodobno i najslabija karika i najvažniji resurs organizacije, njihova usklađenost s mjerama informacijske sigurnosti presudna je za uspjeh bilo kojeg procesa upravljanja informacijskom sigurnošću [136]. Zaposlenici koji ne poštuju smjernice informacijske sigurnosti nehotice olakšavaju pojavu sigurnosnih incidenata protiv svojih organizacija [105] budući da je veliki broj kršenja informacijske sigurnosti na radnom mjestu rezultat neuspjeha zaposlenika u usklađenju sa organizacijskih smjernicama za informacijsku sigurnost [124].

Ako zaposlenik odluči ne pridržavati se politike informacijske sigurnosti, ti resursi koje koristi u svakodnevnom radu ostaju ranjivi na rizike informacijske sigurnosti pa je ranjivost važno stanje koje proizlazi iz neusklađenosti zaposlenika s politikom informacijske sigurnosti. Međutim, ako zaposlenik izvršava ono što je propisano u politici informacijske sigurnosti, doprinosi zaštiti informacijske imovine organizacije [77] i uspješnom ublažavanju povreda informacijske sigurnosti [14].

Istraživanje koje su proveli Angraini i suradnici [204] obuhvatilo je analizu 53 istraživačka rada, od ukupno pronađenih 305, objavljenih na temu usklađenosti s politikom informacijske sigurnosti u razdoblju između 2014. i 2019. godine, gdje su rezultati analize pokazali kako nedostaje više istraživanja o procjeni usklađenosti s politikom informacijske sigurnosti primjenom određenih metrika kao i da je potrebno poboljšati model usklađenosti s politikom informacijske sigurnosti s organizacijskim teorijama.

Procjena stupnja usklađenosti pomaže organizacijama u određivanju njihovog pridržavanja kontrola definiranih u standardima gdje je sukladnost sa standardima koji su međunarodno priznati uobičajena osnova za mjerenje informacijske sigurnosti [41] budući da su organizacije često prisiljene uskladiti se sa zahtjevima vanjske revizije ili regulatornih tijela što znači da njihovo provođenje sigurnosnih politika nije nužno izvedeno iz uvjerenja u važnost sigurnosnih praksi već kao rezultat vanjskih zahtjeva [68]. Tako da, čak i ako je organizacija implementirala sigurnosne politike i procedure za poboljšanje informacijske sigurnosti, nerijetko se događa da su njihov utjecaj i učinkovitost upitni jer usklađenost zaposlenika sa sigurnosnim politikama i procedurama ostaje problematična [151] budući da zaposlenici imaju tendenciju sigurnost informacija smatrati neugodnošću, a nove politike i s njima povezane kontrole dočekati s otporom [68] što dovodi do zaključka da, bez usklađenosti, politike postoje samo na papiru na kojem su ispisani ili u bitovima na kojima su pohranjeni [204].

Najčešći razlozi zbog kojih zaposlenici ne poštuju zahtjeve informacijske sigurnosti uključuju činjenicu da im je ispunjavanje rokova važnije za njihov uspjeh i očuvanje posla od poštivanja zahtjeva sigurnosti koji negativno utječu na njihovu produktivnost te obvezu posluha prema rukovoditeljima (zbog straha da ne padnu u nemilost) ukoliko im oni kažu da učine nešto protiv zahtjeva informacijske sigurnosti [97]. Albrechtsen [205] taj nesrazmjer između onog što je propisano o informacijskoj sigurnosti i radnji zaposlenika objašnjava kombinacijom *nedostatka motivacije* kod zaposlenika, *nedostatka znanja* o tome kako ispravno postupati zbog lošeg upravljanja informacijskom sigurnošću i *sukoba interesa između zahtjeva informacijske*

sigurnosti i funkcionalnosti gdje je mnogim zaposlenicima mnogo kritičnije ako ne mogu raditi nekoliko sati nego osigurati informacijsku sigurnost [205].

Motivacija zaposlenika je ključ učinkovite sigurnosti radi zaštite od ljudi koji su već motivirani za napadanje mreže ili zloupotrebljavanje informacija [97] jer nezainteresiranost zaposlenika za prijetnje informacijske sigurnosti i provođenje koraka potrebnih za ublažavanje prijetnji predstavlja veliku opasnost za sigurnost organizacije [159].

Nepoznavanje definiranih zahtjeva informacijske sigurnosti od strane zaposlenika može se objasniti nedostatkom vremena za proučavanje dokumentacije, nedostatkom informacija o tome gdje je dokumentacija dostupna, nedostatkom poticaja za proučavanje dokumentacije i nedostatkom znanja za razumijevanje uputa [205] zbog čega se još jednom naglašava važnost provedbe sigurnosne edukacije, obuke i podizanja svijesti [77] te potrebe da politike, aktivnosti, incidenti i prakse informacijske sigurnosti trebaju biti vidljivi i neprestano se oglašavati zaposlenicima, po mogućnosti porukama prilagođenim karakteristikama ličnost primatelja poruke [159], kako bi oni mogli donositi odluke koje su u skladu s poželjnim smjerom organizacije [194].

Kada se aktivnosti informacijske sigurnosti sukobljavaju ili otežavaju njihove vlastite zadatke, zaposlenici mogu prepoznati potrebu za poštivanjem politika, no i dalje pokazivati namjere nepoštivanja uslijed činjenice da im je važniji cilj ispunjenje zadataka do poštivanja politika informacijske sigurnosti [194]. Također, zaposlenici pokazuju tendenciju ponašanja u skladu s ponašanjem kolega, što znači da, ako se nečiji suradnici ne pridržavaju sigurnosnih politika organizacije, postoji velika vjerojatnost da će se slično ponašati i ta osoba te svjesno ne slijediti sigurnosne politike [194] zbog čega je važan društveni pritisak od kolega i nadređenih oko naglašavanja važnosti poštivanja politika informacijske sigurnosti. [206], odnosno poboljšanja kulture informacijske sigurnosti koja motivira usklađenost s kolegama [194], [124], [183].

Čak i ako su formalizirane sigurnosne politike i evaluira se usklađenost zaposlenika, ta usklađenost može biti loša ako nema odgovarajuće nagrade za pridržavanje pravila odnosno kazne za nepridržavanje iz čega bi zaposlenici mogli zaključiti da sigurnosne politike nisu važne niti obvezne jer usklađenost ili neusklađenost ne čini razliku [67]. Razumijevanje načina na koji organizacije određuju politike informacijske sigurnosti, kao i vrednuju i nagrađuju ili kažnjavaju pojedince za njihovo postupanje u skladu s politikama ili protivno njima, ima izravan utjecaj na stupanj do kojeg pojedinac vjeruje da su sigurnosne kontrole obavezne [137].

Nagrade i kazne, temeljene na teoriji nagrađivanja ponašanja koja su poželjna („mrkva") i sankcioniranja nepoželjnih ponašanja („batina") [67], tradicionalni su pokretači radnog učinka u poslovanju te su primjenjive i kao sredstvo za motiviranje zaposlenika u svrhu održavanja informacijske sigurnosti [97], [128]. Iz tog razloga, Siponen i suradnici [206] navode kako rukovodstvo mora odrediti sankcije zbog neusklađenosti sa sigurnosnim politikama da bi se poslala jasna poruka zaposlenicima kako će njihova nesukladnost biti otkrivena i podvrgnuta sankcijama. Isti autori navode kako uvođenje nagrada ima zanemariv utjecaj na usklađenost zaposlenika s politikama informacijske sigurnosti. S druge strane, Bulgurcu i suradnici [77], na temelju rezultata svog istraživanja, ističu kako, iako nagrade možda ne tjeraju zaposlenike na vjerovanje da su zahtjevi sigurnosne politike obavezni, one se i dalje mogu koristiti za motiviranje usklađenosti zaposlenika zbog toga što nagrade utječu na percepciju koristi od usklađenosti, a što zauzvrat utječe na odnos zaposlenika prema usklađenosti.

Nagrade za usklađenost sa zahtjevima informacijske sigurnosti mogu uključivati razne materijalne i nematerijalne stavke, od promaknuća, povišice, pohvale i priznanja, novčanih bonusa za uzorno ponašanje i/ili rad, preko slobodnog dana ili besplatnog parkirnog mjesta, do poklon bonova, ulaznica za razna događanja ili sitnih poklona u obliku knjige, USB memorije, MP3 playera i sl. [97], dok moguće sankcije mogu obuhvaćati degradaciju, gubitak povlastica, gubitak ugleda, neplaćeni dopust, ukor, otkaz, novčane ili nenovčane kazne i sl. [77].

Rezultati istraživanja koje su proveli Chen i suradnici [168] sugeriraju da strogost sankcije nema izravnog utjecaja na usklađenost s politikom informacijske sigurnosti te se zaposlenikov izbor usklađenosti ili neusklađenosti s politikom informacijske sigurnosti uglavnom ne temelji na troškovima ili formalnoj kazni, već na neformalnim sankcijama i osobnim sposobnostima [168], a uključivanje krajnjih korisnika u proces razvoja sigurnosne politike može imati značajan utjecaj na njihove stavove prema usklađenosti [207].

Dodatno, rezultati istraživanja koje su proveli Xue i suradnici [202] pokazuju da očekivanje kazne ne utječe na namjeru poštivanja politika već je učinak očekivanja kazne zasjenjen percipiranom pravednošću kazne što ukazuje na to da se zaposlenici odlučuju na usklađenost s obaveznim politikama uglavnom zbog toga što ih smatraju pravednima, dok je očekivanje kazne manja briga. Percepcija zaposlenika o pravičnosti temelji se na njihovoj ocjeni uklapanja između oštrine kazne i nepoželjnog ponašanja gdje se kazna smatra pravednom kad se vidi da je ona primjerena određenom prekršaju koji se kažnjava te na usporedbi kazne nametnute različitim pojedincima koji su počinili slične prekršaje u očekivanju jednakosti u dodjeli kazne.

Ako se kažnjavanje dosljedno primjenjuje za sve zaposlenike neovisno o hijerarhijskom položaju, zaposlenici će razviti percepciju pravednosti [202]. Isti autori navode i da stvarno kažnjavanje smanjuje percepciju pravednosti kazne. Na primjer, ako su zaposlenici kažnjeni, njihova percepcija pravednosti vjerojatno će se smanjiti, što će dovesti do smanjene namjere usklađenosti. Kako zaposlenici postaju sve manje usklađeni, vjerojatno će dobivati više kazni, što će dovesti do začaranog ciklusa u kojem se zaposlenici pretjerano kažnjavaju, ali se njihova percepcija pravednosti i usklađenost nastavljaju pogoršavati zbog čega organizacije trebaju biti oprezne u provođenju kazni [202].

3.5.7. Tehničke mjere

Iako je zadnjih desetak godina napravljen pomak s operativne i taktičke prema strateškoj razini upravljanja informacijskom sigurnošću i povezanim rizicima, a samim time i pomak s tehničkih na organizacijske mjere odnosno kontrole, s posebnim fokusom na ljudski čimbenik, to ne znači da tehničke mjere više nemaju važnu ulogu u informacijskoj sigurnosti [1]. Dapače, tehničke mjere i dalje su primjenjive kao i prije deset godina te bi bez njih danas bili pregaženi od strane raznoraznog „uobičajenog" zlonamjernog softvera [208].

Tehničke mjere ključne su za dobro planirani proces upravljanja informacijskom sigurnošću, posebno za provođenje politike za brojne IT funkcije koje nisu pod izravnom ljudskom kontrolom. Mrežni i računalni sustavi donose milijune odluka svake sekunde, a djeluju na načine i brzinom koju ljudi ne mogu kontrolirati u stvarnom vremenu [28] zbog čega je bitno nastaviti s jačanjem sigurnosnim tehnologija [1]. Ako su pravilno primijenjena, rješenja za tehničke mjere mogu poboljšati sposobnost organizacije za uravnoteženje često sukobljenih ciljeva, kako bi se informacije učinile lako i široko dostupnima i očuvala povjerljivost, dostupnost i integritet informacija [28] što je pokazatelj da su tehnička pitanja i dalje primjenjiva u trenutnom i budućem okruženju informacijske sigurnosti [1].

Tehničke mjere, koje podrazumijevaju automatizaciju i standardizaciju dijelova sustava radi pomoći u operativnim zadacima vezanim uz informacijsku sigurnost mogu se podijeliti na mjere fizičke zaštite informacijske imovine, kao što su npr. sustavi zaštite od požara, alarmni sustavi, fizičke barijere za kontrolu prolaza, sustav video nadzora i sl. i informacijsko-komunikacijske mjere zaštite, kao što su npr. kriptografija, biometrija, izrada sigurnosnih kopija, vatrozidi, antivirusni sustavi, sustavi za otkrivanje/sprečavanje upada u sustav (engl. *Intrusion Detection/Prevension System – IDS/IPS*), mehanizmi autorizacije (engl.

Authorization) i provjere autentičnosti (engl. *Authentication*), mehanizmi zaštite baza podataka i sl. [209], [208], [83].

Budući da cilj ovog rada nije detaljan opis tehničkih mjera informacijske sigurnosti, u nastavku se nalazi samo djelomičan kratki osvrt na neke od temeljnih tehničkih mjera koje su postale neophodne za zaštitu povjerljivosti, integriteta i dostupnosti informacija u današnjem svijetu.

3.5.7.1. Antivirusni sustav (engl. Antivirus)

Antivirusni sustav (engl. *Antivirus*), kao vrsta računalnog softvera koja pokušava prepoznati, spriječiti i ukloniti računalne viruse i druge zlonamjerne programe na mreži, poslužiteljima ili klijentskim računalima, u današnjem je kontekstu postao neophodna zaštita od različitih napada, koji dolaze prije svega s Interneta i od zlonamjernih napadača [35]. Antivirusni sustavi razvijeni su za otkrivanje prisutnosti zlonamjernog softvera, prepoznavanje njegove prirode, njegovo uklanjanje, kao i zaštitu informacijske imovine od budućih zaraza [23]. Potreba za antivirusnim sustavom se dodatno pojačala zbog porasta broja bankarskih/financijskih transakcija koje se prenose putem Interneta [35].

Antivirusni sustav radi na principu da skenira datoteke u potrazi za poznatim virusima koji se podudaraju s definicijama u rječniku virusa i identificira sumnjivo ponašanje iz bilo kojeg računalnog programa koji bi mogao ukazivati na zarazu odnosno prisutnost zlonamjernog kôda. Ako se nađe zaražena datoteka, onemogućuje se njeno pokretanje te se takva datoteka ili premješta na posebno mjesto za daljnji pregled od strane administratora sustava (karantena) ili se jednostavno briše iz sustava [23].

Antivirusni sustav ponekad se naziva i sustav za zaštitu od zlonamjernog softvera (engl. *Antimalware*), a otkrivanje zlonamjernog kôda bi u idealnom slučaju trebalo istovremeno minimizirati lažne pozitivne rezultate (lažni alarmi) i lažne negativne rezultate (propušteni zlonamjerni softver). Uz to, antivirusni sustav suočen je i s drugim teškim izazovima, kao što su činjenica da su taktike zlonamjernog softvera sofisticirane i stalno se razvijaju, da zlonamjerni softver može u potpunosti postojati u memoriji računala bez utjecaja na datoteke, da zlonamjerni softver može napadati antivirusne procese ili da rad antivirusnog sustava može smanjiti performanse računala i time iživcira korisnike koji ga zbog toga isključe [23].

3.5.7.2. Vatrozid (engl. Firewall)

Vatrozid (engl. *Firewall*) je program ili namjenski hardverski uređaj koji provjerava mrežni promet koji prolazi kroz njega i odbija ili dopušta promet na temelju niza pravila definiranih u njegovoj konfiguraciji [23]. Osnovni zadatak vatrozida je regulirati protok prometa između računalnih mreža različitih razina povjerenja [28], na primjer, između lokalne mreže (engl. *Local Area Network – LAN*) i javne mreže (Interneta). Vatrozid kontrolira protok prometa sprječavajući neovlaštene korisnike u pristupanju određenim dijelovima mreže i njenim uslugama iz drugih mreža [23].

Vatrozidi su kritični elementi sigurnosti mreže koji služe kao prijeko potrebno sredstvo odvraćanja, ali oni neće riješiti sve sigurnosne probleme [23] jer kao ni programi protiv zlonamjernog softvera ne mogu otkriti većinu prijevara s ciljem krađe identiteta (*Phishing* prijevare) jer ne sadrže sumnjivi kôd [39].

Vatrozidi gledaju kontrolna pravila po kojima je podatkovni paket ili dopušten ili odbijen odnosno odlučuju treba li paketu dopustiti pristup u pouzdanu mrežu. Da bi provjerio da li je paket u skladu s kontrolnim pravilima, vatrozid samo pregledava zaglavlje TCP/IP protokola i ne provjerava sadržaj podataka mrežnog paketa što znači da, čak i ako podaci sadrže zlonamjerni kôd, vatrozid će dopustiti da taj paket prođe ako je zaglavlje paketa u skladu s pravilima konfiguriranim u vatrozidu. Dakle, organizacija može imati vatrozid, ali njena pouzdana mreža može svejedno biti ugrožena [35].

3.5.7.3. Sustav za otkrivanje/sprečavanje upada (engl. Intrusion Detection/Prevention System - IDS/IPS)

Vatrozid je nužna komponenta cjelokupne topologije mrežnog osiguranja, ali sam po sebi je nedovoljan [35] budući da donose odluke na temelju primarnih atributa prometa, odnosno izvorišne i odredišne IP adrese ili broju porta [83]. **Sustav za otkrivanje/sprečavanje upada** (engl. *Intrusion Detection / Prevention System – IDS/IPS*), kao najsloženiji i najinteligentniji mrežni uređaj, dopunjuje vatrozid pružajući temeljit pregled zaglavlja paketa i njegovog sadržaja, čime štiti od upada, koje vatrozid inače doživljava kao naizgled bezazlen mrežni promet [35]. U ovom kontekstu, upad predstavlja „*nuspojavu u kojoj napadač pokušava ući u informacijski sustav ili poremetiti njegovo normalno djelovanje, gotovo uvijek s namjerom nanošenja štete*" [28].

Otkrivanjem ranih znakova upada organizacija može brzo obuzdati napad i spriječiti ili barem značajno ublažiti gubitak ili štetu informacijskim sredstvima [28] pa tako dobar IDS/IPS sustav predstavlja veliko poboljšanje u odnosu na osnovni vatrozid jer se, između ostalog, može konfigurirati s politikama koje mu omogućuju donošenje autonomnih odluka o tome kako se nositi s otkrivenim prijetnjama - od automatskog odbacivanja (ekstrakcije) sumnjivih paketa i istodobno propuštanje prolaska legitimnih paketa do postavljanja uljeza u „karantenu" [23].

Dakle, IDS/IPS sustav dubinski pregledava sadržaj svakog paketa koji prolazi mrežom kako bi otkrio bilo kakve zlonamjerne aktivnosti, gdje se svaki paket rastavlja do dijela u kojem se nalazi podatkovni sadržaj koji se provjerava radi li se o zlonamjernom kodu, a zatim se paket ponovo sastavlja u izvorni oblik te se paket šalje dalje [35].

Razlika između IDS i IPS sustava je u tome da su IDS sustavi pasivni i idu samo toliko daleko da aktiviraju alarm, ali neće aktivno blokirati mrežni promet [39], odnosno njegovi senzori evidentiraju potencijalnu sumnjivu aktivnost [83] i omogućuju sanaciju problema [23] dok IPS sustav radi isto kao IDS, ali može prekinuti stvarnu sesiju komunikacije, filtrirati po izvornim IP adresama i blokirati pristup ciljanom odredištu [39] odnosno reagiraju na sumnjive aktivnosti automatski izvršavanjem prekidanja veze ili podešavanjem vatrozida kako bi blokirao mrežni promet iz sumnjivog zlonamjernog izvora [23], [83].

Sustavi otkrivanja upada informacijske sigurnosti (IDS sustavi) postali su komercijalno dostupni krajem 1990-ih godina, a trenutno proširenje IDS tehnologije je ugradnja tehnologije za sprečavanje upada koja aktivnim odzivom može spriječiti uspješan upad u organizaciju. Upravo zbog činjenice da rijetko postoji sustav za sprečavanje upada koji nema ujedno i funkciju otkrivanja, nije neuobičajeno koristiti i pojam sustav za otkrivanje i sprečavanje upada (IDPS sustav) [28].

Budući da je primarna svrha IDPS sustava prepoznati i prijaviti upad, postupak obavješćivanja o upadu je kritičan jer, ako organizacija nije obaviještena da je u tijeku sigurnosni upad, IDPS ne ispunjava svoju svrhu [28].

3.5.7.4. Sustav za upravljanje sigurnosnim informacijama i događajima (engl. Security Information and Event Management – SIEM)

Sustavi za upravljanje sigurnosnim informacijama i događajima (engl. *Security Information and Event Management – SIEM*) slični su IDS/IPS sustavima, ali generiraju

upozorenja na temelju analize podataka iz sistemskih zapisa (engl. *Logs*) [35]. SIEM sustavi predstavljaju softverski omogućen pristup združivanju, filtriranju i upravljanju reakcijama na događaje, od kojih se mnogi prikupljaju zapisom aktivnosti IDS/IPS sustava i uređaja za upravljanje mrežom [28].

Sustav za upravljanje sigurnosnim informacijama i događajima (SIEM) pomaže organizacijama u upravljanju eksplozivnim rastom svojih sistemskih zapisa te pruža zajedničku platformu za snimanje i analizu unosa. Organizacije prikupljaju podatke sistemskih zapisa iz izvora kao što su vatrozidi, IDS-ovi i IPS-ovi, web poslužitelji i poslužitelji baza podataka, a SIEM sustav za prikupljanje i analizu uzima podatke iz sistemskih zapisa u bilo kojem obliku u kojem su nastali, s bilo kojeg uređaja koji ih kreiraju i standardiziraju te podatke u uobičajeni format [39].

U idealnom slučaju SIEM sustav može biti izuzetno koristan za forenziku jer može automatski povezati događaje između nekoliko izvora podataka, a zatim izvući relevantne podatke i predstaviti ih korisniku. No, budući da SIEM sustav funkcionira korištenjem podataka iz mnogih drugih izvora, njegova vrijednost ovisi o tome koji se izvori podataka u njega unose, koliko je pouzdan svaki izvor podataka i koliko dobro SIEM može normalizirati podatke i korelirati događaje [23].

3.5.7.5. Autentikacija (engl. Authentication) i autorizacija (engl. Authorization)

Kontrola pristupa, bilo da se radi o fizičkoj ili logičkoj kontroli pristupa, sastoji se od tri osnovna koraka, koji obuhvaćaju identifikaciju, provjeru autentičnosti (autentikaciju) i autorizaciju. **Identifikacija** (engl. *Identification*) podrazumijeva mehanizam kontrole pristupa kojim neprovjereni ili neovlašteni entiteti koji traže pristup resursu pružaju jednoznačnu oznaku kojom su poznati u sustavu [28].

Provjera autentičnosti ili **autentikacija** (engl. *Authentication*) je postupak dokazivanja da je korisnik ono što tvrdi da jest [23] odnosno predstavlja mehanizam kontrole pristupa koji zahtijeva provjeru valjanosti i provjeru točnosti navodnog identiteta subjekta [28]. Dokazivanje da je tvrdnja za identitet korisnika valjana i vjerodostojna zahtijeva neki oblik „dokaza identiteta" gdje taj dokaz može biti nešto što korisnik zna, nešto što korisnik ima ili nešto što korisnik jest [23] gdje snažna provjera autentičnosti zahtijeva najmanje dva mehanizma provjere autentičnosti koja se crpe iz dva različita faktora provjere autentičnosti [28]. Najčešći način provjere autentičnosti je unošenje lozinke ili PIN-a (nešto što korisnik zna), korištenje

tokena i pametnih kartica (nešto što korisnik ima) ili biometrijskih uređaja za skeniranje otiska, mrežnice, lica i sl. (nešto što korisnik jest) [23].

Jednom kada se korisnik identificira i ovlasti, dodjeljuje mu se niz dozvola i privilegija, poznatih kao **autorizacija** (engl. *Authorization*) koji definiraju što može učiniti s informacijom i sustavom [83]. Za razliku od identifikacije, koja zahtijeva neku vrstu korisničkog imena i provjere autentičnosti, koja zahtijeva, primjerice, lozinku, autorizacija, kao mehanizam kontrole pristupa koji predstavlja podudaranje potvrđenog entiteta s popisom informacijske imovine i odgovarajućim razinama pristupa [28], implementirana je u dio sigurnosne politike unutar organizacije [83].

3.5.7.6. Sigurnosna kopija (engl. Backup)

Sigurnosne kopije podataka (engl. *Backup*) prva su obrana od pada sustava, oštećenja podataka, iskorištavanja koja vode do pitanja integriteta podataka i slučajnog gubitka podataka [35]. Kad ništa drugo ne uspije, pogotovo kada su napadači uspješno izmijenili ili izbrisali podatke na načine koje je teško ili nemoguće identificirati, robusne, pouzdane i dostupne sigurnosne kopije će „spasiti dan" jer postavljaju gornju granicu štete koju napadač može napraviti [23]. Sigurnosne kopije podataka omogućuju nastavak rada učinkovitim obnavljanjem podataka i osiguravaju stalnu dostupnost sustava, premda je potrebno određeno vrijeme za obnovu sustava vraćanjem podataka za oštećeni ili srušeni dio sustava [35]. Nažalost, dobre sigurnosne kopije ne pomažu ako najveća šteta dođe od otkrivanja osjetljivih podataka te, zapravo, mogu pogoršati problem ako nisu pohranjene na siguran način [23].

Bez mogućnosti pravodobne izrade sigurnosne kopije i obnavljanja poslužitelja i klijentskih računala, problem koji bi se u kratkom roku mogao riješiti, brzo se može pretvoriti u katastrofu [23]. Najbolji primjer toga je napad ucjenjivačkim softverom (engl. *Ransomware*) nakon čega može biti nemoguće povratiti pristup svojim podacima ako ne postoji održiva sigurnosna kopija.

Iako se zadnjih godina pouzdanost hardverskih i softverskih sustava povećala, još uvijek postoje rizici rušenja hardvera, operacijskog sustava, aplikacija i baza podataka što rezultira gubitkom ili oštećenjem podataka čime dolazimo do zaključka kako je redovita izrada sigurnosne kopije podataka potrebna i danas [35]. Iz tog razloga, trebaju biti uspostavljene procedure izrade sigurnosne kopije koje propisuju način i učestalost izrade sigurnosne kopije i redovito ih ažurirati radi provjere njihove cjelovitosti [23]. Prilikom izrade sigurnosne kopije

može se raditi o *potpunoj sigurnosnoj kopiji* koja podrazumijeva umnožavanje svih datoteka za cijeli sustav, uključujući sve aplikacije, komponente operacijskih sustava i podatke, *diferencijalnoj sigurnosnoj kopiji* koja se odnosi na umnožavanje svih datoteka koje su promijenjene ili dodane od posljednje pune sigurnosne kopije ili *inkrementalnoj sigurnosnoj kopiji* odnosno umnožavanju samo datoteka koje su izmijenjene od prethodne inkrementalne sigurnosne kopije [28].

3.6. Zakoni i norme iz domene informacijske sigurnosti

Područje informacijske sigurnosti složeno je zbog čega je obuhvaćeno s više primjenjivih zakona, smjernica i standarda, a stručnjaci iz domene informacijske sigurnosti koji upravljaju ili uspostavljaju sustav upravljanja informacijskom sigurnošću, sve te propise trebaju uzeti u obzir prilikom razvoja planova i sustava [210].

Cilj ovog poglavlja nije navesti svu postojeću zakonsku regulativu i međunarodne norme, okvire i smjernice, niti bi to bilo izvedivo u okviru ove disertacije, već staviti naglasak na najpoznatije međunarodne standarde primjenjive u cijelom svijetu, ali i spomenuti onu zakonsku regulativu koja se najčešće navodi u istraživanjima vezanim za informacijsku sigurnost, ograničavajući se na Sjedinjene Američke Države i Europsku uniju s posebnim osvrtom na Republiku Hrvatsku.

3.6.1. Zakonska regulativa

Za razliku od etike koja predstavlja društveno prihvatljivo ponašanje, zakoni su formalno usvojena pravila za prihvatljivo ponašanje u modernom društvu. Ključna razlika između zakona i etike je u tome što zakoni imaju autoritet upravljačkog tijela, a etika ne [28].

U nastavku se nalazi kratak opis najcitiranijih zakona u istraživanjima vezanim uz informacijsku sigurnost koji se odnose na Sjedinjene Američke Države i Europsku uniju s posebnim osvrtom na Republiku Hrvatsku.

3.6.1.1. Sjedinjene Američke Države

Popis u nastavku sažima neke dalekosežnije zakone i propise koji nisu nužno svi izravno vezani uz informacijsku sigurnost već i na način na koji organizacije provode IT operacije, ali se zbog svoje prirode najčešće spominju u znanstvenim radovima iz domene informacijske sigurnosti. To se prvenstveno odnosi na Zakon o prenosivosti i odgovornosti zdravstvenog osiguranja,

Zakon o obiteljskim obrazovnim pravima i privatnosti, Savezni zakon o upravljanju informacijskom sigurnošću, Sarbanes-Oxleyjev zakon i Gramm-Leach-Blileyjev zakon.

Zakon o prenosivosti i odgovornosti zdravstvenog osiguranja (engl. *Health Insurance Portability and Accountability Act – HIPAA*) predstavlja skup propisa koji postavljaju pravila za pravilno postupanje s osobnim zdravstvenim podacima [25] zahtijevajući da zdravstvene organizacije provode kontrole sigurnosti i privatnosti kako bi se osigurala privatnost pacijenata [39], bez obzira jesu li podaci u papirnom ili elektroničkom obliku [84].

Zakon o obiteljskim obrazovnim pravima i privatnosti (engl. *Family Educational Rights and Privacy Act – FERPA*) bavi se osiguravanjem privatnosti informacija o obrazovanju učenika. Za učenike mlađe od 18 godina, zakon daje roditeljima posebna prava na uvid u informacije povezane s obrazovanjem njihovog djeteta, no kada učenik napuni 18 godina, ta se prava uglavnom prenose na same učenike [210]. Prema ovom zakonu, škole moraju dobiti pismeno odobrenje roditelja ili punoljetnog učenika prije objavljivanja bilo kakvih podataka sadržanih u evidenciji o obrazovanju [39].

Savezni zakon o upravljanju informacijskom sigurnošću (engl. *Federal Information Security Management Act – FISMA*) prvi je put usvojen 2002. godine, a 2014. godine je izmijenjen i preimenovan u **Savezni zakon o modernizaciji informacijske sigurnosti** (engl. *Federal Information Security Modernization Act*) s istim akronimom FISMA [210] kako bi se ažurirao s modernim prijetnjama, kao i sigurnosnim kontrolama i dobrim praksama [39]. Ovaj zakon zahtijeva od svih saveznih agencije da razviju, dokumentiraju i provode sigurnosni program za sve informacije kojima upravlja agencija. Jedna od odredbi ovog zakona je da se zahtijeva godišnji pregled sigurnosnog programa od strane agencije. Općenito, zahtjevi FISMA-e opisuju ono što mnogi smatraju dobrom praksom u vezi s informacijskom sigurnošću [210].

Sarbanes-Oxleyjev zakon (engl. *Sarbanes-Oxley Act – SOX*) američki je savezni zakon kojim se provode zahtjevi izvješćivanja i interne kontrole elektroničkih sustava financijskog izvještavanja [84]. Primarna svrha ovog zakona bila je regulirati financijsku praksu i korporativno upravljanje uslijed nekoliko javnih financijskih skandala koji su uključivali korporativne prijevare (Enron, WorldCom, Arthur Andersen) [210]. SOX također diktira politike koje se odnose na neovisnost revizora, korporativno upravljanje, procjenu unutarnje

kontrole i poboljšano financijsko izvještavanje [39] te zahtijeva da sve organizacije, bez obzira na veličinu, imaju definiran, vjerodostojan i detaljan plan informacijske sigurnosti [210].

Gramm-Leach-Blileyjev zakon (engl. *Gramm-Leach-Bliley Act – GLBA*) američki je savezni zakon kojim se zahtijeva zaštita privatnih podataka od strane banaka i drugih financijskih institucija [84]. Namjera GLBA-a, koji se usredotočuje na financijske podatke, slična je onoj koju HIPAA čini za zdravstvene informacije [210]. GLBA zahtijeva da financijske institucije pruže svojim klijentima obavijest o privatnosti koja objašnjava koje informacije tvrtka prikuplja o klijentu, gdje se podaci dijele i kako tvrtka štiti te podatke, a ovu obavijest o privatnosti moraju im dati prije sklapanja ugovora o poslovanju [39].

3.6.1.2. Europska unija

Na razini Europske unije postoje tri najznačajnije regulative vezane uz sigurnost informacija, a to su:

- Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (NIS direktiva) s pripadajućom Provedbenom uredbom Komisije (EU) 2018/151 od 30. siječnja 2018. o utvrđivanju pravila za primjenu Direktive (EU) 2016/1148 Europskog parlamenta i Vijeća u odnosu na dodatne specifikacije elemenata koje pružatelji digitalnih usluga moraju uzeti u obzir u upravljanju rizicima kojima je izložena sigurnost njihovih mrežnih i informacijskih sustava i parametara za utvrđivanje ima li incident znatan učinak,
- Uredba (EU) 2016/679 Europskog parlamenta i Vijeća o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) te
- Uredba (EU) 2019/881 Europskog parlamenta i Vijeća o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti).

Direktiva o sigurnosti mrežnih i informacijskih sustava - NIS direktiva (engl. *Networks and Information Security (NIS) Directive*) [211] definira ključne sektore (energetika, transport, bankarstvo, infrastrukture financijskog tržišta, zdravstveni sektor, opskrba i distribucija vode, digitalna infrastruktura) za koje je potrebno postići jednako visoku razinu sigurnosti mrežnih i

informacijskih sustava u cijeloj Europskoj uniji razvojem nacionalnih sposobnosti kibernetničke sigurnosti, jačanjem suradnje na razini EU-a i obvezivanjem operatora ključnih usluga i pružatelja digitalnih usluga na izvješćivanje o incidentima te donosi preporuke za pružatelje digitalnih usluga (internetsko tržište, internetske tražilice, usluge računalstva u oblaku) koje je potrebno uskladiti u okviru država članica. NIS direktiva je usvojena 2016. godine te ju je trebalo do svibnja 2018. godine prenijeti u nacionalni zakon. To je zahtijevalo od država članica: usvajanje nacionalne strategije kibernetičke sigurnosti, određivanje jednog ili više nacionalnih nadležnih tijela s potrebnim ovlastima za procjenu i provedbu usklađenosti, određivanje jednog ili više timova odgovornih za odgovor na incidente računalne sigurnosti (engl. *Computer Security Incident Response Teams - CSIRT*) za praćenje prijetnji, odgovaranje na incidente i sudjelovanje u CSIRT mreži Europske unije te sudjelovanje u novoj grupi suradnje, koja podupire stratešku suradnju i razmjenu informacija između država članica [212].

Opća uredba o zaštiti podataka (engl. *General Data Protection Regulation - GDPR*) [213] pravni je akt kojim se građanima Europske unije omogućava bolja kontrola nad njihovim osobnim podacima. Uredbom se ojačavaju postojeća prava, ali i omogućuju nova. Definirana su tzv. prava ispitanika koja, između ostalog, uključuju: lakši pristup svojim podacima, uključujući pružanje više informacija o tome kako se ti podaci obrađuju i garanciju da su te informacije dostupne na jasan i razumljiv način; pravo na prenosivost podataka, čime se olakšava prijenos osobnih podataka između dva pružatelja usluge; pravo na brisanje („pravo na zaborav"), koje omogućuje brisanje podataka u slučaju kada pojedinac više ne želi da se njegovi podaci obrađuju i ne postoji zakonski razlog za zadržavanje podataka.

Aktom o kibersigurnosti (engl. *Cybersecurity Act*) [214] daje se Agenciji Europske unije za kibersigurnost (ENISA) snažna operativna uloga u borbi protiv računalnih prijetnji i napada. Ovim aktom uspostavljen je i novi europski program kibersigurnosne certifikacije, postupak kojim se učvršćuje sigurnost internetskih usluga i potrošačkih uređaja, čime se ističe važnost certificiranja ključne infrastrukture, proizvoda, procesa i usluga, odnosno kontrolira kibersigurnost proizvoda i usluga koje se prodaju u Europskoj uniji.

3.6.1.3. Republika Hrvatska

U Republici Hrvatskoj postoji niz zakonskih i podzakonskih akata koji se tiču informacijske sigurnosti, od koji su najznačajniji Zakon o informacijskoj sigurnosti s pripadajućom uredbom, Zakon o tajnosti podataka s pripadajućom uredbom, Zakon o zaštiti tajnosti podataka, Zakon o

provedbi opće uredbe o zaštiti podataka te Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga zajedno s pripadajućom uredbom.

Zakon o informacijskoj sigurnosti (NN 79/07) [215] utvrđuje pojam informacijske sigurnosti, mjere i standarde informacijske sigurnosti, područja informacijske sigurnosti, te nadležna tijela za donošenje, provođenje i nadzor mjera i standarda informacijske sigurnosti, a primjenjuje se na državna tijela, tijela jedinica lokalne i područne (regionalne) samouprave te na pravne osobe s javnim ovlastima, koje u svom djelokrugu koriste klasificirane i neklasificirane podatke.

Zakon o tajnosti podataka (NN 79/07, 86/12) [216] utvrđuje pojam klasificiranih i neklasificiranih podataka, stupnjeve tajnosti, postupak klasifikacije i deklasifikacije, pristup klasificiranim i neklasificiranim podacima te njihovu zaštitu i nadzor nad provedbom, a primjenjuje se na državna tijela, tijela jedinica lokalne i područne (regionalne) samouprave, pravne osobe s javnim ovlastima te pravne i fizičke osobe koje, u skladu s ovim zakonom, ostvare pristup ili postupaju s klasificiranim i neklasificiranim podacima.

Zakon o zaštiti tajnosti podataka (NN 108/96) [217] prestao je važiti 06.08.2007. stupanjem na snagu Zakona o tajnosti podataka (NN 79/07, 86/12), osim odredaba glave 8. i 9. koje se odnose na poslovnu i profesionalnu tajnu.

Zakon o provedbi Opće uredbe o zaštiti podataka (NN 42/18) [218] pravni je akt kojim se osigurava provedba Uredbe (EU) 2016/679 (GDPR), propisuju visine novčanih kazni za kršenje odredbi vezanih za zaštitu osobnih podataka te ujedno definira Agencija za zaštitu osobnih podataka (AZOP) kao nadležno nacionalno tijelo za zaštitu osobnih podataka uz detaljno raspisivanje njenih ovlasti, uloga i odgovornosti.

Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/18) [219] predstavlja prenošenje NIS direktive u nacionalno zakonodavstvo na način da je ovaj zakon utvrdio odgovorna tijela na nacionalnoj i sektorskim razinama, rad tijela odgovornih za odgovor na incidente računalne sigurnosti (engl. *Computer Security Incident Response Teams - CSIRT*) te propisao minimalne sigurnosne standarde i obveze izvješćivanja u slučajevima značajnih incidenata. Republika Hrvatska je, uz sedam definiranih sektora u NIS direktivi (energetika, transport, bankarstvo, infrastrukture financijskog tržišta, zdravstveni sektor, opskrba i distribucija vode, digitalna infrastruktura) prepoznala i dodatni, osmi sektor, koji se odnosi na poslovne usluge za državna tijela. Također, ovaj zakon obuhvaća i preporuke

za pružatelje digitalnih usluga koje se odnose na internetsko tržište, internetske tražilice i usluge računalstva u oblaku.

3.6.2. Međunarodne norme i okviri

Postoje razne prednosti koje vrijedi razmotriti iz različitih normi (engl. *Standards*) i okvira (engl. *Framework*s) koji se mogu primijeniti po pitanju informacijske sigurnosti u organizaciji:

- norme se mogu koristiti kako bi se klijentima pokazalo da organizacija ozbiljno razmišlja o sigurnosti,
- norme mogu omogućiti bolju koordinaciju organizacijskih promjena za sve dionike, jer će implementacija norme često nametati usklađivanje svih zaposlenika,
- norme se mogu nametnuti i kao preduvjet podizvođačima i dobavljačima kako bi se ojačala sigurnost lanca opskrbe u organizaciji,
- proizvodi i usluge koji su certificirani u skladu sa sigurnosnim standardima mogu steći konkurentsku prednost jer će se klijenti uvijek osjećati sigurni u njihovu opskrbu
- norme mogu pomoći organizaciji da njene interne sigurnosne kontrole i procesi budu u skladu s partnerima, kupcima i zakonodavstvom, čineći poslovanje lakšim na različitim tržištima [25].

Norme su vrlo korisne i mogu pomoći u definiranju opsega djelovanja, ali je u konačnici na upravi, rukovodstvu i voditelju informacijske sigurnosti da nađu najbolji način za vođenje i nadzor programa informacijske sigurnosti tako da je prilagođen specifičnim potrebama pojedine organizacije [57].

Norme se razlikuju u pristupima na koji predstavljaju preporuke pa tako američki Nacionalni institut za standarde i tehnologiju (engl. *National Institute of Standards and Technology - NIST*) predstavlja i sistematizira katalog kontrola, međunarodna serija ISO/IEC 27000 više je procesno orijentirana u razvoju sustava za upravljanje informacijskom sigurnošću, PCI DSS norma predstavlja standard zaštite podataka vezano za kartično plaćanje, a COBIT opisuje kontrolne ciljeve informacijske tehnologije [57]. Više o ovim normama dano je u nastavku.

ISO/IEC 27000 serija normi predstavlja niz uputa i dobrih praksi koje je propisala Međunarodna organizacija za standardizaciju (engl. *International Organization for Standardization - ISO*), prvenstveno za uspostavu i održavanje sustava za upravljanje informacijskom sigurnošću (engl. *Information Security Management System – ISMS*) u

organizaciji, ali ne ograničavajući se isključivo u tu svrhu. U spomenutoj seriji postoji nekoliko desetaka normi, kao što je vidljivo u Tablici 3.3., a neke od najvažnijih za spomenuti su ISO/IEC 27001:2013 Zahtjevi za sustav upravljanja informacijskom sigurnošću, ISO/IEC 27002:2013 Kodeks dobre prakse za kontrole informacijske sigurnosti, ISO/IEC 27005:2018 Upravljanje rizicima informacijske sigurnosti ili ISO/IEC 27014:2013 Korporativno upravljanje informacijskom sigurnošću.

Tablica 3.3. Serija normi ISO/IEC 27000

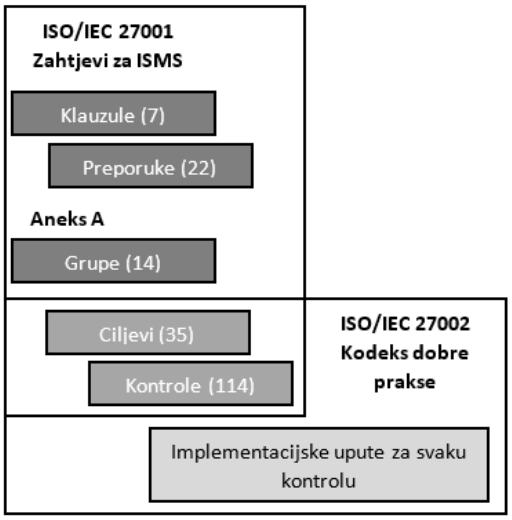
Naziv norme	Opis norme
ISO/IEC 27000:2018	Information security management systems — Overview and vocabulary
ISO/IEC 27001:2013	Information security management systems — Requirements
ISO/IEC 27002:2013	Code of practice for information security controls
ISO/IEC 27003:2017	Information security management systems — Guidance
ISO/IEC 27004:2016	Information security management — Monitoring, measurement, analysis and evaluation
ISO/IEC 27005:2018	Information security risk management
ISO/IEC 27006:2015	Requirements for bodies providing audit and certification of information security management systems
ISO/IEC 27007:2020	Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing
ISO/IEC 27009:2020	Information security, cybersecurity and privacy protection — Sector-specific application of ISO/IEC 27001 — Requirements
ISO/IEC 27010:2015	Information security management for inter-sector and inter-organizational communications
ISO/IEC 27011:2016	Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations
ISO/IEC 27013:2015	Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
ISO/IEC 27014:2013	Governance of information security
ISO/IEC 27017:2015	Code of practice for information security controls based on ISO/IEC 27002 for cloud services
ISO/IEC 27018:2019	Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
ISO/IEC 27019:2017	Information security controls for the energy utility industry
ISO/IEC 27021:2017	Competence requirements for information security management systems professionals
ISO/IEC 27031:2011	Guidelines for information and communication technology readiness for business continuity
ISO/IEC 27032:2012	Guidelines for cybersecurity
ISO/IEC 27033-1:2015	Network security — Part 1: Overview and concepts
ISO/IEC 27033-2:2012	Network security — Part 2: Guidelines for the design and implementation of network security

Tablica 3.3. Serija normi ISO/IEC 27000 (nastavak)

Naziv norme	Opis norme
ISO/IEC 27033-3:2010	Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues
ISO/IEC 27033-4:2014	Network security — Part 4: Securing communications between networks using security gateways
ISO/IEC 27033-5:2013	Network security — Part 5: Securing communications across networks using Virtual Private Networks (VPNs)
ISO/IEC 27033-6:2016	Network security — Part 6: Securing wireless IP network access
ISO/IEC 27034-1:2011	Application security — Part 1: Overview and concepts
ISO/IEC 27034-2:2015	Application security — Part 2: Organization normative framework
ISO/IEC 27034-3:2018	Application security — Part 3: Application security management process
ISO/IEC 27034-5:2017	Application security — Part 5: Protocols and application security controls data structure
ISO/IEC 27034-6:2016	Application security — Part 6: Case studies
ISO/IEC 27034-7:2018	Application security — Part 7: Assurance prediction framework
ISO/IEC 27035-1:2016	Information security incident management — Part 1: Principles of incident management
ISO/IEC 27035-2:2016	Information security incident management — Part 2: Guidelines to plan and prepare for incident response
ISO/IEC 27036-1:2014	Information security for supplier relationships — Part 1: Overview and concepts
ISO/IEC 27036-2:2014	Information security for supplier relationships — Part 2: Requirements
ISO/IEC 27036-3:2013	Information security for supplier relationships — Part 3: Guidelines for information and communication technology supply chain security
ISO/IEC 27036-4:2016	Information security for supplier relationships — Part 4: Guidelines for security of cloud services
ISO/IEC 27037:2012	Guidelines for identification, collection, acquisition and preservation of digital evidence
ISO/IEC 27038:2014	Specification for digital redaction
ISO/IEC 27039:2015	Selection, deployment and operations of intrusion detection and prevention systems (IDPS)
ISO/IEC 27040:2015	Storage security
ISO/IEC 27041:2015	Guidance on assuring suitability and adequacy of incident investigative method
ISO/IEC 27042:2015	Guidelines for the analysis and interpretation of digital evidence
ISO/IEC 27043:2015	Incident investigation principles and processes
ISO/IEC 27050-1:2019	Electronic discovery — Part 1: Overview and concepts
ISO/IEC 27050-2:2018	Electronic discovery — Part 2: Guidance for governance and management of electronic discovery
ISO/IEC 27050-3:2020	Electronic discovery — Part 3: Code of practice for electronic discovery
ISO/IEC 27102:2019	Information security management — Guidelines for cyber-insurance
ISO/IEC 27701:2019	Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

Izvor: *vlastiti prikaz na temelju popisa normi s https://www.iso.org/ics/35.030/x/*

Dvije najpoznatije norme iz ISO 27000 serije su svakako ISO/IEC 27001 i ISO/IEC 27002 koje su komplementarne na način da se ISO/IEC 27001 može koristiti za certificiranje sustava za upravljanje informacijskom sigurnošću gdje norma sadrži sedam klauzula i 22 preporuke te u Aneksu navodi 14 grupa predloženih sigurnosnih kontrola za zadovoljenje preporuka, a ISO/IEC 27002, kao kodeks dobre prakse za sigurnosne kontrole raspisuje tih 14 grupa kontrola i pruža implementacijske upute za svaku od 114 kontrola koliko je ukupno kontrola raspoređeno u tih 14 grupa. Odnos ove dvije norme vidljiv je na Slici 3.3.



Slika 3.3. Odnos međunarodnih normi ISO/IEC 27001 i ISO/IEC 27002.
Izvor: *prilagođeno prema* [57]

Ovdje je bitno za napomenuti kako poštivanje same norme (uključujući i certifikaciju po ISO/IEC 27001) samo po sebi ne jamči odgovarajuću sigurnost. Međutim, uspostavljanjem temeljnih procesa informacijske sigurnosti na temelju normi, voditelj informacijske sigurnosti može bolje upravljati složenošću, poboljšati komunikaciju i uvjeriti dionike [57].

Norma ISO/IEC 27014 objavljena 2013. godine posvećena je u potpunosti korporativnom upravljanju informacijskom sigurnošću te u svom sažetku, podsjeća na važnost dobrog korporativnog upravljanja ne samo da bi se osiguralo poštovanje zakonskih i regulatornih okvira, već i sačuvala imovina i ugled organizacije [57].

Iako nisu dio serije ISO/IEC 27000, norme ISO 31000 i ISO/IEC 31010, uz ISO/IEC 27005, također se mogu koristiti u upravljanju rizicima informacijske sigurnosti. Dok se ISO/IEC 27005 usredotočuje na specifičnosti upravljanja rizicima informacijske sigurnosti, ISO 31000 pruža izvrstan temelj za općenitu procjenu rizika u organizaciji, a ISO/IEC 31010 obuhvaća

različite tehnike upravljanja rizikom, spuštanjem na sljedeću razinu prema referentnom modelu procesa [25]. Međutim, prilikom korištenja ISO 31000 za upravljanje rizicima informacijske sigurnosti potrebno je imati na umu da postoje nijanse upravljanja informacijskim rizicima jer svaki rizik može imati višestruke ocjene iz različitih perspektiva (ovisno o tome utječe li modelirani utjecaj na povjerljivost, integritet i/ili dostupnost) pa sve ovo treba uzeti u obzir u procesu upravljanja rizicima. Druga glavna razlika je kontinuirano ocjenjivanje iterativnog postupka koji slijedi upravljanje rizikom informacijske sigurnosti [25].

U konačnici, još jedna norma koja nije dio ISO/IEC 27000 serije, ali je vrlo usko povezana s informacijskom sigurnošću je ISO 22301: 2012, kao daleko najbolja norma za upravljanje kontinuitetom poslovanja koja je stvorena kako bi omogućila voditeljima kontinuiteta poslovanja da naprave plan koji odgovara veličini i složenosti organizacije, tako da ispunjava svrhu bilo da se radi o maloj tvrtki ili velikoj korporaciji [25].

Nacionalni institut za standarde i tehnologiju (engl. *National Institute for Standards and Tehnology – NIST*) razvio je NIST Okvir za kibernetičku sigurnost (engl. *NIST Cybersecurity Framework*), koji je prvi put objavljen 2014. godine kao odgovor na izvršni nalog američkog predsjednika koji zahtijeva povećanu kibernetičku sigurnost. Okvir je usredotočen na komponente kritične infrastrukture, ali je primjenjiv na mnoge opće sustave. Smjernice nude strukturiranu metodu za osiguranje sustava koji mogu pomoći revizorima uskladiti poslovne pokretače i sigurnosne zahtjeve [39].

NIST također objavljuje niz posebnih publikacija koje pokrivaju mnoge aspekte informacijskih sustava, gdje je trenutan broj posebnih publikacija 160 komada, u finalnoj verziji[7]. Neke od tih posebnih publikacija su NIST Special Publication (SP) 800-12 koja se odnosi na uvod u računalnu sigurnost, NIST SP 800-53 koja sadrži cjelokupnu listu sigurnosnih kontrola, NIST SP 800-39 za upravljanje rizicima informacijske sigurnosti, NIST SP 800-61 dediciranu odgovorima na incidente ili NIST SP 800-50 koja se bavi sigurnosnim osvješćivanjem i obukom.

Upravo je NIST-ova posebna publikacija 800-50 *Izgradnja programa osviještenosti i obuke o sigurnosti informacijske tehnologije* jedno od najboljih sveobuhvatnih objašnjenja o tome kako treba graditi program osvješćivanja o sigurnosti, s fokusom na kontinuirano jačanje poruka programa tijekom čitave karijere zaposlenika. Dokument navodi četiri koraka koji se smatraju

[7] Popis posebnih publikacija dostupan je na adresi: https://csrc.nist.gov/publications/sp800; učitano 05.05.2020.

ključnim za uspjeh programa podizanja svijesti, a to su dizajn (potrebno je izraditi potpunu procjenu organizacije i razviti strategiju obuke koja se šalje rukovoditeljima na odobrenje), razvoj materijala za obuku i osvješćivanje (potrebno je izraditi sav sadržaj radnih materijala potreban za cijeli program), implementacija (potrebno je upoznati zaposlenike s važećim materijalom za obuku i osvješćivanje osiguravajući da ga prati sveobuhvatan plan komunikacije koji svima objašnjava svrhu) te post implementacija (potrebno je održavati sadržaj aktualnim i prikupljati povratne informacije te ih neprestano prilagođavati i poboljšavati kako bi se osiguralo da zaposlenici ostanu angažirani, a program aktualan i relevantan [25].

Standard zaštite podataka industrije platnih kartica (engl. *Payment Card Industry Data Security Standard – PCI DSS*) sveobuhvatan je sigurnosni standard koji uključuje zahtjeve za upravljanje sigurnošću, politikama, procedurama, mrežnom arhitekturom, dizajnom softvera i drugim kritičnim zaštitnim mjerama [39], a koji je nastao kako bi se zaštitili korisnici platnih kartica od prijevara i preduhitrili zakonski zahtjevi prema industriji platnih kartica [39].

PCI DSS jedinstven je jer nije pravni zahtjev ili propis, nego vlasnički standard koji je razvila sama industrija platnih kartica [210] i to zajedničkim naporima industrijskih tvrtki koje uključuju American Express, Visa, Discover Financial Services, JCB i MasterCard Worldwide [28]. Standard se odnosi na sve organizacije koje sudjeluju u bilo kojem od procesa koji se tiču obrade platnih kartica, a usklađenost s PCI DSS standardom obvezno je za sve tvrtke koje obrađuju, pohranjuju ili prenose podatke vlasnika kartica [39].

Trenutno važeća verzija je 3.2.1. objavljena u svibnju 2018. godine, a suština PCI-DSS okvira je specifikacija od 12 zahtjeva za usklađenost najviše razine, podijeljenih u šest skupina, koje se nazivaju kontrolni ciljevi. Ti kontrolni ciljevi su: izgraditi i održavati sigurnu mrežu i sustave, zaštititi podatke vlasnika kartica, održavati program upravljanja ranjivostima, implementirati snažne mjere kontrole pristupa, redovito nadgledati i testirati mreže te održavati politiku informacijske sigurnosti [220]. Kao što se vidi, ovaj popis kontrolnih ciljeva je prilično sveobuhvatan, iako na izuzetno visokoj razini, ali ako je svako od tih kontrolnih područja pravilno dizajnirano i upravljano, tada bi podaci s kartica klijenta trebali biti sigurni [25].

Kontrolni ciljevi informacijske i srodne tehnologije (engl. *Control Objecitioves of Information and related Technology – COBIT*) okvir je koji nije ograničen na sigurnost informacija već se odnosi na, kako mu i samo ime kaže, kontrolne ciljeve za IT. Prva verzija COBIT-a datira iz 1996. dok je posljednja verzija, pod nazivom COBIT 2019, objavljena 2018.

godine. Zadnja verzija, COBIT 2019 sadrži 40 kontrolnih (odnosno korporativnih i upravljačkih) ciljeva tj. procesa organiziranih u pet domena (jednoj strateškoj i četiri operativne) [221].

Korporativna domena **evaluacija, usmjeravanje i nadzor** (engl. *Evaluate, Direct and Monitor*) odnosi se na procjenu strateških opcija i usmjeravanje višeg rukovodstva na odabrane strateške opcije i praćenje postizanje strategije. Upravljačke domene su **usklađivanje, planiranje i organiziranje** (engl. *Align, Plan and Organize*) koja se odnosi na cjelokupnu organizaciju, strategiju i prateće aktivnosti za IT, **izgradnja, nabavka i implementacija** (engl. *Build, Acquire and Implement*) koja obuhvaća definiciju, stjecanje i primjenu IT rješenja i njihovu integracija u poslovne procese, **isporuka, usluga i podrška** (engl. *Deliver, Service and Support*) koja se bavi operativnom isporukom i podrškom IT uslugama, uključujući sigurnost te **nadzor, evaluacija i procjena** (engl. *Monitor, Evaluate and Assess*) koja se bavi nadzorom performansi i usklađenosti IT-a s internim ciljevima izvedbe, ciljevima unutarnje kontrole i vanjskim zahtjevima [222].

Za razliku od prethodne verzije (COBIT 5) koja se temeljila na pet temeljnih načela: ispunjavanje potreba dionika, obuhvaćanje organizacije od kraja do kraja, primjena jednstvenog integriranog okvira, omogućavanje holističkog pristupa i odvajanje strateškog od operativnog upravljanja [25], COBIT 2019 temelji se na šest upravljačkih načela: omogućavanje vrijednosti dionicima, holistički pristup, dinamični sustav upravljanja, strateško upravljanje razdvojeno od operativnog, prilagođenost potrebama organizacije, sustav strateškog upravljanja od kraja do kraja organizacije [221].

3.7. Kritična nacionalna infrastruktura

U današnje vrijeme, kad su napadi na povjerljivost, integritet i dostupnost organizacija i njihovu informacijsku imovinu, uslijed globalne umreženosti, postale svakodnevica, ti napadi posebno dolaze do izražaja kod tzv. *kritične infrastrukture,* gdje nedostupnost kritične infrastrukture može imati ekonomski utjecaj daleko izvan sustava na koji se odnosila izravna i fizička šteta, što znači da nestanak kritične nacionalne infrastrukture može dovesti do velikih poremećaja u društvu i gospodarstvu [223] na lokalnoj, regionalnoj, nacionalnoj ili čak i globalnoj razini [114].

Koncept kritične (nacionalne) infrastrukture pojavio se u javnosti sredinom devedesetih godina 20. stoljeća, kada su Sjedinjene Američke Države počele priznavati kako postoji skup objekata

i usluga okupljenih za pružanje funkcija koje su bile 'kritične' za vođenje zemlje i dobrobit njezinih građana [224]. Međunarodna organizacija za standardizaciju (ISO) definira kritičnu infrastrukturu kao „*skup organizacija i objekata koji su nužni za funkcioniranje društva i gospodarstva u cjelini*" [225] dok Vijeće Europske unije u Direktivi 2008/114/EZ o utvrđivanju i označivanju europske kritične infrastrukture i procjeni potrebe poboljšanja njezine zaštite (Direktiva 2008/114/EZ) [226] proširuje tu definiciju i navodi kako kritičnu infrastrukturu čini „*imovina, sustav ili njihov dio koji se nalazi u državama članicama i neophodan je za održavanje vitalnih društvenih funkcija, zdravlja, sigurnosti, zaštite, gospodarske i socijalne dobrobiti ljudi, čiji bi poremećaj rada ili čije bi uništenje, kao posljedica neuspjelog održavanja tih funkcija, moglo imati znatan učinak u državi članici*".

Referenciranje na pojedinu državu članicu u ovoj definiciji ujedno objašnjava zašto se često kritična infrastruktura naziva i kritična *nacionalna* infrastruktura, budući da se tu radi o elementima koji su toliko bitni da bi nedostupnost ili uništenje takve infrastrukture, sustava ili imovine imalo značajan utjecaj na nacionalnu sigurnost, nacionalnu ekonomsku sigurnost, nacionalno zdravlje ili zaštitu ili bilo koju kombinaciju tih pitanja [119] što je u skladu s definicijom nacionalne kritične infrastrukture hrvatskog Zakona o kritičnim infrastrukturama (NN 56/13) [227] koji navodi kako su to „*sustavi, mreže i objekti od nacionalne važnosti čiji prekid djelovanja ili prekid isporuke roba ili usluga može imati ozbiljne posljedice na nacionalnu sigurnost, zdravlje i živote ljudi, imovinu i okoliš, sigurnost i ekonomsku stabilnost i neprekidno funkcioniranje vlasti*".

Spomenuta Direktiva 2008/114/EZ [226] prepoznaje dva kritična sektora koji čine energetika i prijevoz, dok različite države u svijetu prepoznaju različit broj sektora koji čine kritičnu nacionalnu infrastrukturu gdje sektori odnosno vrste organizacija koje su uključene u popise kritičnih objekata i usluga variraju, ali uglavnom se vidi slaganje oko toga da su informacijska i komunikacijska tehnologija (ICT), energetika, financijski sektor, opskrba hranom, vodno gospodarstvo, zdravstvo i prometni sustav prepoznati kao kritična nacionalna infrastruktura (Tablica 3.4.).

Tablica 3.4. Kritična nacionalna infrastruktura pet odabranih država

	UK	Njemačka	SAD	Kanada	Hrvatska
1.	Komunikacijske usluge	ICT	Komunikacijske usluge	ICT	Komunikacijska i informacijska tehnologija
2.	Hitne službe	Hitne i spasilačke službe	Hitne službe		Javne službe
3.	Energetika	Energetika	Energetika	Energetika i komunalije	Energetika
4.	Financijske usluge	Financijske usluge	Financijske usluge	Financijske usluge	Bankarstvo
5.	Hrana	Hrana	Hrana i poljoprivreda	Hrana	Hrana
6.	Državna uprava	Državna uprava	Objekti državne uprave	Državna uprava	
7.	Zdravstvo	Javno zdravstvo	Javno zdravstvo	Zdravstvo	Zdravstvo
8.	Promet	Promet	Promet	Promet	Promet
9.	Voda	Opskrba vodom i kanalizacija	Sustavi opskrbe vodom i kanalizacije	Voda	Vodno gospodarstvo
10.	Obrana		Obrambene industrijske baze		
11.	Civilni nuklearni sektor		Nuklearni reaktori, materijal i otpad		
12.	Kemijska industrija		Kemijska industrija		Proizvodnja, skladištenje i prijevoz opasnih tvari
13.	Svemirska industrija				
14.		Objekti kulturne baštine			Nacionalni spomenici i vrijednosti
15.			Kritična proizvodnja	Proizvodnja	
16.			Informacijska tehnologija		
17.			Poslovni objekti		
18.			Brane		
19.				Zaštita	
20.					Znanost i obrazovanje
∑	**13**	**10**	**16**	**10**	**11**

Izvor: *vlastiti prikaz na temelju* [228], [229], [230], [231], [227], [232]

Republika Hrvatska Zakonom o kritičnim infrastrukturama (NN 56/13) [227] definirala je deset sektora koji čine kritičnu nacionalnu infrastrukturu (energetika, komunikacijska i informacijska tehnologija, promet, zdravstvo, vodno gospodarstvo, hrana, financije, proizvodnja, skladištenje i prijevoz opasnih tvari, javne službe, nacionalni spomenici i vrijednosti), a Odlukom o određivanju sektora iz kojih središnja tijela državne uprave identificiraju nacionalne kritične infrastrukture te liste redoslijeda sektora kritičnih infrastruktura (NN 108/2013) [232] Vlada Republike Hrvatske dodatno je prepoznala sektor znanosti i obrazovanja kao element kritične nacionalne infrastrukture što u konačnici daje 11 sektora kritične nacionalne infrastrukture (Tablica 3.5.).

Međutim, provedba Zakona o kritičnim infrastrukturama nije zaživjela u opsegu za željeni napredak po pitanju zaštite kritične infrastrukture, budući da je, iako je Vlada Republike

Hrvatske svojom odlukom definirala kritične nacionalne sektore, izostala identifikacija konkretnih infrastruktura u tim sektorima te samim tim i određivanje dodatnih sigurnosnih zahtjeva prema istima [233]. Identifikacija konkretnih organizacija koje čine kritičnu nacionalnu infrastrukturu iz pojedinog sektora djelomično je riješena donošenjem Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/18) [219] te pripadajućom Uredbom (NN 68/18) [234], ali u manje sektora nego što ih je definirao Zakon o kritičnim infrastrukturama [235], kao što prikazuje Tablica 3.5.. Zakon o kibernetičkoj sigurnosti nastao je na temelju Direktive o sigurnosti mrežnih i informacijskih sustava (NIS direktiva) [211] koja propisuje sedam sektora operatora ključnih usluga koji uključuju energetiku, prijevoz, bankarstvo, infrastrukture financijskog tržišta, zdravstveni sektor, opskrbu vodom za piće i njezinu distribuciju te digitalnu infrastrukturu, dok je Republika Hrvatska, kao osmi sektor, u nacionalni zakon dodala poslovne usluge za državna tijela.

Tablica 3.5. Kritični sektori u Republici Hrvatskoj

	Zakon o kritičnim infrastrukturama (NN 56/13)	**Odluka Vlade Republike Hrvatske (NN 108/2013)**	**Zakon o kibernetičkoj sigurnosti (NN 64/18)**
Sektor	Energetika	Energetika	Energetika
	Komunikacijska i informacijska tehnologija	Komunikacijska i informacijska tehnologija	Digitalna infrastruktura
	Promet	Promet	Prijevoz
	Zdravstvo	Zdravstvo	Zdravstveni sektor
	Vodno gospodarstvo	Vodno gospodarstvo	Opskrba vodom za piće i njezina distribucija
	Hrana	Hrana	
	Financije	Financije	Bankarstvo
	Proizvodnja, skladištenje i prijevoz opasnih tvari	Proizvodnja, skladištenje i prijevoz opasnih tvari	
	Javne službe	Javni sektor	
	Nacionalni spomenici i vrijednosti	Nacionalni spomenici i vrijednosti	
		Znanost i obrazovanje	
			Infrastrukture financijskog tržišta
			Poslovne usluge za državna tijela
Ukupno	**10**	**11**	**8**

Izvor: *vlastiti prikaz na temelju* [227], [232], [219]

Kibernetički napadi na kritičnu nacionalnu infrastrukturu koji se mogu provoditi za financijsku dobit (npr. putem otkupnine), radi manipuliranja javnim mišljenjem, kako bi se pokazala snaga

i sposobnosti napadača, provela špijunaža ili jednostavno uzrokovale fizičke smetnje u radu [212], postali su nova norma u sektorima kao što su energetika, zdravstvena zaštita ili promet, a koliki je značaj tih napada, govori i činjenica kako je Svjetski gospodarski forum (World Economic Forum) kibernetičke napade na kritičnu infrastrukturu ocijenio petim najvišim rizikom za 2020. godinu [236]. Kibernetički napadi mogu iskoristiti tehničke ranjivosti u računalnim sustavima ili nedostatak svijesti među ljudima koji koriste računalne sustave, međutim, ovi napadi često ciljaju oboje [212].

Neki od najrazornijih kibernetičkih napada koje smo mogli vidjeti tijekom posljednjih nekoliko godina pokazuju dobru usklađenost modernih oblika kibernetičkog kriminala sa tradicionalnim kriminalom [25], a slučajevi napada na iransku nuklearnu elektranu ili ukrajinsku elektroenergetsku mrežu među nepoznatijim su kibernetičkim napadima na kritičnu infrastrukturu u svijetu.

Prvo izoliran sredinom lipnja 2010. godine, Stuxnet maliciozni softver koji je posebno dizajniran za napad na industrijska računala sa Windows operacijskim sustavom i preuzimanje kontrole nad programirljivim logičkim upravljačima (engl. *Programmable Logic Controller - PLC*) [114], korišten je za napad na PLC sustav iranskog nuklearnog programa te se smatra jednim od najuspješnijih industrijskih napada u povijesti kibernetičkih napada [29]. Općenito pripisan američkim i izraelskim obavještajnim agencijama, Stuxnet maliciozni softver uspio je uništiti centrifuge u iranskoj nuklearnoj elektrani, iako njena mreža nije bila spojena na vanjsku mrežu, preuzevši kontrolu nad Siemensovim programirljivim logičkim upravljačima, a prijavljeno je i da su obavještajne agencije izgradile repliku iranskog objekta koristeći istu Siemensovu opremu kako bi naučili kako je najbolje napasti [237].

Prvi potvrđeni primjer destruktivnog kibernetičkog napada na elektroenergetsku mrežu dogodio se u Ukrajini 2015. godine gdje je kibernetički napad na tri tvrtke za distribuciju električne energije izazvao nestanak struje koji je pogodio 225.000 korisnika [212]. Smatra se kako su napadači koristili lažne poruke e-pošte kako bi pristupili ciljanim mrežama šest mjeseci prije napada, tijekom kojih su stekli sigurnosne vjerodajnice i znanje o infrastrukturi potrebno za dovršetak napada, a tijekom prekida rada, napadači su također zatrpali pozivni centar energetskih tvrtki telefonskim prometom kako bi ometali komunikaciju tijekom odgovora na incident. Sofisticiraniji napad nanio je još jedan prekid rada u 2016. godini, a ukrajinska sigurnosna služba optužila je ruske sigurnosne službe za orkestriranje oba napada [238], [212].

Uz ova dva, možda i najpoznatija kibernetička napada na kritičnu nacionalnu infrastrukturu, postoje brojni drugi napadi korištenjem raznih oblika ucjenjivačkog softvera (engl. *Ransomware*) i drugih oblika zlonamjernog softvera, od kojih su WannaCry i NotPetya bili najrazvikaniji [239]. Globalni napad WannaCry zlonamjernog softvera koji je ciljao zdravstvene organizacije započeo je u svibnju 2017. godine i uspio je zaraziti više od 200.000 računala raširenih u 150 zemalja, uključujući sustave Nacionalne zdravstvene službe Velike Britanije. Procijenjeno je da je za napade WannaCry zlonamjernim softverom plaćeno više od 312 otkupnina u kripto valuti, a jedna od tvrtki koja je pretrpjela WannaCry napad u ožujku 2018. godine je i tvrtka za proizvodnju zrakoplova Boeing [123]. S druge strane, NotPetya ili Nyetya ili ExPetr zlonamjerni softver prvi put se pojavio u lipnju 2017. godine, a iako se isprva smatralo kako se radi o još jednom globalnom ucjenjivačkom softveru, kao što je WannaCry, pokazalo se da se radi o softveru za brisanje podataka (engl. *Wipeware*) [239] budući da, iako sadrži komponentu ucjenjivačkog softvera, NotPetya ne može dekriptirati žrtvine podatke, čak i ako se plati otkupnina [240]. Jedan od najzvučnijih napada ovim zlonamjernim softverom bio je napad na dansku logističku tvrtku za kontejnere, Maersk, 2017. godine koji je tvrtku stajao oko 300 milijuna dolara [241].

Najpoznatiji domaći primjer napada na kritičnu nacionalnu infrastrukturu bio je nedavni napad na naftnu kompaniju INA d.d. koji je započeo na Valentinovo 2020. godine i trajao neprekidno više dana. Službene izjave INA-e po tom pitanju bile su šture i uključivale obrazloženje kako se radi o napadima uskraćivanja usluge (engl. *Denial of Service*) dok su se mogle čuti i neslužbene informacije da su razmjeri napada znatno veći i da se radi o napadu ucjenjivačkog softvera za koji je tražena otkupnina od 150 bitcoina što je oko 100 milijuna kuna [242]. Zasad još nisu poznati službeni uzrok, razmjer i posljedice ovog napada.

Još jedan domaći primjer kibernetičkih napada koji su izazvali zanimanje javnosti bili su napadi lažnog predstavljanja radi krađe identiteta u 2018. g. usmjereni na državni i javni sektor koji su postali naširoko poznati zbog primjera Grada Đakova čiji je službenik uplatio 50 tisuća eura na račun Johna Smitha ne provjeravajući autentičnost elektroničke pošte koju je zaprimio od, kako je stajalo u zaglavlju poruke, gradonačelnika Đakova [243].

4. KULTURA INFORMACIJSKE SIGURNOSTI

Značajan obujam kršenja informacijske sigurnosti nastaje kao posljedica ljudskog čimbenika [7], [18] zbog činjenice da zaposlenici, bilo namjerno ili iz nemara, često zbog nedostatka znanja, predstavljaju najveću prijetnju informacijskoj sigurnosti [95]. Štoviše, čak i ako je organizacija uspostavila sustav upravljanja informacijskom sigurnošću prema preporukama sigurnosnih standarda i dobre prakse, to ne znači da je zajamčeno sigurnosno prihvatljivo ponašanje zaposlenika [244] čime se javlja potreba za uspostavom organizacijske kulture informacijske sigurnosti kao ključnim elementom za upravljanje ljudskim čimbenicima uključenim u informacijsku sigurnost [95]. Naime, dok standardi za upravljanje informacijskom sigurnošću pružaju opće smjernice u upravljanju tehnologijom informacijske sigurnosti, okvir kulture informacijske sigurnosti može se koristiti kao posebne smjernice uspostave i procjene kulture informacijske sigurnosti za poboljšanje sigurnosnog ponašanja zaposlenika u organizaciji [244].

Međutim, unatoč široko prepoznatljivoj važnosti informacijske sigurnosti kao vitalnog elementa u organizaciji, ne postoji jasno razumijevanje kako organizacije zapravo obrađuju kulturu informacijske sigurnosti među zaposlenicima u određenom okruženju [18] budući da nije lak zadatak potaknuti kulturu u kojoj svi zaposlenici upravljaju i štite informacije u svakom trenutku u skladu s organizacijskom politikom i regulatornim zahtjevima [80]. U svakoj organizaciji kultura informacijske sigurnosti proizlazi iz načina na koji se ljudi ponašaju prema informacijama i njihovoj sigurnosti [160], zbog čega se pristup organizacije prema informacijskoj sigurnosti treba usredotočiti na ponašanje zaposlenika gdje o tom ponašanju ovisi uspjeh ili neuspjeh organizacije [245]. Stoga je važno stvoriti kulturu koja je svjesna sigurnosti informacija [246] čime se umanjuju rizici za informacijsku imovinu i posebno smanjuje rizik lošeg ponašanja zaposlenika i štetne interakcije s informacijskom imovinom [245].

Razvoj snažne kulture informacijske sigurnosti nije jednokratna aktivnost, već je trajni proces koji treba kontinuirano njegovati ako se želi ugraditi u širu kulturu organizacije. To zahtijeva podršku i angažiranje na najvišoj organizacijskoj razini gdje rukovodstvo, čija je odgovornost njegovati kulturu informacijske sigurnosti [10], svojim primjerom pokazuje što je za organizaciju prihvatljivo ponašanje sa stajališta informacijske sigurnosti [145]. Međutim, u svojim nastojanjima da postignu rezultate, rukovodstvo se ponekad previše fokusira na brojeve,

poboljšanje prihoda i smanjivanje troškova pri čemu mogu zanemariti važnost stvaranja zdravih organizacija s jakim kulturama kao važnim sastojkom u postizanju najboljih rezultata [247].

Također, u organizacijama ponekad ne postoje politike ili procedure upravljanja informacijskom sigurnošću već se radi o nedokumentiranim procesima gdje se znanje za provedbu dobre sigurnosti nalazi unutar domene zaposlenika čime se javlja određena slabost u upravljanju informacijskom sigurnošću i nemogućnost uspostavljanja valjane kulture informacijske sigurnosti [10]. Sigurnosna politika utječe na način na koji zaposlenici stupaju u interakciju s informacijskom imovinom, uspostavlja osnovu za donošenje etičkih odluka pri rukovanju s organizacijskim informacijama i u konačnici usmjerava njihovo ponašanje da bude u skladu sa zakonodavnim, regulatornim i ugovornim zahtjevima [161]. Rukovodstvo, čije aktivno sudjelovanje snažno utječe na kulturu unutar organizacije koja zauzvrat utječe na stavove zaposlenika i percipirano ponašanje u usklađenju poštivanja politika informacijske sigurnosti [75], [248], treba poticati zaposlenike na etično ponašanje jednih prema drugima i svim organizacijskim sredstvima [249]. Etično ponašanje i ponašanje u skladu s propisanim sigurnosnim politikama treba se provoditi kao prihvaćeni način ponašanja u radnom okruženju i postati dio zaposlenikove svakodnevice [160] što se postiže aktivnim sudjelovanjem svih zaposlenika u aktivnostima vezanim uz upravljanje informacijskom sigurnošću. Tako McIlwraith parafrazirajući Konfucija ističe: „Recite im i oni će možda poslušati, pokažite im i oni će možda naučiti, *uključite* ih i razumjet će" [71].

U relevantnim istraživanjima iz domene kulture informacijske sigurnosti autori su se bavili temama koje uključuju mjerenje [15], [245] i procjenu kulture informacijske sigurnosti [250], prihvaćanja kulture informacijske sigurnosti [251], odnos između kulture informacijske sigurnosti i organizacijske kulture [8], [179], [162], [95], razvoj konceptualnih modela [95], [252] i okvira za kulturu informacijske sigurnosti [11], [253], [6], kao i utvrđivanje čimbenika kulture informacijske sigurnosti [250], [59], [252], [7], [184], [184], [252], [254], [5]. Također, bilo je i nekoliko sistematskih pregleda literature vezanih uz kulturu informacijske sigurnosti [11], [15], [255], [256], [252], [257]. U rezultatima tih istraživanja prepoznata je činjenica da su postojeća istraživanja u velikoj mjeri deskriptivna, filozofska ili teorijska, kao i nedostatak znanja u prepoznavanju čimbenika i mjerenja utjecaja na kulturu informacijske sigurnosti zbog čega postoji potreba za sveobuhvatnim empirijskim istraživanjem [252], [11], [12], [255], [59].

Postojeća literatura naglašava važnost kulture informacijske sigurnosti te daje prijedloge i smjernice o tome kako procijeniti kulturu informacijske sigurnosti, međutim ne pruža jasno

razumijevanje kako se kultura informacijske sigurnosti mora konceptualizirati kako bi istraživači razvili instrument za razumijevanje i mjerenje modela kulture informacijske sigurnosti [15]. Štoviše, Okere i suradnici [155] navode kako ne postoji metoda ili set alata za procjenu kulture informacijske sigurnosti jer ne postoji objavljeni ili široko prihvaćeni i konsolidirani pristup koji bi odredio kako procijeniti kulturu zbog čega je potrebno više istraživanja u ovom području. S druge strane, AlHogail i Mirza [258] napominju kako je jedan od načina za mjerenje statusa kulture informacijske sigurnosti organizacije korištenje upitnika kako bi se postiglo razumijevanje čimbenika koji utječu na sigurnosno ponašanje zaposlenika.

Da je potrebno više istraživanja po pitanju kulture informacijske sigurnosti i čimbenika koji utječu na nju ukazuje i Alnatheer [15] koji u svom pregledu literature vezanom uz istraživanja kulture informacijske sigurnosti navodi kako su samo dva istraživačka modela [259], [245] dala validirani instrument za procjenu kulture informacijske sigurnosti. To je u skladu s rezultatima iscrpnog pregleda literature za objavljene radove na području kulture informacijske sigurnosti između 2003. i 2013. godine, gdje su AlHogail i Mirza [138] utvrdili da je samo 22% od ukupno objavljenih radova predstavilo neki okvir gdje ti okviri uzimaju u obzir različita pitanja u kulturi informacijske sigurnosti.

Sve to upućuje na potrebu daljnjeg istraživanja koncepta kulture informacijske sigurnosti, odnosa kulture informacijske sigurnosti i organizacijske kulture, kao i čimbenika koji utječu na kulturu informacijske sigurnosti u organizaciji, kako bi se mogao izraditi okvir za procjenu kulture informacijske sigurnosti i time omogućilo organizacijama prepoznavanje kritičnih čimbenika uspjeha kulture informacijske sigurnosti, a time i uspješnijeg upravljanja informacijskom sigurnošću.

4.1. Koncept kulture u području informacijske sigurnosti

Kultura informacijske sigurnosti pojavila se krajem 1990-ih godina kao mjera za promicanje sigurnog ponašanja zaposlenika u organizacijama [60] kako bi se smanjile posljedice namjernog ili nenamjernog djelovanja ljudi kao najveće prijetnje informacijskoj sigurnosti organizacije [140], [14], [95]. Kultura informacijske sigurnosti može se shvatiti kao skup obilježja informacijske sigurnosti koje organizacija cijeni, pretpostavka o tome što je prihvatljivo, a što nije u vezi sa informacijskom sigurnošću odnosno koje se ponašanje vezano za informacijsku sigurnost potiče, a koje ne te, u konačnici, promatrati kao način na koji se ljudi ponašaju prema informacijskoj sigurnosti u organizaciji [140].

Kultura informacijske sigurnosti u organizaciji može se prepoznati na više načina, od promatranja vidljivih inicijativa rukovodstva, poput unapređenja sigurnosne osviještenosti, sigurnosne obuke ili provedbe sigurnosnih politika, preko iskazivanja zaposlenikovih uvjerenja o sigurnosti do dokumentiranja i analize ponašanja zaposlenika u vezi sa sigurnošću [260]. Bez obzira na koji način prepoznavali kulturu informacijske sigurnosti u organizaciji, treba uvijek imati na umu kako se kultura unutar organizacije neprestano mijenja [245] te ju se može promatrati i shvaćati živim sustavom [79], a ne nekakvom nepromjenjivom strukturom [260].

Kultura informacijske sigurnosti predstavlja višeslojni koncept sastavljen od više razina i komponenti koji obuhvaća osnovne pretpostavke vezane uz informacijsku sigurnost i načine kako zaštititi informacije i postupati s njima u bilo kojem obliku, stavove i uvjerenja zaposlenika u odnosu na informacijsku sigurnost, kontrole, usklađenost i načine kako zaštititi i imati interakciju s informacijama. Između ostalog, ona podrazumijeva i poznavanje organizacijske politike informacijske sigurnosti i zahtjeva za usklađenost, razumijevanje što su incidenti informacijske sigurnosti te kako minimizirati rizik za informacije prilikom njihove obrade [17]. Kao što je vidljivo iz prethodno navedenog, upravo je postojanje dostatnog znanja o informacijskoj sigurnosti jedan od osnovnih preduvjeta za obavljanje bilo koje normalne aktivnosti na siguran način [163].

Primjerice, bez potrebnih vještina i sposobnosti, bilo bi nemoguće pravilno obavljati poslove vezane uz sigurnost zbog čega bi zaposlenici, za obavljanje svakodnevnih zadataka na siguran način, morali imati dovoljno znanja o tome kako sigurno obavljati svoje zadatke. Isto tako, da bi izradili dokument politike informacijske sigurnosti, osoba ili tim odgovoran za sastavljanje politike mora znati što treba uključiti u takvu politiku kako bi se na odgovarajući način riješile sigurnosne potrebe organizacije. U konačnici, ako bi neko od uvjerenja zaposlenika bilo u sukobu s iskazanim vrijednostima organizacije, znanje zašto je potrebna posebna kontrola, može igrati ključnu ulogu u osiguravanju usklađenosti [163]. Postojanje dostatnog znanja kao preduvjeta dobre kulture informacijske sigurnosti dodatno se komplicira brzinom promjene u okruženju informacijskog sustava s obzirom na sigurnosne prijetnje, što čini nerazumnim za pretpostaviti da će pojedinačna znanja / vještine biti aktualna, a ponašanje pojedinca ostati onakvo kakvo se očekuje [261].

4.1.1. Definicija kulture informacijske sigurnosti

Postoji mnoštvo definicija kulture informacijske sigurnosti od kojih je jedna od njih da je to „*sustav zajedničkih vrijednosti (definiranje onoga što je važno) i normi (definiranje*

odgovarajućih stavova i ponašanja)" [262] gdje se kultura „*može konceptualizirati kao skup zajedničkih razumijevanja koja se izražavaju u zajedničkim obrascima djelovanja i značenja, poput zajedničkog jezika*" [41]. Schlienger i Teufel [74] definiraju kulturu informacijske sigurnosti kao „*sve sociološko-kulturološke mjere koje podržavaju metode tehničkih aktivnosti, tako da informacijska sigurnost postaje prirodan aspekt u svakodnevnoj aktivnosti svakog zaposlenika*" iz čega je vidljiv nekadašnji naglasak na tehničku komponentu informacijske sigurnosti.

Da Veiga i Eloff [245] ističu kako kultura informacijske sigurnosti predstavlja „*stavove, pretpostavke, uvjerenja, vrijednosti i znanje koje zaposlenici / dionici koriste radi interakcije s organizacijskim sustavima i postupcima u kojem trenutku gdje interakcija rezultira prihvatljivim ili neprihvatljivim ponašanjem (tj. incidentima) koje se očituje u artefaktima i kreacijama koje postaju dio načina na koji se stvari odvijaju u organizaciji radi zaštite njenih podataka*". Mahfuth i suradnici [13] vide kulturu informacijske sigurnosti kao „*integracijski proces uvjerenja, percepcija, stavova, vrijednosti, pretpostavki i znanja koji vode, usmjeravaju i upravljaju percepcijama i stavovima zaposlenika u utjecanju na sigurnosno ponašanje zaposlenika ili kako bi se pronašlo prihvatljivo ponašanje zaposlenika kada su u interakciji s informacijskom imovinom u svojim organizacijama*", dok Malcolmson [263] ističe kako je sigurnosna kultura „*naznačena u pretpostavkama, vrijednostima, stavovima i vjerovanjima koje imaju članovi organizacije te njihovom ponašanju, a koje bi mogle potencijalno utjecati na sigurnost organizacije i mogu ili ne moraju imati, izričitu, poznatu poveznicu na taj utjecaj*".

Za Alhogaila i Mirzu [11] kultura informacijske sigurnosti može se definirati kao „*skup percepcija, stavova, vrijednosti, pretpostavki i znanja koji usmjerava ljudsku interakciju s informacijskom imovinom u organizaciji s ciljem utjecaja na ponašanje zaposlenika radi očuvanja informacijske sigurnosti*", slično kao i za Alnatheera [15] koji promatra kulturu informacijske sigurnosti kao „*percepcije, stavove i pretpostavke informacijske sigurnosti koje su prihvaćene i poticane u organizaciji, odnosno način na koji se stvari obavljaju u organizaciji radi zaštite imovine informacija*".

Možda najopsežnija i najsveobuhvatnija definicija kulture informacijske sigurnosti je ona koju su predložili da Veiga i suradnici [257], a koja kaže sljedeće: „*Kultura informacijske sigurnosti kontekstualizirana je ponašanjem ljudi u organizacijskom kontekstu radi zaštite informacija s kojima organizacija postupa, kroz usklađenost s politikama i procedurama informacijske sigurnosti i razumijevanje kako implementirati zahtjeve na oprezan i pažljiv način da bi bili*

ugrađeni u redovne inicijative za komunikaciju, osvješćivanje, obuku i edukaciju. Ponašanje s vremenom postaje dio načina na koji se stvari rade, tj. druga priroda, kao rezultat pretpostavki zaposlenika, vrijednosti i uvjerenja, njihovog znanja o, odnosa prema i percepciji zaštite informacijske imovine. Kultura informacijske sigurnosti usmjerena je vizijom višeg rukovodstva zajedno s podrškom menadžmenta u skladu s politikom informacijske sigurnosti, a pod utjecajem unutarnjih i vanjskih čimbenika, podržanih odgovarajućim ICT okruženjem, vidljivim u artefaktima organizacije i prikazanom ponašanju od strane zaposlenika, stvarajući tako okruženje povjerenja s dionicima i uspostavljajući integritet." [257].

Kao što vidimo, različiti autori, s različitom složenošću i dubinom opisuju kulturu informacijske sigurnosti, no bez obzira o kojem se autoru radilo, moguće je primijetiti naglasak na djelovanju odnosno ponašanju ljudi koje bi trebalo biti usklađeno s očekivanim ponašanjem definiranim u sigurnosnim politikama. Sigurnosne politike, usmjeravane vizijom rukovodstva organizacije, utječu na ponašanje zaposlenika na način da njeguju kulturu informacijske sigurnosti [149] i predstavljaju neophodni element sigurnosne kulture, međutim, politika neće biti učinkovita u usmjeravanju ponašanja zaposlenika ako je zaposlenici nisu pročitali ili razumjeli [161]. Tako je Da Veiga [149] empirijski utvrdila da su ukupni prosječni rezultati za kulturu informacijske sigurnosti znatno pozitivniji za zaposlenike koji su pročitali politiku informacijske sigurnosti u usporedbi sa zaposlenicima koji nisu, što ilustrira pozitivan utjecaj politike na kulturu informacijske sigurnosti u kontekstu procjene kulture informacijske sigurnosti. Tako su zaposlenici koji su pročitali politiku informacijske sigurnosti imali bolje razumijevanje iste te su vjerovali da je politika praktična i primjenjiva na radno okruženje tijekom izvršavanja njihovih svakodnevnih zadataka čime se pokazuje kako poznavanje politike informacijske sigurnosti doprinosi pozitivnom utjecaju na kulturu informacijske sigurnosti [161].

4.1.2. Važnost kulture informacijske sigurnosti

Literatura o kulturi informacijske sigurnosti prepoznaje kako je najvažnije uvjerenje koje utječe na sigurnost organizacije upravo uvjerenje, kako zaposlenika tako i same organizacije, da je sigurnost informacija važna [198], a budući da je sigurnost informacija postala jedno od izazovnih pitanja u današnjim organizacijama, važno je stvoriti sveobuhvatnu kulturu sigurnosti unutar organizacije za učinkovito upravljanje informacijskom sigurnošću [59].

Učinkovitost raznih tehničkih sigurnosnih kontrola temelji se na ljudima koji tijekom svojih redovnih aktivnosti svakodnevno imaju interakciju s informacijama [138] gdje je kultura informacijske sigurnosti posebno važna za organizacije budući da se ljudska dimenzija

informacijske sigurnosti ne može potpuno riješiti tehničkim i upravljačkim mjerama [60]. Cilj kulture informacijske sigurnosti je zaštita informacijske imovine [264] putem promicanja opreznog i sigurnog ponašanja zaposlenika [70], [138], čime se umanjuje prijetnja povjerljivosti, integritetu i dostupnosti informacijske imovine [80], kao i vjerojatnost pojave kršenja sigurnosti [192].

Uspostavljanjem organizacijske kulture informacijske sigurnosti koja obuhvaća vrijednost i važnost sigurnosti [3] ugrađuje se sigurnost u ponašanje zaposlenika [197] čime sigurno ponašanje može postati prirodan način obavljanja svakodnevnih aktivnosti [44], [70] odnosno normalan dio svakodnevnog ponašanja zaposlenika organizacije [88], [138]. Upravo preispitivanjem informacijske sigurnosti kao sastavnog dijela posla, navika i ponašanja zaposlenika, kultura informacijske sigurnosti postaje čimbenik koji omogućuje učinkovitu sigurnosnu praksu [265] uklapajući ju u svakodnevne radnje [145].

Kultura informacijske sigurnosti, definirana opredjeljenjem rukovodstva, odgovornostima i osviještenošću zaposlenika o informacijskoj sigurnosti, ima pozitivan učinak na poštivanje informacijske sigurnosti [266] gdje zaposlenici poštuju politiku informacijske sigurnosti djelujući na odgovarajući način ako imaju potrebna znanja i vještine [267], [138].

Međutim, važno je imati na umu kako kultura informacijske sigurnosti u organizaciji može ili pridonijeti zaštiti informacija ili stvoriti rizik [16] budući da je kultura među najvećim bogatstvima koje organizacija može imati, kad je jaka, zdrava i potiče pravo ponašanje, ali istovremeno, ona je ranjiva imovina koja se može oštetiti ili izgubiti ako rukovoditelji nisu svjesni njene vrijednosti i ne paze na moguće prakse, stavove, prijetnje ili događaje mijenjanja kulture [247]. Primjerice, spajanjem dvije organizacije mijenja se tehnička infrastruktura, preinačuju se formalne sigurnosne politike, a normativne strukture sukobljavaju čime novonastale promjene obično narušavaju prevladavajuću kulturu informacijske sigurnosti, čineći tako novu organizaciju vrlo ranjivom [268]. To dovodi do toga da, ako sigurnosna kultura organizacije nije snažna, tada će i adekvatne tehnološke sigurnosne mjere postati neadekvatne [269].

4.1.3. Karakteristike dobre kulture informacijske sigurnosti

Kultura informacijske sigurnosti mora se smatrati dijelom programa informacijske sigurnosti koji usmjerava ponašanje zaposlenika budući da takva kultura može doprinijeti zaštiti podataka i umanjiti rizik koji predstavlja ponašanje zaposlenika [270], a kako bi imale pozitivnu i snažnu

kulturu informacijske sigurnosti, organizacije moraju osigurati kombinaciju ljudskih, procesnih i tehnoloških zaštitnih mjera [5], [270]. Za stvaranje dobre kulture informacijske sigurnosti nije dovoljno samo slijediti postojeće standarde i prakse informacijske sigurnosti već je potrebno stvoriti nova saznanja o informacijskoj sigurnosti [34] jer je kultura koja promiče dobro ljudsko ponašanje vezano za sigurnost kroz znanje, vrijednosti i pretpostavke daleko učinkovitija od propisa koji jednostavno određuju uloge i obveze zaposlenika [6].

Sigurnost može biti učinkovita samo ako zaposlenici znaju, razumiju i prihvaćaju potrebne mjere predostrožnosti [6], što znači kako je moguće da korisnici dobro razumiju svoje uloge, ali još uvijek se ne pridržavaju sigurnosnih pravila jer su u sukobu s njihovim uvjerenjima i vrijednostima zbog čega je imperativ također osigurati da korisnici imaju ispravan stav, a time i željeno ponašanje, prema informacijskoj sigurnosti [163].

Drugim riječima, nužno je da kultura odražava pozitivan stav o sigurnosti informacija u čitavoj organizaciji [183] kako bi svi zaposlenici, od administrativnog osoblja, preko čistača pa sve do generalnog direktora, aktivno sudjelovali u održavanju što je moguće sigurnijeg organizacijskog okruženja [25]. Da bi se to postiglo, potrebno je razumjeti koje temeljne vrijednosti, uvjerenja i pretpostavke pokreću ponašanje zaposlenika kako bi se moglo utjecati na promjenu sa stava kako je informacijska sigurnost odgovornost IT odjela, na stav kako je informacijska sigurnost odgovornost svih [261] i promicati kulturu u kojoj zaposlenici dijele odgovornost za obranu organizacije od sigurnosnih napada [99]. Kultura čiji je cilj osigurati da informacijska sigurnost bude odgovornost svih zaposlenika [258], promiče odgovornost pojedinaca u provođenju informacijske sigurnosti u organizacijama [37] gdje se, u idealnom slučaju, svi zaposlenici pridržavaju politike i pravila informacijske sigurnosti čak i kad nikoga nema u blizini i kad se njihovo ponašanje ne nadgleda [261].

Dok dobra i snažna kultura, koja je svjesna sigurnosti informacija, može pomoći smanjenju ljudskih prijetnji zaštiti informacija i na taj način pomoći u smanjenju proboja podataka ili incidenata u organizacijama [257], [253], slaba sigurnosna kultura može učiniti sve zaštitne mjere neučinkovitima. Na primjer, politika i obuka o sigurnom korištenju lozinki su uzaludne ako organizacijska kultura potiče razmjenu lozinki. Slično tome, politika upravljanja pravima pristupa provedena klasifikacijskim matricama, označavanjem dokumenata, vatrozidima i sporazumima o povjerljivosti neće biti učinkovita ako se rukovoditelji dosljedno oglušuju ili odbacuju mjere zaštite povjerljivosti [271].

U snažnoj kulturi informacijske sigurnosti očekuje se manje incidenata informacijske sigurnosti, primjerice manje dijeljenja lozinki s kolegama ili obraćanje pažnje na izbjegavanje razgovora o povjerljivim informacijama na javnom mjestu [161] gdje će istodobno svi zaposlenici biti motivirani razmišljati o svom ponašanju u svakom trenutku, procijeniti kako njihovo ponašanje utječe na sigurnost i što mogu učiniti kako bi poboljšali sigurnost [58]. Međutim, treba imati u vidu da je kultura informacijske sigurnosti jaka toliko koliko je jaka njena najslabija karika. Na primjer, posjedovanje sveukupne sigurnosne kulture jakih lozinki besmisleno je ako je kultura sigurnosti lozinke u visokorizičnom odjelu organizacije slaba [79].

U konačnici, ne postoji 'ispravna' ili 'najbolja' kultura za sve organizacije već je najprikladnija kultura za organizaciju ona koja joj najbolje pomaže nositi se s potrebama poslovnog okruženja [272] što znači da svaka organizacija za sebe mora vidjeti kakav će stav zauzeti i koji bi pristup bio najbolji u konkretnoj situaciji. Dodatni element na koji bi organizacije trebale obratiti pažnju prilikom formuliranja sigurnosnih inicijativa radi uspostave kulture informacijske sigurnosti je činjenica da postoje razlike u sigurnosnim kulturama među različitim profesijama [273].

Ramachandran i suradnici [274] proveli su kvalitativno istraživanje o kulturi informacijske sigurnosti iz perspektive četiri različite profesije: informacijskih sustava, računovodstva, ljudskih resursa i marketinga. Rezultati istraživanja ukazuju da postoje razlike u uvjerenjima o tome što čini informacijsku sigurnost, tko je odgovoran za nju i vjerojatnost njihove usklađenosti sa sigurnošću pod pritiskom rokova izvedbe. Konkretno, podaci sugeriraju da računovodstvena profesija ima snažnu kulturu informacijske sigurnosti, marketinška profesija slabu kulturu informacijske sigurnosti, dok su profesije vezane uz informacijske sustave i ljudske resurse između njih dvije [273], [274].

U smislu općih uvjerenja, računovođe i profesionalci iz područja ljudskih resursa su konzervativni, u skladu s pravilima i željni organizirane strukture s jasnim razgraničenjem odgovornosti dok marketinški stručnjaci vjeruju u riskiranje, zaobilaženje pravila i potvrđivanje njihove neovisnosti, a sve u potrazi za uspjehom. Profesionalci iz domene informacijskih sustava pripadaju između ove dvije krajnosti, vjerujući da je potrebno izbjegavati rizik pri obavljanju svoje dužnosti u odnosu na informacijsku infrastrukturu, ali u ostalim segmentima želeći biti neovisni o pravilima i usmjeravanju rukovodstva [273]. Istraživanje također pokazuje da se sigurnost informacija i dalje doživljava kao tehnički problem, da čak i najkonzervativnije skupine koje se pridržavaju pravila mogu kršiti sigurnosna pravila pod pritiskom izvedbe, a da

sama osviještenost nije dovoljna za izgradnju snažne sigurnosne kulture [274]. Dakle, iako profesionalne skupine mogu dijeliti pojedinačne karakteristike sigurnosne kulture, čini se da je cjelokupna sigurnosna kultura svake profesionalne skupine relativno jedinstvena [273].

Organizacijska kultura informacijske sigurnosti uključuje uspostavljanje politika, standarda, programa obuke i edukacije [136], no bez podrške i uključenosti rukovodstva čija je uloga vrlo važna u razvoju, kako organizacijske kulture i kulturnih promjena, tako i kulture informacijske sigurnosti [141], neminovan ishod je izostanak kulture informacijske sigurnosti u organizaciji i pojava ravnodušnosti po pitanju informacijske sigurnosti među zaposlenicima [24] jer se na taj način zaposlenicima šalje poruka od strane rukovodstva kako sigurnost nije bitna [198].

Općenito gledajući, informacijska sigurnost, kao podskup ukupne sigurnosti u organizaciji, uvelike ovisi o samoj organizacijskoj kulturi [141], što znači da stroga kontrola sigurnosti u inače slabo kontroliranoj organizaciji vjerojatno neće uspjeti [58]. Na taj način vidljiva je i međusobna povezanost kulture informacijske sigurnosti i organizacijske kulture, gdje svaka organizacija ima kulturu u kojoj su zajednice od interesa ujedinjene sličnim vrijednostima i dijele zajedničke ciljeve [28].

4.2. Organizacijska kultura

Tijekom vremena, organizacije uspostavljaju kulturu, odnosno način na koji se stvari odvijaju u organizaciji [272], temeljenu na prošlom i sadašnjem vodstvu, povijesti, zemljopisnoj rasprostranjenosti, načinu donošenja odluka, profitabilnosti, industrijskim propisima i svakoj pojedinoj osobi u organizaciji gdje svaki pojedinac svakodnevno donosi svoj jedinstveni skup vrijednosti, pozadina, iskustava i sposobnosti na radno mjesto. Na taj način kultura može imati značajan utjecaj na ono što se događa u organizacijama, kako se stvari rade ili kako organizaciju doživljavaju zaposlenici i kupci, ali isto tako, kultura može utjecati i na organizacijsku konkurentsku prednost ili nedostatak iste [247].

Iako ne postoji jedna univerzalno prihvaćena definicija koncepta organizacijske kulture, gdje Kummerow i Kirby [275] navode kako je identificirano čak više od 160 različitih definicija, jednu od najčešće prihvaćenih i najopsežnijih definicija pružio je Edgar Schein koji je u prvom izdanju svoje knjige *Organizacijska kultura i vodstvo,* objavljenom 1985. godine, definirao organizacijsku kulturu kao „*obrazac osnovnih pretpostavki koji je određena grupa izumila, otkrila ili razvila dok je učila suočiti se s problemima vanjske prilagodbe i unutarnje integracije, a što je dovoljno dobro funkcioniralo da bi se moglo smatrati valjanim i, prema*

tome, moglo tome poučiti nove članove kao ispravnom načinu percipiranja, razmišljanja i osjećanja u odnosu na te probleme" [276]. Dvadeset pet godina kasnije, u četvrtom izdanju svoje knjige objavljenom 2010. godine, Scheinova je definicija organizacijske kulture u osnovi bila ista: „*obrazac zajedničkih osnovnih pretpostavki koje je grupa naučila dok je rješavala svoje probleme vanjske prilagodbe i unutarnje integracije, a što je dovoljno dobro funkcioniralo da se može smatrati valjanim i, prema tome, biti naučeno od strane novih članova kao ispravan način percepcije, razmišljanja i osjećanja u odnosu na te probleme*" [277]. To nakupljeno učenje je obrazac ili sustav uvjerenja, vrijednosti i normi ponašanja koje se uzimaju zdravo za gotovo kao osnovne pretpostavke i na kraju postaju nesvjesne [278].

Kao što je vidljivo, postoji relativno mala razlika između Scheinovih definicija organizacijske kulture iz 1985. i 2010. godine, što ukazuje na to da on nije bitno izmijenio svoju definiciju tijekom 25 godina i četiri izdanja svoje knjige, a mogući razlog zašto je ta definicija jedna od najviše prihvaćenih i najčešće citiranih definicija organizacijske kulture je činjenica da se ona ne usredotočuje samo na sadržaj organizacijske kulture (tj. što je organizacijska kultura), već također skreće pozornost na proces u kojem se formira i na funkciju koju služi [275].

Ova definicija skreće pozornost na niz ključnih karakteristika organizacijske kulture koje su prihvatili mnogi, ako ne i većina istraživača na tom polju, a koje uključuju karakteristiku da se organizacijska kultura razvija s vremenom; da se temelji na praktičnom iskustvu prilagođavanja okolini; da ju dijele članovi organizacije i da utječe na njihovo mišljenje i osjećaje; te da se održava procesom socijalizacije [275] čime organizacijska kultura postaje „*osnovni obrazac zajedničkih pretpostavki, vrijednosti i uvjerenja koje se smatraju ispravnim načinom razmišljanja i reagiranja na probleme i prilike s kojima se organizacija suočava*" [272].

Sam Schein napominje kako je najveća opasnost u pokušaju razumijevanja kulture njeno preveliko pojednostavljenje, što znači da, iako je primamljivo reći da je kultura samo „*način na koji radimo stvari ovdje*", „*obredi i rituali naše tvrtke*", „*klima u organizaciji*", „*sustav nagrađivanja*" ili „*naše osnovne vrijednosti*", to su sve manifestacije kulture, ali nijedna ne predstavlja razinu gdje je kultura bitna budući da kultura postoji na nekoliko 'razina', koje se kreću od vrlo vidljive do vrlo prešutne i nevidljive, te se za razumijevanje kulture mora upravljati dubljim razinama [279]. Tako se Scheinov model organizacijske kulture, koji je detaljnije opisan u točki *4.2.2. Modeli organizacijske kulture korišteni u kontekstu informacijske sigurnosti* sastoji od tri razine i to, razine artefakata, razine prihvaćenih vrijednosti te razine osnovnih pretpostavki, uz obrazloženje da, ako ne odgonetnete obrazac

osnovnih pretpostavki koje mogu djelovati, nećete znati kako ispravno protumačiti artefakte niti koliko vjerodostojnosti dati prihvaćenim vrijednostima što, drugim riječima znači, da suština kulture leži u obrascu osnovnih temeljnih pretpostavki, gdje nakon što njih shvatite, možete lako razumjeti ostale površinske razine i s njima se nositi na odgovarajući način [277].

Isto tako, u organizacijsku kulturu, uz spomenute kolektivno postavljene pretpostavke, uvjerenja i vrijednosti, ulaze i ideologije, značenja, očekivanja, stavovi, norme, organizacijski mitovi, simboli, rituali i drugi oblici uzornog ponašanja [275] gdje kultura stvara snažan pritisak na ljude da se slažu, misle i djeluju na konzistentne načine unutar organizacije [272]. Ipak, kada se primjenjuje na područje informacijske sigurnosti, razmatranje samo organizacijske kulture nije dovoljno za razumijevanje utjecajnih čimbenika koji stoje iza kulture informacijske sigurnosti već je potrebno obratiti pozornost i na druge čimbenike koji utječu na postojanje kulture informacijske sigurnosti unutar organizacije [34].

4.2.1. Odnos organizacijske kulture i kulture informacijske sigurnosti

Kultura informacijske sigurnosti često se prepoznaje kao vitalna supkultura unutar organizacijske kulture [79], [41] odnosno njen dio [11] zbog činjenice da je informacijska sigurnost postala organizacijska funkcija [249], međutim, to ne mora biti uvijek tako. Lim i suradnici [68] u svom istraživanju ističu kako literatura pokazuje da postoje tri vrste odnosa između organizacijske kulture i kulture informacijske sigurnosti, gdje prvi tip pretpostavlja odnos u kojem je kultura informacijske sigurnosti odvojena od organizacijske kulture, drugi tip pretpostavlja odnos u kojem je kultura informacijska sigurnosti supkultura organizacijske kulture dok treći tip pretpostavlja odnos u kojem je kultura informacijske sigurnosti ugrađena u samu organizacijsku kulturu.

Prvi tip odnosa je situacija u kojoj informacijska sigurnost nije sastavni dio organizacijske kulture već je potpuno odvojena od nje, a članovi organizacije (zaposlenici) često ili nisu uključeni ili su na minimalnoj razini uključenosti s provedbom sigurnosti u organizaciji. U ovakvom tipu odnosa, sigurnosna svijest organizacije je niska uslijed čega zaposlenici imaju vrlo malo znanja o sigurnosnim pitanjima i ne osjećaju da je to i njihova odgovornost. Organizacije često teže promatrati sigurnost kao trošak [23] te se često bore za financiranje sigurnosnih inicijativa. U ovakvoj situaciji jedino se IT odjel brine o informacijskoj sigurnosti [68].

U drugom tipu odnosa zaposlenici unutar odjela više su svjesni sigurnosnih zahtjeva, a povremena obuka za informacijsku sigurnost provodi se kao pridržavanje zahtjeva rukovodstva. Rukovodstvo počinje posvećivati više pažnje provedbi prakse informacijske sigurnosti, međutim, još uvijek postoji manja međusektorska koordinacija u upravljanju informacijskom sigurnošću organizacije. Štoviše, samo mala skupina ljudi sudjeluje u sigurnosnim mjerama koje se provode u organizacijama, a kultura informacijske sigurnosti organizacije mješavina je sigurnosnih supkultura, od kojih svaka odgovara potrebama povezanim s odgovornostima i zadacima pojedinih profesionalnih skupina kao što su kadrovska služba ili računovodstveni odjel [68].

Treći tip odnosa ukazuje na situaciju u kojoj je sigurnosna praksa organizacije odgovornost svih zaposlenika. Provedba sigurnosnih mjera odvija se na holistički način i pretpostavlja relativno visoku razinu uključenosti. U ovoj situaciji, redovito se ažuriraju sigurnosne politike, zaposlenici osjećaju vlasništvo nad informacijama i motivirani su u pridržavanju sigurnosnih politika. Ova priroda odnosa u kojoj je kultura informacijske sigurnosti ugrađena u organizacijsku kulturu pretpostavlja situaciju u kojoj svijest o informacijskoj sigurnosti nesvjesno postaje svakodnevna rutinska aktivnost. Svi zaposlenici prihvaćaju vrijednosti koje će im omogućiti kultura informacijske sigurnosti u svrhu boljeg odlučivanja o pitanjima informacijske sigurnosti u organizaciji [68].

Zaključak istraživanja koje su proveli Lim i suradnici [68] je da organizacije koje imaju srednji do visoki sigurnosni profil rizika trebaju ugraditi kulturu informacijske sigurnosti u organizacijsku kulturu kako bi utjecale na postupke i ponašanje zaposlenika u vezi s praksama informacijske sigurnosti. U suprotnom, izazovi kao što su poteškoće u pribavljanju dovoljnog budžeta za sigurnosne aktivnosti zbog izostanka podrške rukovodstva, definiranje mjesta odgovornosti, organizacijska motivacija za provedbu sigurnosnih mjera, različita percepcija sigurnosnog rizika te provođenje mjera informacijske sigurnosti od strane male skupine ljudi, neće biti pravovremeno i primjereno riješeni [68].

4.2.2. Modeli organizacijske kulture korišteni u kontekstu informacijske sigurnosti

Budući da su istraživanja pokazala kako na kulturu informacijske sigurnosti u većoj ili manjoj mjeri utječe organizacijska kultura [8] te je potrebno organizacijsku kulturu uzeti u obzir prilikom uspostave i razvijanja kulture informacijske sigurnosti kako bi se osiguralo da su identificirane najprimjerenije kontrole i potom implementirane na uspješan način [245], nije neobično da postoje brojni radovi koji za izradu modela ili radnih okvira kulture informacijske

sigurnosti koriste upravo postojeće modele i radne okvire razvijene u kontekstu organizacijske kulture.

Dva najpoznatija takva modela organizacijske kulture korištena u istraživanjima kulture informacijske sigurnosti su trorazinski model organizacijske kulture koji je razvio Edgar Schein 1985. godine [276] i radni okvir organizacijske kulture koji su 2000. godine predstavili James Detert, Roger Schroeder i John Mauriel [280].

4.2.2.1. Scheinov model organizacijske kulture

Prvi od dva najčešće korištena modela organizacijske kulture u istraživanjima kulture informacijske sigurnosti [179], [259], [162], [163], [95], [88] je model organizacijske kulture kojeg je razvio Edgar Schein [276], a koji je prepoznat kao jedna od najkorisnijih tipologija za razvrstavanje različitih elemenata za koje se misli da čine sadržaj organizacijske kulture [275].

Scheinov model sastoji se od tri razine :

1. *Artefakti* - Artefakti su prva i najlakša razina za zapažanje prilikom dolaska u neku organizaciju, gdje se artefaktima smatraju pojave koje se vide, čuju i osjete kad se naiđe na novu grupu s nepoznatom kulturom. Artefakti uključuju vidljive proizvode grupe, poput fizičkog okruženja, jezika, korištene tehnologije, stila oblačenja, manirama obraćanja i emocionalnim prikazima, ispričanim pričama o organizaciji, objavljenim popisima vrijednosti ili zamjetnim ritualima i ceremonijama. Drugim riječima, na razini artefakata, kultura je vrlo jasna i ima neposredni emotivni utjecaj te ju je lako promatrati, ali se zapravo ne zna zašto se članovi organizacije ponašaju baš tako te se samo promatranjem ne može zaista dešifrirati što se događa [279], [278].
2. *Prihvaćene vrijednosti i uvjerenja,* kao druga razina organizacijske kulture, predstavljaju naglašena, javno objavljena načela i vrijednosti za koje grupa tvrdi da pokušava postići, poput 'kvalitete proizvoda', 'cjenovnog vodstva' ili 'sigurnosti'. Mnoge tvrtke u Silicijskoj dolini, poput Googlea i Netflixa, najavljuju svoju kulturu u pogledu takvih vrijednosti u svim materijalima za regrutaciju i u knjigama o sebi [278]. Prihvaćene vrijednosti organizacije uključuju strategije, ciljeve, filozofije i druge dokumente koji opisuju vrijednosti, principe i viziju organizacije [155].

   Svo grupno učenje u konačnici odražava nečija izvorna uvjerenja i vrijednosti - njegov ili njezin osjećaj o onome što bi trebalo biti, različito od onoga što jest. Kada se grupa prvi put stvori ili kada se suoči s novim zadatkom ili problemom, prvo rješenje

predloženo za suočavanje s njim odražava neke pretpostavke pojedinca o tome što je ispravno ili pogrešno, što hoće ili neće raditi. Oni pojedinci koji prevladavaju, koji mogu utjecati na grupu da prihvati određeni pristup problemu, kasnije će biti identificirani kao vođe ili osnivači, ali grupa još nema zajedničko znanje kao grupa jer još nije poduzela zajedničku akciju u odnosu na ono što bi trebalo učiniti. Što god se predloži smatrat će se samo kao ono što vođa želi. Sve dok grupa nije poduzela zajedničku akciju i zajedno promatrala ishod te akcije, još uvijek ne postoji zajednička osnova za utvrđivanje hoće li ono što vođa želi biti valjano [277], [278].

3. *Zajedničke prešutne pretpostavke* - Ono što uistinu pokreće svakodnevno ponašanje jesu naučene, zajedničke, prešutne pretpostavke na kojima ljudi temelje svoj pogled na stvarnost - onakav kakav jest i treba biti. Iz toga proizlazi ono što se obično smatra „načinom na koji ovdje radimo stvari“, ali čak ni zaposlenici organizacije ne mogu bez pomoći rekonstruirati osnovne pretpostavke na kojima počiva njihovo svakodnevno ponašanje. Oni znaju samo da je to put i računaju na to jer kada rješenje problema opetovano funkcionira, uzima ga se zdravo za gotovo, a ono što je nekada bila hipoteza, potpomognuta samo pretpostavkom ili vrijednošću, postupno se počinje tretirati kao stvarnost te se dolazi do vjerovanja da stvari doista tako funkcioniraju. Osnovne pretpostavke u ovdje definiranom smislu postale su toliko uzete zdravo za gotovo da će se naći malo varijacija unutar društvenih jedinica. Zapravo, ako se osnovna pretpostavka čvrsto drži u grupi, članovi će smatrati nezamislivim ponašanje temeljeno na bilo kojoj drugoj pretpostavci [279],[278]. Ako uvjerenja i vrijednosti postaju dijeljene i uzete zdravo za gotovo, čine jezgru organizacijske kulture [155].

4.2.2.2. Radni okvir organizacijske kulture Deterta i suradnika

Drugi najčešće korišten model organizacijske kulture u istraživanjima kulture informacijske sigurnosti [198], [281], [191], [58] je radni okvir razvijen od strane Deterta i suradnika [280] kojim je predstavljena sveobuhvatna inicijativa za promjenom. Autori su izradili sistematizaciju općih dimenzija organizacijske kulture koje se najčešće koriste u postojećim istraživanjima i povezali kako te opće dimenzije odgovaraju specifičnim vrijednostima i uvjerenjima koja su podložna praksi potpunog upravljanja kvalitetom (engl. *Total Quality Management – TQM*). Autori su došli na tu ideju zbog činjenice da odnos kulture i primjene novih ponašanja i praksi nije bila na odgovarajući način istražena zbog nedostatka sveobuhvatnog okvira za definiranje i mjerenje organizacijske kulture zbog čega su autori predstavili svoj okvir.

Taj radni okvir organizacijske kulture sastoji se od osam dimenzija [280]:

1. *Osnova istine i racionalnosti* - Usredotočuje se na stupanj u kojem zaposlenici vjeruju da je nešto stvarno ili nije stvarno i na to kako se otkriva istina. Ova dimenzija može utjecati na stupanj do kojeg ljudi usvajaju bilo normativne bilo pragmatične ideale.
2. *Priroda vremena i vremenski horizont* - Koncept vremena u organizaciji otkriva se u smislu usvaja li organizacija dugoročno planiranje, strateško planiranje i postavljanje ciljeva ili se fokusira prvenstveno na ovdje i sada, reagirajući na kratkoročni vremenski horizont.
3. *Motivacija* - Unutar organizacije motivacija je temeljno načelo upravljanja. Ova dimenzija naglašava da je važno prepoznavanje načina motiviranja zaposlenika, tj. jesu li oni motivirani iznutra ili vanjskim silama. Također, karakteristike motivacije su i pitanja jesu li zaposlenici sami po sebi dobri ili loši, trebaju li biti nagrađeni ili kažnjeni i može li se manipuliranjem tuđe motivacije promijeniti napor ili krajnji rezultat.
4. *Stabilnost naspram promjene/inovacije/osobnog rasta* - Stabilnost i promjena usko su povezane s motivacijom. Neke su osobe otvorene za promjene (preuzimatelji rizika), dok je drugima silno potrebna stabilnost (izbjegavatelji rizika), a to se može primijeniti i na organizacije. Organizacije koje preuzimaju rizik smatraju se inovativnima i potiču kontinuirana poboljšanja. Organizacije koje izbjegavaju rizik obično su manje inovativne, s malo poticaja za promjenama.
5. *Orijentacija na posao, zadatak, suradnike* – Ova dimenzija predstavlja središnju točku rada u ljudskom životu i ravnotežu između rada kao proizvodne i društvene aktivnosti. Neke osobe vide rad kao nešto što je samo sebi svrha i brinu se o postignućima i produktivnosti. Druge osobe vide rad kao sredstvo za postizanje drugih ciljeva, poput ugodnog života i razvijanja društvenih odnosa. Ovdje su važna pitanja poput odgovornosti koju zaposlenici osjećaju prema svom položaju i njihove edukacije s obzirom na svoje uloge i odgovornosti.
6. *Izolacija naspram suradnje* – Ova se dimenzija fokusira na način na koji zaposlenici mogu raditi, bilo sami ili u suradnji s drugima te sadrži temeljna uvjerenja o prirodi ljudskih odnosa i o tome kako se rad obavlja najefikasnije i najučinkovitije. U nekim organizacijama većinu posla obavljaju pojedinci, a suradnja se često smatra kršenjem autonomije. Druge organizacije pozdravljaju suradnju i potiču timski rad, često organizirajući rad putem grupa od više zaposlenika.

7. *Kontrola, koordinacija i odgovornost* - Organizacije se razlikuju u stupnju koncentracije ili podjele kontrole. Tamo gdje postoji čvrsta kontrola postoje formalizirana pravila i procedure koje određuje nekolicina, kako bi se usmjerilo ponašanje većine. Tamo gdje je manja kontrola postoji fleksibilnost i autonomija radnika, s manje pravila ili formalnih procedura i zajedničkog odlučivanja.
8. *Orijentacija i fokus - unutarnji i/ili vanjski* - Ova se dimenzija odnosi na prirodu odnosa između organizacije i njenog okruženja i činjenicu pretpostavlja li organizacija da ona kontrolira svoje vanjsko okruženje ili da okruženje kontrolira nju. Organizacija može imati unutarnju orijentaciju (usredotočenost na ljude i procese unutar organizacije), vanjsku orijentaciju (usredotočenost na vanjske sastavnice, kupce, konkurente i okruženje) ili kombinaciju obje [280], [58].

4.2.3. Teorije ljudskog ponašanja korištene u kontekstu informacijske sigurnosti

U nastavku se nalazi kratki opis najčešće korištenih teorija ponašanja osoba koji potječu iz područja društvenih znanosti i psihologije, a koje istraživači koriste u istraživanjima iz domene informacijske sigurnosti, a napose kulture informacijske sigurnosti. Budući da detaljan opis ovih teorija izlazi iz okvira ove disertacije, napravljen je tek površni osvrt na nekoliko teorija koje pomažu u objašnjavanju ponašanja osoba u kontekstu kulture informacijske sigurnosti

Istraživanja vezana uz korištene teorije ljudskog ponašanja u kontekstu dostupnih istraživanja iz domene informacijske sigurnosti [157], [195], [282], [189] ukazuju na to da su opća teorija i teorija planiranog ponašanja, uz ostale teorije koje uključuju teoriju motivacije za zaštitom, teoriju društvenih veza i teoriju društvenog učenja ključne teorije za razumijevanje namjere ponašanja zaposlenika da se pridržavaju politike informacijske sigurnosti u organizaciji.

4.2.3.1. Teorija planiranog ponašanja (engl. Theory of Planned Behavior)

Teorija planiranog ponašanja, kao jedna od najprediktivnijih teorija uvjeravanja koja se koristi u različitim domenama [166] nastala je kao proširenje Teorije razložne akcije (engl. *Theory of Reasoned Action*) [77], a pretpostavlja da na ponašanje pojedinca utječe stav, percipirana kontrola ponašanja, subjektivne norme i namjere [201].

Stav osobe prema ponašanju je stupanj u kojem ona preferira ili ne preferira određeno ponašanje. Ako osoba percipira rezultat ponašanja kao pozitivan, oblikovat će pozitivan stav prema takvom ponašanju. Subjektivne norme ili društveni zahtjevi predstavljaju normativna uvjerenja koja se tiču ponašanja. Da bi osoba usvojila ponašanje, ona mora prije svega biti

motivirana da udovolji svojim društvenim zahtjevima. Percipirana kontrola ponašanja znači da osoba oblikuje svoje namjere u pogledu određenog ponašanja na temelju svojih osobnih uvjerenja [195]. Drugim riječima, ako ljudi pozitivno ocjenjuju ponašanje (stav) i ako misle da se druge njima važne osobe žele ponašati na isti način (subjektivna norma) te ako imaju sposobnost i potencijal da to ponašanje izvrše (percipirana kontrola ponašanja), tada imaju jaču namjeru takvog ponašanja [201].

Istraživanje koje su proveli Bulgurcu i suradnici [77] pruža empirijske dokaze koji potvrđuju da će zaposlenici, ako su svjesni bilo kakve koristi (unutarnje ili vanjske) koju bi mogli imati od poštivanja politike informacijske sigurnosti, vjerojatnije poštivati politiku. Uz to, autori su otkrili da su sigurnosna osviještenost i usklađenost pozitivno povezani s unutarnjim troškovima kao što su krivnja ili sramota. Takvi su faktori primjeri društvenih zahtjeva, koji daju potvrdu drugom dijelu teorije, subjektivnim normama [195].

4.2.3.2. Opća teorija odvraćanja (engl. General Deterrence Theory)

Opća teorija odvraćanja, kao jedna od najčešće korištenih teorija u sigurnosnim istraživanjima informacijskih sustava, osobito unutar bihevioralnih istraživanja informacijske sigurnosti [283], objašnjava kako ljudi izbjegavaju devijantno ponašanje u kontekstu društva, a temelji se na negativnim motivacijama urođenim u formalnim sankcijama [201], [67].

Glavni aspekti teorije su izvjesnost sankcija ili vjerojatnost kažnjavanja zbog kršenja određenih pravila, te strogoća sankcija ili stupanj kazne povezane s devijantnim ponašanjem [195]. Mehanizam za kažnjavanje obuhvaća zatvorsku kaznu, novčane kazne ili otpuštanje. Kako izvjesnost sankcije, tako i strogoća sankcije negativno utječu na namjere pojedinaca da se uključe u loše ponašanje u organizacijama [201]. D'Arcy i suradnici [284] potvrđuju ovu teoriju i primjećuju kako je manje vjerojatno da će zaposlenici zloupotrijebiti politiku sigurnosti informacija ako im je svijest o kazni visoka.

4.2.3.3. Teorija motivacije za zaštitom (engl. Protection Motivation Theory)

Teorija motivacije za zaštitom, razvijena je kako bi se razjasnio priziv straha (engl. *Fear Appeal*) [166] te tvrdi kako motivacija proizlazi iz procjene prijetnji i procjene suočavanja [195].

Procjena prijetnji sastoji se od percipirane ranjivosti, tj. procjene pojedinca o vjerojatnosti prijetećih događaja i percipirane ozbiljnosti, tj. težine posljedica događaja [166], dok se

procjena suočavanja odnosi na procjenu pojedinca o svojim sposobnostima da se nosi s potencijalnim gubitkom ili štetom nastalom prijetnjom i spriječi ih te se dijeli na tri čimbenika: samoefikasnost, učinkovitost odgovora i trošak odgovora [195]. Samoefikasnost je sposobnost ili prosudba pojedinca u vezi s njegovim sposobnostima usvajanja preporučenog ponašanja, učinkovitost odgovora uvjerenje pojedinca o uočenim koristima, dok trošak odgovora naglašava uočene oportunitetne troškove u vidu novčanih sredstava, vremena ili napora koji se ulažu u usvajanje preporučenog ponašanja [166].

Primjeri istraživanja iz domene informacijske sigurnosti koji su koristili ovu teoriju su istraživanja koja su proveli Ifinedo [166] te Johnston i Warkentin [285]. U slučaju istraživanja koje je proveo Ifinedo [166], percipirana ranjivost bile su prijetnje koje proizlaze iz neusklađenosti s politikom informacijske sigurnosti, percipirana ozbiljnost bile su neposredne prijetnje sigurnosti informacija organizacije proizišle iz neusklađenosti s politikom informacijske sigurnosti dok se samoefikasnost odnosila na vrste vještina i mjera potrebnih za zaštitu informacija u informacijskom sustavu, učinkovitost odgovora na poštivanje politike informacijske sigurnosti kao učinkovitog mehanizma za otkrivanje prijetnje informacijskoj imovini, a trošak odgovora predstavljao je uočene oportunitetne troškove u vidu vremena, novca i napora utrošenih na usklađenost sa sigurnosnom politikom. Rezultati tog istraživanja pokazali su da su se samoefikasnost, trošak odgovora i učinkovitost odgovora pozitivno odnosili na ponašanje usklađenosti [166]. Ovaj nalaz ne samo da potvrđuje teoriju, već pokazuje da su stavovi i percepcije zaposlenika, kao i njihova razina kompetentnosti važni za poticanje sigurnosne usklađenosti [195].

Rezultati drugog istraživanja [285], čiji je cilj bio istražiti utjecaj priziva straha na usklađenost krajnjih korisnika, pokazali su kako priziv straha utječe na namjere ponašanja korisnika oko usklađenosti s preporučenim pojedinačnim sigurnosnim radnjama, ali taj utjecaj nije ujednačen kod svih krajnjih korisnika.

4.2.3.4. Teorija društvenih veza (engl. Social Bond Theory)

Teorija društvenih veza sugerira kako društvene veze mogu odvratiti pojedinca od počinjenja zločina, bez obzira na njegovu sklonost. Ova je teorija uobičajena na području kriminologije i nastoji objasniti društveno ponašanje koje nije u skladu s društvenim pravilima [195].

Istraživanje koje su proveli Lee i Lee [286] pokazuje kako snažne društvene veze negativno utječu na namjere prema zloupotrebi računala. Teorija pokazuje da veze uključenosti mogu

ojačati uvjerenja da je zloupotreba računala društveno neprihvatljiva i može odvratiti pojedince od zlouporabe sigurnosnih politika. Međutim, postoji i obrnuti učinak: kada su društvene veze slabe, to može dovesti do povećane sklonosti kršenju utvrđene politike računalne sigurnosti [195].

4.2.3.5. Teorija društvenog učenja (engl. Social Learning Theory)

Slično teoriji društvenih veza**, teorija društvenog učenja** sugerira da na percepciju pojedinca prema počinjenju zločina mogu utjecati akcije i uvjerenja osoba s kojima se povezuju, čak i ako su rizik i kazna zločina veliki [195].

Ako se pojedinac udruži s delinkventnim kolegama njegov vlastiti osjećaj delinkvencije može se povećati. Istraživanja o utjecaju teorije društvenog učenja u organizacijama otkrila su da zloupotreba računala od strane vršnjaka, kao i osoba iz višeg menadžmenta, ima pozitivan odnos s motivacijom pojedinca da se uključi u zloupotrebu računala. Taj je učinak posebno snažan kada pojedinci imaju negativnu percepciju o organizaciji, bez obzira na razinu postojećih sigurnosnih mjera i politika [199], [195].

4.3. Čimbenici kulture informacijske sigurnosti

Uspostava pozitivne kulture informacijske sigurnosti učinkovit je način promicanja sigurnosnog ponašanja i praksi među zaposlenicima u organizaciji, zbog čega je potrebno razumjeti koji čimbenici čine kulturu informacijske sigurnosti [15], [54]. Ipak, iako se koncept kulture informacijske sigurnosti proučavao gotovo 20 godina, mnogi autori prepoznaju kako još uvijek ne postoji konsenzus o standardnom skupu dimenzija odnosno čimbenika koji čine kulturu informacijske sigurnosti već se koriste različite perspektive i koncepti što uzrokuje probleme istraživačima u identificiranju stvarnog koncepta kulture informacijske sigurnosti, kao i praktičarima u uspostavi i procjeni pozitivne kulture informacijske sigurnosti u organizaciji, ograničavajući tako njen puni potencijal [287], [15], [264], [163], [197], [287], [12], [252]. Dodatno, analiza koju su proveli da Veiga i suradnici [257] pokazala je da su znanstvene interpretacije definicija i čimbenika kulture informacijske sigurnosti mnogo šire od njihovog razumijevanja od strane industrije [257].

Mahfuth i suradnici [13] proveli su pregled relevantne literature kako bi identificirali kulturu informacijske sigurnosti na temelju definicija i okvira u studijama između 2003. i 2016. godine. Međutim, iako su uspjeli identificirati neke dimenzije kulture informacijske sigurnosti u svom pregledu, nije bilo daljnje analize tih dimenzija. Karlsson i suradnici [255] proveli su opsežni

pregled u rasponu od 2000. do 2013. godine klasificirajući istraživanja vezana uz kulturu informacijske sigurnosti temeljem četiri glavne kategorije: teme istraživanja, ishodišne teorije istraživanja, svrhe istraživanja i metoda istraživanja. Iako je ova studija dala značajna otkrića pružajući jasan sažetak pojedinih istraživanih tema, uključujući teorije i koncepte koji utječu na koncept kulture informacijske sigurnosti, ipak se nije usredotočila na to kako te ishodišne teorije utječu na dimenzije kulture informacijske sigurnosti. Alhogail i Mirza [11] u svom sustavnom pregledu literature o istraživanjima povezanim s kulturom informacijske sigurnosti za razdoblje od 2003. do 2013. godine otkrili su 12 od prepoznata 62 istraživanja koja su raspravljala o modelima i okvirima kulture informacijske sigurnosti, gdje je zanimljivo da su ovi modeli koristili međusobno različite dimenzije.

To je u skladu s rezultatima istraživanja koje su proveli Nasir i suradnici [244] koji su u svom pregledu identificirali više od 20 dimenzija kulture informacijske sigurnosti iz relevantnih istraživanja gdje su te dimenzije različite u pogledu broja, formiranja i definiranja u konceptualizaciji kulture informacijske sigurnosti. Također, isti autori otkrili su da se različiti izrazi koriste za označavanje iste dimenzije i naznaka da su dimenzije promijenjene nakon analize čimbenika i pouzdanosti što ukazuje da ne postoje široko prihvaćene dimenzije odnosno čimbenici za kulturu informacijske sigurnosti i da je i dalje to područje koje se razvija [287]. Ovaj opći nedostatak dogovora o tome što predstavlja kulturu informacijske sigurnosti predstavlja dilemu u smislu identificiranja čimbenika ili elemenata koji su potrebni za stvaranje kulture informacijske sigurnosti [288] te veliki jaz u istraživanjima kulture informacijske sigurnosti jer istraživači i praktičari nemaju pristup standardnom referentnom modelu kulture informacijske sigurnosti što zauzvrat ograničava daljnju generalizaciju i primjenu rezultata istraživanja vezanih za kulturu informacijske sigurnosti [287].

U konačnici, vidljivo je kako su potrebna dodatna istraživanja koja trebaju pružiti sveobuhvatni pogled koji vodi i integrira važne čimbenike koji oblikuju ili utječu na kulturu informacijske sigurnosti [264] budući da postoji prepoznati nedostatak znanja u prepoznavanju ključnih čimbenika i mjerenja njihovog utjecaja na kulturu informacijske sigurnosti [252] jer su empirijska istraživanja ponašanja krajnjih korisnika i čimbenika koji utječu na sigurnost kulture i dalje u svojim začecima, a praktična primjena odvojena od istraživanja [59].

4.4. Postojeći modeli i radni okviri kulture informacijske sigurnosti

Pregled literature otkrio je da postoji ograničen broj istraživanja koja su razvila okvir koji se može upotrijebiti za stvaranje i procjenu kulture informacijske sigurnosti da bi se osigurala učinkovitost takvog pristupa kao i valjanost sadržaja [264]. Štoviše, Alhogail i Mirza [11] utvrdili su da je samo 14 radova (22% od sveukupno identificiranih radova) predstavilo okvir. Osim toga, minimalan broj istraživanja koristio je isti okvir za stvaranje i procjenu kulture informacijske sigurnosti [264], a većini raspoloživih okvira nedostaje sveobuhvatan stav koji integrira ljude, organizaciju i tehnologiju kako bi putem cjelokupnog okvira pružio pomoć ljudima zaduženim za informacijsku sigurnost u organizaciji u provedbi i usvajanju kulture informacijske sigurnosti [11]. Stoga postoji snažna potreba za sveobuhvatnim okvirom za uspostavom i procjenom kulture koja je svjesna sigurnosti [258].

Karlsson i suradnici [255], na temelju provedenog pregleda istraživanja o kulturi informacijske sigurnosti između 2000. i 2013. godine, zaključili su kako nijedan rad u to vrijeme nije istraživao utjecaj ('plodove') kulture informacijske sigurnosti na sigurnost informacija u organizacijama. Daljnji pregled definicija i okvira kulture informacijske sigurnosti izveli su Mahfuth, Yussof, Baker i Ali [13] u rasponu od 2003. do 2016. godine, zaključujući da ne postoji standardna definicija kulture informacijske sigurnosti te utvrdili da su se akademske definicije kulture informacijske sigurnosti uglavnom usredotočile na Scheina [277] i njegov rad vezan uz organizacijsku kulturu, čiji je model korporativne kulture postao široko prihvaćen među istraživačima informacijske sigurnosti. Međutim, ovaj model opisuje korporativnu kulturu općenito, a ne posebno kulturu informacijske sigurnosti [95], [79]. Iz tog razloga, Van Niekerk i Von Solms [95] dodali su Scheinovom troslojnom modelu četvrti sloj, sloj znanja, koji omogućuje poboljšani model za opisivanje kulture informacijske sigurnosti budući da je, za uspostavu prihvatljive i učinkovite kulture informacijske sigurnosti, potrebno usredotočiti se na poboljšanje sigurnosnog ponašanja ljudi u organizacijama usredotočujući se na potrebna znanja zaposlenika [13].

Isto tako, Nasir, Arshah, Ab Hamid i Fahmy [287] proveli su sustavni pregled literature o kulturi informacijske sigurnosti i utvrdili da postoji nedosljednost u definiranju čimbenika koji konceptualiziraju idealnu kulturu informacijske sigurnosti, što još jednom ukazuje na potrebe daljnjeg istraživanja, ključnih čimbenika koji čine kulturu informacijske sigurnosti kako bi se mogao izraditi sveobuhvatan model odnosno radni okvir kulture informacijske sigurnosti.

Naposljetku, vlastitim pregledom relevantne literature utvrđeno je nekoliko desetaka radova koji se koncentriraju na dvadesetak modela odnosno radnih okvira kulture informacijske sigurnosti gdje se modeli i okviri predstavljeni u spomenutim radovima temelje na različitim pretpostavkama i problemima. U nastavku je dan kratak rezime tih modela i okvira, a Tablica 4.1. sažeto prikazuje spomenute okvire vezane za kulturu informacijske sigurnosti.

Schlienger i Teufel [179], [259] za svoju su analizu koristili radni okvir temeljen na Scheinovom modelu [276] koji se sastoji od tri razine koje čine artefakti, prihvaćene vrijednosti i dijeljene pretpostavke. U [259] razvijen je upitnik za procjenu kulture informacijske sigurnosti temeljen na Scheinovim razinama, nakon čega su autori u [179] predstavili radni okvir kulture informacijske sigurnosti organizacije u cilju stvaranja, promjene i održavanja kulture informacijske sigurnosti, a sam okvir temelji se na pet glavnih faza: pred-evaluacija, strateško planiranje, operativno planiranje, provedba i naknadna evaluacija.

Martins i Eloff [140], [160] ističu kako ponašanje zaposlenika ima značajan utjecaj na sigurnost informacija u organizaciji, a kako bi se pokušalo usmjeriti to ponašanje na pravi put, predlažu konceptualni okvir koji se sastoji od organizacijske, grupne i individualne razine na koje utječu promjene bilo iz tehnološke, ekonomske, ljudske, financijske ili neke druge perspektive. Organizacijsku razinu čine politike i procedure, analiza rizika, usporedba s drugima i budžet. Grupnu razinu čine rukovodstvo i povjerenje, a individualnu osviještenost i etičko ponašanje.

Skupina autora [198], [281], [191], [58] razvila je radni okvir za proučavanje kulture informacijske sigurnosti u organizaciji zasnovan na osam dimenzija okvira organizacijske kulture kako su ga predstavili Detert i suradnici [280]. Chia i suradnici [198] i [281] svoj rad temelje na osviještenosti o informacijskoj sigurnosti kako bi se proučio utjecaj organizacijske kulture na kulturu informacijske sigurnosti, gdje njihov zaključak pokazuje važnost podrške najvišeg menadžmenta i svijesti i uključenosti zaposlenika. Koh i suradnici [191] ispituju kako korporativno upravljanje sigurnošću utječe na kulturu informacijske sigurnosti, a posebno na osjećaj odgovornosti i vlasništva nad sigurnošću kod zaposlenika koji se bave informacijskom sigurnošću. Ruighaver i suradnici [58] raspravljaju o svakoj od osam dimenzija u smislu njezine korisnosti za izgradnju kulture informacijske sigurnosti te tvrde kako je idealna kultura informacijske sigurnosti ona koja je u ravnoteži između unutarnjih i vanjskih čimbenika.

Kraemer i Carayon [289] proveli su istraživanje o čimbenicima kulture računalne i informacijske sigurnosti putem intervjua rukovoditelja informacijske sigurnosti i sigurnosnih specijalista te mrežnih administratora te došli do šest ključnih dimenzija odnosno čimbenika

kulture računalne i informacijske sigurnosti koje čine sudjelovanje zaposlenika, obuka, prakse zapošljavanja, sustav nagrađivanja, podrška rukovodstva te komunikacija i povratna informacija.

Van Niekerk i Von Solms [162], [163], [95], [88] temelje svoj model kulture informacijske sigurnosti na Scheinovom modelu [276] organizacijske kulture odnosno trima razinama koje čine artefakti, prihvaćene vrijednosti i zajedničke prešutne pretpostavke uz dodatak četvrte razine koju čini znanje, budući da je znanje o informacijskoj sigurnosti preduvjet za obavljanje bilo kakvih aktivnosti na siguran način. Autori napominju kako u kulturi informacijske sigurnosti, upravo znanje podupire i podržava preostale tri razine organizacijske kulture. Nadalje, autori su na konceptualnoj razini predstavili različite interakcije između razina takve kulture informacijske sigurnosti. Stoga bi idealna kultura bila ona u kojoj su sve četiri temeljne razine jače od minimalno prihvatljive osnove, a također su savršeno usklađene jedna s drugom.

Dojkovski i suradnici [290], [291] u svom istraživanju ističu ključne probleme koji se tiču razvoja informacijske sigurnosti u australskim malim i srednjim poduzećima iznoseći ključne čimbenike kulture informacijske sigurnosti iz perspektive vlasnika poduzeća i samih zaposlenika. Ti čimbenici grupirani su u upravljačke čimbenike, kao što su, između ostalog politike i procedure, rukovodstvo ili upravljanje promjenama, čimbenike ponašanja, od kojih su neki odgovornost, povjerenje i motivacija, zatim individualno i organizacijsko učenje, učenje na daljinu, suradnja, kolaboracija i dijeljenje znanja te u konačnici etnička, nacionalna i organizacijska kultura kao čimbenik. Autori predlažu kako se glavni izazovi u razvoju kulture informacijske sigurnosti odnose na osviještenost vlasnika poduzeća i kontriranje opuštenom, neopterećenom pristupu sigurnosnim pitanjima koji je čest kod australskih zaposlenika [290].

Dojkovski i suradnici [139], [292] predstavili su dodatnu modifikaciju prethodnog radnog okvira koja je osmišljena kako bi se poboljšala primjena kulture informacijske sigurnosti u malim i srednjim poduzećima u Australiji. Identificirali su tri vanjska utjecaja: nacionalnu i etičku kulturu; vladine inicijative za podizanje svijesti i postavljanje usporedbe informacijske sigurnosti; te dobavljače koji malim i srednjim poduzećima mogu ponuditi pouzdanost. Nadalje, autori su identificirali brojne unutarnje utjecaje, uključujući korporativno upravljanje; organizacijsku kulturu koja ima velik utjecaj na kulturu informacijske sigurnosti; upravljačke čimbenike kao što su, između ostalog, sigurnosne politike i procedure, analiza rizika ili budžet. Pored toga, individualno i organizacijsko učenje, uključujući učenje na daljinu, obuka i edukacija može biti vrijedna inicijativa za razvoj kulture informacijske sigurnosti za mala i

srednja poduzeća. Također, osviještenost je ključna za stvaranje i njegovanje pozitivne kulture informacijske sigurnosti, kao i redovito pregledavanje i ocjenjivanje mjera za održavanje kulture informacijske sigurnosti. Također, čimbenici ponašanja koji uključuju niz vanjskih i unutarnjih inicijativa za stvaranje poželjnog sigurnosnog ponašanja. U konačnici, autori tvrde kako je potrebna usredotočenost rukovodstva na jačanje svijesti zaposlenih o kulturi informacijske sigurnosti i strateški planovi kako bi se osiguralo da se kultura informacijske sigurnosti može ugraditi u organizaciju.

Alnatheer i Nelson [254], [15] predložili su radni okvir za razumijevanje kulture informacijske sigurnosti i njezine prakse u kontekstu Saudijske Arabije. Njihov se rad fokusira na procese implementacije i usvajanja informacijske sigurnosti identificirajući kulturološke čimbenike i pitanja te čimbenike i pitanja upravljanja informacijskom sigurnošću koji pomažu u tom pogledu. Cilj njihova okvira je istražiti je li kultura informacijske sigurnosti prerasla u prakse u organizacijama Saudijske Arabije. Na temelju pregleda literature, autori su identificirali sedam čimbenika (podrška rukovodstva; uspostava učinkovite sigurnosne politike; sigurnosna osviještenost; sigurnosna obuka; procjena i analiza rizika informacijske sigurnosti; politike etičkog ponašanja; sigurnosna usklađenost) kulture informacijske sigurnosti [254] koje svrstavaju u četiri dimenzije koje utječu na kulturu informacijske sigurnosti (korporativno upravljanje; pravno i regulatorno okruženje; građani; nacionalna kultura) [15]. Međutim, nedostaje objašnjenje kako se ovi čimbenici mogu koristiti.

Da Veiga i Eloff [245] predložili su radni okvir za razvoj kulture informacijske sigurnosti unutar organizacije koji se temelji na komponentama informacijske sigurnosti. Tako su u predloženom okviru naveli niz komponenti informacijske sigurnosti koje bi organizacije trebale primijeniti kako bi se pomoglo u rješavanju ljudskih, procesnih i tehničkih prijetnji koje bi spriječile uspostavljanje prihvatljive kulture informacijske sigurnosti unutar organizacije. Skup komponenata informacijske sigurnosti potom je grupiran u kategorije gdje organizacija te komponente provodi na individualnoj, grupnoj ili organizacijskoj razini sigurnosnog ponašanja. Time se naglašava da sigurnosno ponašanje utječe i pokazuje se na svim razinama. Rezultat primjene ovog okvira je kultura informacijske sigurnosti. Međutim, okvir ipak nema prikaz mogućeg odnosa i utjecaja između različitih identificiranih komponenti kulture informacijske sigurnosti.

Lim i suradnici [293], [68] predložili su radni okvir koji pomaže organizacijama u određivanju u kojoj je mjeri željena kultura informacijske sigurnosti ugrađena u organizacijsku kulturu te

istražuje prirodu odnosa među njima. Autori klasificiraju prirodu odnosa kao jedan od tri tipa: kultura informacijske sigurnosti je odvojena od organizacijske kulture, kultura informacijske sigurnosti je supkultura organizacijske kulture ili kultura informacijske sigurnosti je ugrađena u organizacijsku kulturu. Njihov se radni okvir temelji na osam dimenzija okvira organizacijske kulture koji su razvili Detert i suradnici [280] te navode kako je važno ugraditi koncept kulture informacijske sigurnosti u organizacije koja ima za cilj utjecati na sigurnosno ponašanje i postupke zaposlenika [68] dok razina do koje je kultura informacijske sigurnosti ugrađena u organizacijsku kulturu ovisi o pet čimbenika.

Alfawaz i suradnici [261] predstavili su konceptualni okvir za klasifikaciju i organiziranje obilježja organizacijskih subjekata koji su uključeni u prakse informacijske sigurnosti, identificirajući kako znanje, vještine i individualne preferencije utječu na pojedinačne i grupne prakse u pogledu upravljanja informacijskom sigurnošću. Ovaj se konceptualni okvir fokusirao na utjecaj nacionalne i/ili organizacijske kulture, a identificirali su četiri načina ponašanja: 1) „ne znati – ne raditi" način rada; 2) „ne znati – raditi" način rada; 3) „znati – ne raditi" način rada i u konačnici 4) „znati – raditi" način rada. Ponašanje zaposlenika može se mijenjati iz jednog u drugi način, ovisno o organizacijskoj ulozi, stanju tehnološkog razvoja te statusu i dostupnosti sigurnosne obuke.

Hassan i Ismail [59] predstavili su konceptualni model kulture informacijske sigurnosti u kontekstu zdravstvenog sektora. Na temelju pregleda literature identificirali su šest čimbenika koji utječu na kulturu informacijske sigurnosti: ponašanje, upravljanje promjenama, svijest o informacijskoj sigurnosti, sigurnosni zahtjevi, organizacijski sustav i znanje. No, postavljeni model ostao je samo u teoretskoj sferi budući da ga autori nisu validirali empirijskim istraživanjem.

Lopes i Oliveira [54] predložili su utvrđivanje postoji li kultura informacijske sigurnosti u malim i srednjim organizacijama na temelju 11 čimbenika koji su preuzeti iz međunarodne norme ISO/IEC 27002:2005. Autori smatraju kako se može reći da u onim organizacijama kod kojih je usvojeno barem pet identificiranih čimbenika postoji kultura informacijske sigurnosti. Sam okvir ne donosi neku novost budući da koristi otprije definirane čimbenike odnosno kategorije dobre prakse upravljanja informacijskom sigurnošću.

Da Veiga i Martins [80], [17], [294] ističu kako je ključno razumjeti stavove i ponašanje zaposlenika kako bi se mogla oblikovati kultura informacijske sigurnosti na način da se poštuju

odredbe sigurnosne politike i zaštite informacije koje organizacija posjeduje. Autori su razvili upitnik za procjenu kulture informacijske sigurnosti (engl. *Information security culture assessment – ISCA*) koji pomaže u identifikaciji dijelova koje organizacija treba poboljšati kako bi unaprijedila zaštitu osjetljivih informacija od ljudskih prijetnji. Pomoću ISCA upitnika autori su proveli četiri procjene kulture informacijske sigurnosti u 12 država tijekom perioda od osam godina. Uz područja koja je bilo potrebno unaprijediti, podaci su pokazali i kako su sigurnosna obuka i podizanje svijesti o informacijskoj sigurnosti značajni čimbenici koji pozitivno utječu na kulturu informacijske sigurnosti. ISCA upitnik se prvo sastojao od osam čimbenika (upravljanje informacijskom imovinom; upravljanje informacijskom sigurnošću; upravljanje promjenama; upravljanje korisnicima; politike informacijske sigurnosti; program informacijske sigurnosti; povjerenje; vodstvo informacijske sigurnosti) [80], nakon čega je dodan dodatni čimbenik „obuka i osviještenost" [17], odnosno „percepcija privatnosti" kao deseti čimbenik [294].

Alhogail i Mirza [138], [258], [253], [6] razvili su radni okvir koji se fokusira na sigurnosno ponašanje, a koji se sastoji od pet dimenzija (strategija, tehnologija, organizacija, ljudi i okolina) te integrira upravljanje promjenama i ljudski čimbenik u informacijskoj sigurnosti. Valjanost i pouzdanost okvira autori su potvrđivali kombinacijom kvantitativnih podataka iz upitnika i kvalitativnih podataka iz intervjua. Kako autori ističu, okvir je nastao iz razloga što većini dostupnih okvira nedostaje cjelovit pogled koji integrira ljude, organizaciju i tehnologiju u procjeni kulture informacijske sigurnosti.

Chen i suradnici [164] predložili su istraživački model kako bi istražili utjecaj programa podizanja svijesti o informacijskoj sigurnosti na stvaranje kulture informacijske sigurnosti. Rezultat ukazuje da programi sigurnosne edukacije, obuke i osvješćivanja kao i nadzor sigurnosti imaju pozitivan utjecaj na kulturu informacijske sigurnosti i svijest zaposlenika u pogledu organizacijske sigurnosne politike. Dodatno, otkrili su da postoji pozitivan odnos između svijesti o nadzoru sigurnosti i kulture informacijske kulture.

Tang i suradnici [8] razvili su okvir kulture informacijske sigurnosti koji integrira ljudske, organizacijske i tehnološke poglede upravljanja informacijskom sigurnošću, a uključuje četiri dimenzije koje čine usklađenost, komunikacija, odgovornost i upravljanje. Dimenzija 'usklađenost' uglavnom se odnosi na usklađenost zaposlenika s politikama informacijske sigurnosti, posebice u pogledu njihove spremnosti na promjenu radne prakse kako bi se osigurala sigurnost informacijske imovine, njihova predanost politici informacijske sigurnosti

i njihova uvjerenja glede odgovarajuće zaštite informacija. Dimenzija 'komunikacija' odnosi se na način na koji organizacija objašnjava svoje politike informacijske sigurnosti zaposlenicima, kako informira zaposlenike o osobnim utjecajima promjena informacijske sigurnosti i o očekivanjima zaposlenika glede informacijske sigurnosti. Dimenzija 'odgovornost' odnosi se na odgovor organizacije na kršenje politika informacijske sigurnosti od strane zaposlenika, što uključuje akcije koje će organizacija poduzeti ako se zaposlenici ne pridržavaju politika informacijske sigurnosti, osjećaju li se zaposlenici sigurno u organizaciji i smatraju li se zaposlenici odgovornima kad prekrše organizacijska pravila odnosno politike informacijske sigurnosti. Naposljetku, dimenzija 'upravljanje' uključuje pozicioniranje informacijske sigurnosti u organizaciji, poštivanje politike informacijske sigurnosti od strane rukovodstva, kontrole postavljene na imovinu informacijske sigurnosti i percepciju važnosti informacijske sigurnosti na razini rukovodstva [8].

Tolah i suradnici [264], na temelju analize literature, predstavili su konceptualni okvir sastavljen od sedam čimbenika, uzimajući u obzir identificirane ljudske čimbenike koji se mogu koristiti za mjerenje razine kulture informacijske sigurnosti kako bi pomogli istraživačima i praktičarima razumjeti složenost i izazove vezane uz kulturu informacijske sigurnosti.

Masrek i suradnici [250], [192] predstavili su radni okvir za procjenu kulture informacijske sigurnosti na temelju šest identificiranih dimenzija kulture informacijske sigurnosti u kontekstu malezijskih javnih organizacija. Upitnik koji čini temelj okvira nastao je na temelju analize literature te verificiran putem intervjua s ekspertima. U upitniku je sudjelovalo 293 voditelja IT odjela, a rezultati su pokazali kako su sve identificirane dimenzije ključne u razvoju kulture informacijske sigurnosti.

Glaspie i Karwowski [5] predstavili su pregled literature o kulturi informacijske sigurnosti ocrtavajući čimbenike koji doprinose kulturi informacijske sigurnosti u organizaciji, na temelju čega su izradili konceptualni okvir sastavljen od pet ključnih čimbenika pronađenih u literaturi (podrška rukovodstva; stavovi i uključenost; obuka i osviještenost; politika informacijske sigurnosti; odvraćanje i poticanje).

Da Veiga i sur. [257] razvili su organizacijski model kulture informacijske sigurnosti povezujući koncepte koji čine kulturu informacijske sigurnosti dobivene iz znanstvene literature i perspektive iz prakse. Analiza je pokazala da su znanstvene interpretacije čimbenika koji mogu pozitivno utjecati na kulturu informacijske sigurnosti mnogo šire od shvaćanja industrije. Na temelju pregleda literature, autori su identificirali ukupno 25 čimbenika koji

mogu pomoći u uspostavi kulture informacijske sigurnosti u organizaciji s teoretskog stajališta dok su polustrukturiranim intervjuom s predstavnicima industrije došli do 9 glavnih osobina idealne kulture informacijske sigurnosti kako ih vidi praksa. Te osobine su: zaštićene i sigurne informacije; osviješteni i educirani zaposlenici; usklađenost; savjesno ponašanje; primjereni sustavi; obuka, osviještenost, edukacija i komunikacija; integritet; politike i procedure te podrška rukovodstva i vodstvo.

Tablica 4.1. Modeli i okviri kulture informacijske sigurnosti

Rbr.	**Autori**	**Dimenzije/čimbenici**
1.	Schlienger i Teufel (2003) [179]; Schlienger i Teufel (2003) [259]	artefakti; prihvaćene vrijednosti; dijeljene pretpostavke;
2.	Martins i Eloff (2002) [140]; Martins i Eloff (2002) [160]	promjena; politike i procedure; vrednovanje; analiza rizika; budžet; rukovodstvo; povjerenje; osviještenost; etičko ponašanje
3.	Chia, Maynard i Ruighaver (2002) [198]; Chia, Maynard i Ruighaver [281]; Koh, Ruighaver, Maynard i Ahmad (2005) [191]; Ruighaver, Maynard i Chang (2007) [58];	osnove istine i racionalnosti; priroda vremena i vremenski horizont; motivacija; stabilnost naspram promjene/inovacije/osobnog rasta; orijentacija na posao, zadatak, suradnike; izolacija naspram suradnje; kontrola, koordinacija i odgovornost; orijentacija i unutarnji i/ili vanjski fokus
4.	Kraemer i Carayon (2005) [289]	sudjelovanje zaposlenika; obuka; prakse zapošljavanja; sustav nagrađivanja; podrška rukovodstva; komunikacija i povratna informacija
5.	Van Niekerk i Von Solms (2005) [162]; Van Niekerk i Von Solms (2006)[163]; Van Niekerk i Von Solms (2010) [95]; Van Niekerk i Von Solms (2013) [88]	artefakti; prihvaćene vrijednosti; dijeljene pretpostavke; znanje
6.	Dojkovski, Lichtenstein i Warren (2006) [290]; Dojkovski, Lichtenstein i Warren (2007) [291]	politike i procedure; vrednovanje; analiza rizika; budžet; rukovodstvo; odgovor; obuka; edukacija; osviještenost; upravljanje promjenama; odgovornost; integritet; povjerenje; etičnost; vrijednosti; motivacija; orijentacija; osobni rast; kooperacija, kolaboracija i dijeljenje znanja; individualno i organizacijsko učenje; etička, nacionalna i organizacijska kultura

Tablica 4.1. Modeli i okviri kulture informacijske sigurnosti (nastavak)

Rbr.	Autori	Dimenzije/čimbenici
7.	Dojkovski, Lichtenstein i Warren (2007) [139]; Dojkovski, Lichtenstein i Warren (2010) [292]	analiza rizika; budžet; politike i procedure; odgovor; samoprocjena; ugovor o zapošljavanju; e-učenje; obuka; edukacija; neformalna osviještenost; marketing; odgovornost; integritet; povjerenje; etičnost; vrijednosti; motivacija; orijentacija; osobni rast
8.	Alnatheer i Nelson (2009) [254]; Alnatheer (2014) [15]	podrška rukovodstva; uspostava učinkovite sigurnosne politike; sigurnosna osviještenost; sigurnosna obuka; procjena i analiza rizika informacijske sigurnosti; politike etičkog ponašanja; sigurnosna usklađenost
9.	Da Veiga i Eloff (2010) [245]	vođenje i upravljanje; upravljanje sigurnošću i operacijama; sigurnosne politike; upravljanje sigurnosnim programima; upravljanje sigurnošću korisnika; zaštita tehnologije i rad; upravljanje promjenama
10.	Lim, Ahmad, Chang i Maynard (2010) [293]; Lim, Chang, Maynard i Ahmad [68]	uključenost rukovodstva u sigurnosne prakse; dodjela odgovornosti za sigurnost; provođenje sigurnosne politike; sigurnosna osviještenost; sigurnosna obuka i alokacija budžeta za sigurnost
11.	Alfawaz, Nelson i Mohannak (2010) [261]	znanje; vještine; individualne preferencije
12.	Hassan i Ismail (2012) [59]	ponašanje; upravljanje promjenama; svijest o informacijskoj sigurnosti; sigurnosni zahtjevi; organizacijski sustav; znanje
13.	Lopes i Oliveira (2014) [54]	sigurnosna politika; organizacija informacijske sigurnosti; upravljanje imovinom; sigurnost ljudskih resursa; fizička sigurnost i sigurnost okoline; upravljanje komunikacijama i operacijama; kontrola pristupa; nabava, razvoj i održavanje informacijskih sustava; upravljanje incidentima informacijske sigurnosti; upravljanje kontinuitetom poslovanja; sukladnost
14.	Martins i Da Veiga [80]; Da Veiga i Martins* [17]; Martins i Da Veiga [294]**	upravljanje informacijskom imovinom; upravljanje informacijskom sigurnošću; upravljanje promjenama; upravljanje korisnicima; politike informacijske sigurnosti; program informacijske sigurnosti; povjerenje; vodstvo informacijske sigurnosti; obuka i osviještenost*; percepcija privatnosti**
15.	Alhogail i Mirza (2014) [138]; Alhogail i Mirza (2015) [258] Alhogail (2015) [253]; Alhogail (2015) [6];	strategija; tehnologija; organizacija; ljudi; okolina

Tablica 4.1. Modeli i okviri kulture informacijske sigurnosti (nastavak)

Rbr.	Autori	Dimenzije/čimbenici
16.	Chen, Ramamurthy i Wen (2015) [164]	sigurnosne politike; program edukacije, obuke i podizanja svijesti; nadzor sigurnosti
17.	Tang, Li i Zhang [8]	usklađenost; komunikacija; odgovornost; upravljanje
18.	Tolah, Furnell i Papadaki (2017) [264]	podrška rukovodstva; sigurnosna politika; sigurnosna edukacija i obuka, procjena rizika; etičko ponašanje; zadovoljstvo poslom; vlastite osobine
19.	Masrek (2017) [250]; Masrek, Nazrin Harun, Khairulnizan Zaini (2017) [192]	podrška rukovodstva; politike i procedure; usklađenost; osviještenost; budžet; tehnologija
20.	Glaspie i Karwowski (2018) [5]	podrška rukovodstva; stavovi i uključenost; obuka i osviještenost; politika informacijske sigurnosti; odvraćanje i poticanje
21.	Da Veiga, Astakhova, Botha i Herselman (2020) [257]	unutarnji čimbenici (unutarnje stanje organizacije; životni ciklus organizacije; razina cjelokupne organizacijske kulture; sustav zaštite informacija; resursi; rukovodstvo; politike i procedure informacijske sigurnosti; upravljanje rizicima informacijske sigurnosti; upravljanje operacijama; upravljanje promjenama; upravljanje sigurnošću zaposlenika; sigurnosna edukacija, obuka i osviještenost; upravljanje sigurnosnim ponašanjem; osobnost i vrijednosti; potrebe; emocionalno stanje; znanje o informacijskoj sigurnosti; usklađenost s informacijskom sigurnošću; uzajamno povjerenje zaposlenika i poslodavca te samih zaposlenika međusobno; povjerenje kupaca u organizaciju) i vanjski čimbenici (nacionalna kultura; politički i zakonodavni čimbenici; ekonomski čimbenici; socio-kulturološki čimbenici; tehnički i tehnološki čimbenici)

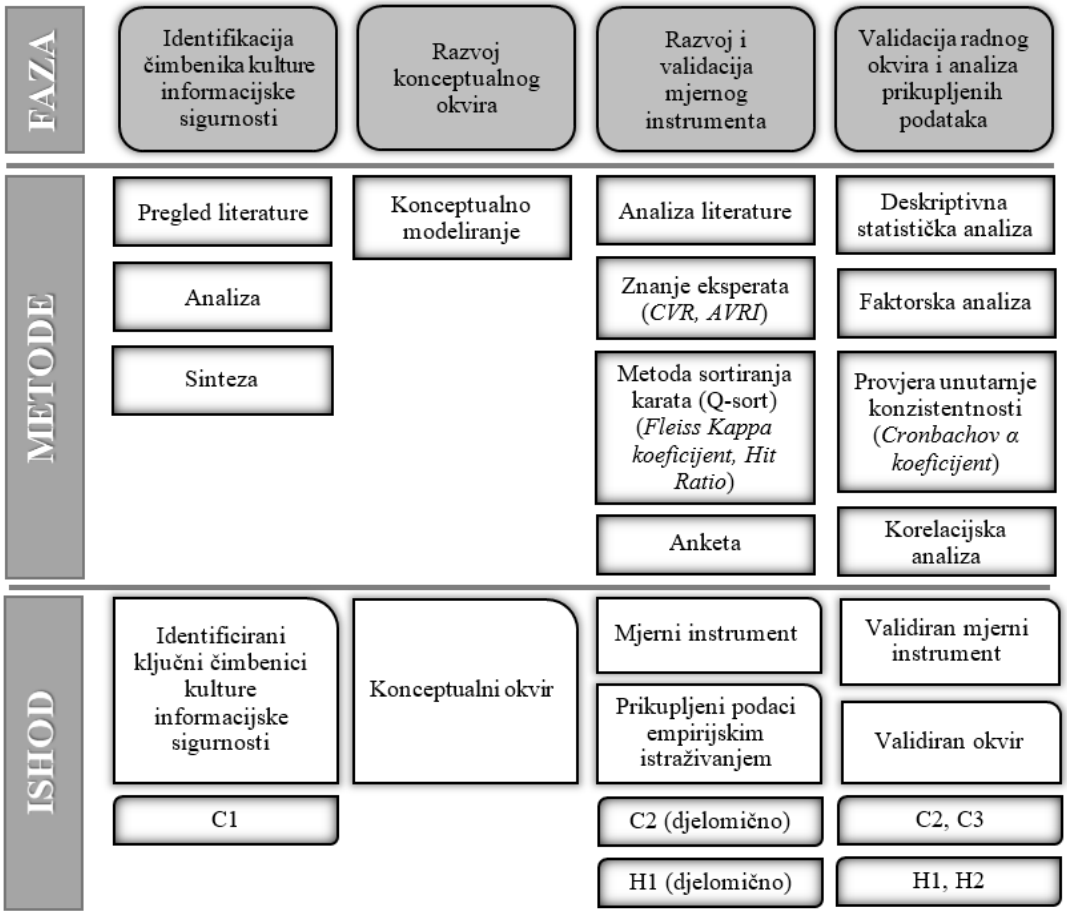
Izvor: *vlastiti prikaz*

Iz navedenog je vidljivo da većina identificiranih okvira i modela pokušava riješiti različita pitanja, zbog čega oni nisu izravno usporedivi jer ne sadrže iste čimbenike. Također, neki od tih okvira ostali su na konceptualnoj razini te nisu validirani empirijskim istraživanjem. Nadalje, smatra se da su različita okruženja i različite pretpostavke formulirali svaki okvir kulture informacijske sigurnosti te su tako neki okviri usredotočeni na rješavanje ljudskih čimbenika, poput pružanja svijesti, programa obuke i edukacije za zaposlenike, neki zanemaruju tehnološku komponentu kulture informacijske sigurnosti dok se neki radovi

usredotočuju isključivo na vanjske čimbenike koji utječu na kulturu informacijske sigurnosti. Međutim, većini raspoloživih okvira nedostaje sveobuhvatno stajalište koje bi integriralo ljude, organizaciju i tehnologiju kako bi organizacijama pružilo sveobuhvatni okvir za pomoć praktičaru informacijske sigurnosti unutar organizacije u primjeni i usvajanju kulture informacijske sigurnosti, kao što su prepoznali i AlHogail i Mirza [258] u svom pregledu literature. Sve to navodi na zaključak kako postoji snažna potreba za sveobuhvatnim okvirom za uspostavom i procjenom kulture informacijske sigurnosti.

5. METODOLOGIJA ISTRAŽIVANJA

Tkalac Verčić i sur. [295] definiraju istraživanje kao „*unaprijed osmišljen, logičan i sustavan proces kojim povezujemo mišljenja i iskustva, dolazimo do novih spoznaja i povećavamo znanje*", a istraživanje u sklopu ove doktorske disertacije sastoji od teoretskog i empirijskog dijela podijeljenih u nekoliko faza temeljenih na upotrebi znanstvenih kvalitativnih i kvantitativnih metoda (Slika 5.1.). Prednost kombiniranja kvalitativnog i kvantitativnog pristupa pri prikupljanju i analizi podataka stjecanje je boljeg razumijevanja problema koji se proučava [296]. Prva faza istraživanja odnosi se na identificiranje ključnih čimbenika kulture informacijske sigurnosti u organizacijskom kontekstu, drugu fazu čini razvoj konceptualnog okvira, treća faza sastoji se od razvoja i validacije mjernog instrumenta, a završna, četvrta faza odnosi se na validaciju okvira i analizu podataka dobivenih empirijskim istraživanjem. Ovdje je važno naglasiti kako pojedine faze ovog istraživanja nisu strogo odvojene već se u nekim dijelovima faze preklapaju ili aktivnosti iz pojedinih faza traju paralelno.



Legenda: CVR (*Content Validity Ratio*) – omjer sadržajne valjanosti; AVRI (*Averaged value of relative importance*) – prosječna vrijednost relativne važnosti; Hit Ratio – omjer pogodaka; C – cilj istraživanja; H – hipoteza istraživanja

Slika 5.1. Hodogram istraživanja

5.1. Identifikacija čimbenika kulture informacijske sigurnosti

Tijekom prve faze istraživanja, korištenjem znanstvenih metoda pregleda, analize i sinteze dostupnih relevantnih istraživanja iz područja kulture informacijske sigurnosti identificirani su ključni čimbenici kulture informacijske sigurnosti u organizacijskom kontekstu, čime je postignut prvi postavljeni cilj istraživanja.

Pregled relevantne literature daje uvid u druga istraživanja koja su vezana uz istraživanje koje se trenutno provodi čime daje temelj za obrazloženje važnosti trenutnog istraživanja kao i mogućnost usporedbe sa srodnim istraživanjima [296]. Drugim riječima, svrha pregleda literature je pružanje obrazloženja potrebe za trenutnim istraživanjem pokazujući da se druga istraživanja nisu bavila istom temom na potpuno isti način te ujedno pokazuje da je istraživač upoznat s dosadašnjim istraživanjima vezanim uz neku temu [297].

Prilikom pregleda literature, autor ove disertacije obratio je pozornost na najčešće pogreške pri prikupljanju literature, kao što su: premalo izvora literature, zastarjeli izvori literature, preopćeniti izvori literature, izvori literature koji nisu povezani s područjem istraživanja ili izostavljanje znanstvenih članaka i pisanje isključivo na temelju knjiga [295].

5.2. Razvoj konceptualnog okvira

Tijekom ove faze istraživanja, korištenjem metode konceptualnog modeliranja izrađen je konceptualni okvir za procjenu i unapređenje kulture informacijske sigurnosti u vidu definiranja kategorija okvira i sastavnih dijelova pojedine kategorije temeljenih na rezultatima prve faze istraživanja.

Konceptualni okvir je struktura za koju istraživač vjeruje da može najbolje objasniti istraživački problem koji se proučava, a koji se odnosi na određene ideje koje istraživač koristi u svom istraživanju [298]. Razvijeni konceptualni okvir u sklopu ovog istraživanja temelji se na konceptima međusobno povezanih varijabli kojima se pokušava objasniti istraživački problem, a nastao je na temelju koncepata koje je predložio autor ove disertacije, empirijskim istraživanjem i važnim teorijama korištenim za sistematizaciju znanja iz područja kulture informacijske sigurnosti.

Predloženi okvir u ovom istraživanju čine manifestne ili promatrane varijable (čestice) kojima se opisuju latentne varijable prve razine (čimbenici) te latentne varijable druge razine (kategorije) koje su opisane tim čimbenicima. *Manifestne ili promatrane varijable* su koncepti

koji se mogu izravno promatrati i mjeriti dok su *latentne varijable ili konstrukti* teoretski koncepti koji se ne mogu izravno promatrati ili mjeriti, već se o njima mogu donositi zaključci tek na temelju manifestnih varijabli [299]. Konceptualni okvir prikazan je u obliku hijerarhijskog dijagrama budući da dijagrami predstavljaju uobičajeni način prikazivanja konceptualnih okvira kako bi se jasno definirale konstrukcije ili varijable teme istraživanja i njihovi odnosi [298].

5.3. Razvoj i validacija mjernog instrumenta

Treća faza istraživanja, koja je ujedno i najopširnija, sastoji se od izrade i validacije mjernog instrumenta. Mejovšek [300] definira mjerni instrument kao „*sredstvo pomoću kojeg se određuje kvantiteta obilježja koje je predmetom mjerenja*" dok Creswell [297] navodi da je instrument „*alat za mjerenje, promatranje ili dokumentiranje kvantitativnih podataka*", a koji sadrži konkretna pitanja i mogućnosti odgovora na ta pitanja, razvijena prije provođenja samog istraživanja. Anketni upitnici kao mjerni instrumenti „za prikupljanje podataka o stavovima i mišljenjima na reprezentativnom uzorku ispitanika" [301] korisna su metoda istraživanja koja omogućuje izravno kvantificiranje subjektivnih stavova sudionika, a u društvenim znanostima predstavljaju temeljni mjerni instrument za prikupljanje podataka [300].

Dodatno, jednostavno ih je implementirati, a pružaju standardizirani način za kvantificiranje određenog aspekta koji se razmatra.

Ovo istraživanje rezultiralo je izradom i validacijom novog mjernog instrumenta pri čemu su se slijedile smjernice koje su predložili Moore i Benbasat [302] koje se sastoje od tri koraka: (1) *kreiranje čestica mjernog instrumenta,* (2) *razvoj mjerne skale (konstrukata)* i (3) *testiranje mjernog instrumenta*.

5.3.1. Kreiranje čestica mjernog instrumenta

Kreiranje čestica mjernog instrumenta temeljilo se na pretraživanju literature iz domene kulture informacijske sigurnosti, na način da su se izdvojile čestice koje su se do sada koristile za opis i mjerenje prepoznatih čimbenika koji utječu na kulturu informacijske sigurnosti, odnosno kreiranje čestica temeljeno je na rezultatima dobivenim u prvoj fazi istraživanja. Pod pojmom 'čestice' podrazumijevaju se tvrdnje u mjernom instrumentu koje služe vrednovanju percipiranih čimbenika kulture informacijske sigurnosti unutar organizacije.

Broj čestica koje mjere pojedini čimbenik kulture informacijske sigurnosti trebao bi na odgovarajući način uzorkovati područje od interesa budući da mjerni instrument s previše čestica može potaknuti pristranost uzorka odgovora (sudionici će davati iste odgovore na različita pitanja), dok one s premalo čestica mogu ugroziti valjanost mjernog instrumenta [303]. Tako Hair i suradnici [304] napominju kako bi trebalo postojati minimalno tri čestice odnosno pitanja po pojedinom konstruktu koji se ispituje. Također, prilikom kreiranja čestica potrebno je, između ostalog, voditi računa da svaka čestica obuhvaća samo jedno pitanje, da se ne koriste nedovoljno sažeti ponuđeni odgovori, negativna ili dvostruko negativna pitanja ili da se ne koriste pitanja koja mogu sugerirati određeni odgovor kao ni emocionalno obojene i stereotipne riječi [301].

5.3.2. Razvoj mjerne skale

Kako bi se osigurala kvaliteta postupaka mjerenja i statističkog zaključivanja, mjerni instrument (kao i radni okvir koji će nastati na temelju mjernog instrumenta) trebaju udovoljavati metrijskim karakteristikama valjanosti (engl. *Validity*) i pouzdanosti (engl. *Reliability*). **Valjanost** uključuje pitanja kako rezultati istraživanja ocrtavaju stvarnost, odnosno označava svojstvo da mjerni instrument stvarno mjeri ono što se tvrdi da mjeri, dok s druge strane, **pouzdanost** predstavlja opseg u kojem se rezultati istraživanja mogu ponoviti tijekom vremena ili kroz različite grupe sudionika, odnosno rješava pitanje ako se istraživanje ponovi, hoće li ono dati iste rezultate [305].

Straub i suradnici [306] sugeriraju da se u postupku utvrđivanja sadržajne valjanosti treba koristiti pregled literature i ekspertno mišljenje te se u ovom dijelu istraživanja kontaktirao prigodni (raspoloživi) uzorak eksperata radi sudjelovanja u provjeri sadržajne valjanosti (engl. *Content Validity*) i konstruktne valjanosti (engl. *Construct Validity*) izdvojenih čestica. U kontekstu ovog istraživanja pod pojmom „eksperti" podrazumijevaju se certificirani profesionalci iz područja informacijske sigurnosti ili revizije informacijskih sustava.

5.3.2.1. Sadržajna valjanost

Sadržajna valjanost jedna je od osnovnih metrijskih karakteristika mjernog instrumenta, a svrha procjene sadržajne valjanosti je utvrditi mjeru do koje čestice obuhvaćaju opseg i dubinu tema koje mjerni instrument namjerava obraditi [307] odnosno stupanj u kojem čestice predstavljaju konstrukt koji se mjeri [306].

U tu svrhu, kontaktirani su eksperti kako bi procijenili prikladnost predloženih čestica, čimbenika i kategorija mjernog instrumenta na temelju njihovog znanja i iskustva u kontekstu kulture informacijske sigurnosti. Provjera sadržajne valjanosti računala se putem dva empirijska pokazatelja: omjera sadržajne valjanosti (engl. *Content Validity Ratio - CVR*) i prosječne vrijednosti relativne važnosti (engl. *Averaged value of relative importance - AVRI*).

Kako bi se utvrdio **omjer sadržajne valjanosti** (eng. *Content Validity Ratio - CVR*), eksperti trebaju svakoj čestici, čimbeniku i kategoriji odrediti relativnu važnost preko skale od tri stupnja (1 – obavezna, 2 – poželjna, 3 – nepotrebna), nakon čega se CVR računa prema modificiranoj formuli koju je predložio Lawshe [308]:

$$CVR = \frac{n - \frac{N}{2}}{\frac{N}{2}}$$

gdje je: *n* broj eksperata koji su procijenili pojedinu česticu, čimbenik i kategoriju kao 'obaveznu' ili 'poželjnu' dok *N* predstavlja ukupan broj eksperata koji su sudjelovali. CVR može poprimiti vrijednosti od -1 do +1, gdje minimalna vrijednost CVR-a kojom se utvrđuje sadržajna valjanost ovisi o broju eksperata, sukladno kriterijima kako ih navodi Lawshe [308] u Tablici 5.1.

Tablica 5.1. Minimalne vrijednosti omjera sadržajne valjanosti u odnosu na broj eksperata

Broj eksperata	Minimalna vrijednost CVR-a
5	0,99
6	0,99
7	0,99
8	0,78
9	0,75
10	0,62
11	0,59
12	0,56
13	0,54
14	0,51
15	0,49
20	0,42
25	0,37
30	0,33
35	0,31
40	0,29

Izvor: [308]

Na temelju dobivenih vrijednosti CVR-a, iz daljnjih koraka razvoja mjernog instrumenta izostavljaju se one čestice, čimbenici i kategorije koje imaju CVR manji od minimalne vrijednosti iz Tablice 5.1., ovisno o broju eksperata koji su sudjelovali u istraživanju.

Drugi empirijski kriterij za utvrđivanje sadržajne valjanosti, **prosječna vrijednost relativne važnosti** pojedine čestice, čimbenika i kategorije, izračunava se kao aritmetička sredina svih vrijednosti relativne važnosti koje su pridružene pojedinoj čestici, čimbeniku i kategoriji [309]. U kontekstu ranije navedene skale od tri stupnja koja se koristila u ovom istraživanju za procjenu eksperata, iz daljnjih koraka potrebno je izuzeti sve čestice, čimbenike i kategorije kojima je prosječna vrijednost relativne važnosti veća od 2, što znači da je većina eksperata procijenila tu česticu, čimbenik ili kategoriju kao nepotrebnu.

5.3.2.2. Konstruktna valjanost

Konstruktna valjanost procjenjuje se statističkim i praktičnim postupcima [296], a odnosi se na pitanje mjeri li mjerni instrument različite konstrukte koje bi trebao mjeriti [310] odnosno obrazložiti na što se misli pojedinim konstruktom. Prema Straubu i suradnicima [306], konstruktna valjanost pokazuje postoji li međusobna povezanost mjera koje je odabrao istraživač, na način da obuhvaćaju suštinu konstrukta. U kontekstu ovog istraživanja, konstruktna valjanost mjernog instrumenta i predloženog radnog okvira mora pokazati da su kategorije i čimbenici kulture informacijske sigurnosti koje koristi autor ovog rada, relevantne i u praksi.

Kako bi se provjerila konstruktna valjanost, korištena je metoda **zatvorenog sortiranja karata** (koja se naziva još i Q-sortiranje) [311]. Temelj ove metode je uključivanje eksperata u procjeni čestica i čimbenika, gdje eksperti trebaju svrstati čestice i čimbenike u odvojene kategorije s obzirom na sličnosti i različitosti među česticama odnosno čimbenicima. Drugim riječima, eksperti svaku manifestnu varijablu trebaju pridružiti samo jednoj od unaprijed definiranih latentnih varijabli odnosno konstrukata.

Konstruktna valjanost mora ispunjavati uvjete konvergentne (engl. *Convergent Validity*) i diskriminantne valjanosti (engl. *Discriminant Validity*) [304]. Konvergentna valjanost je mjera koja objašnjava u kolikom opsegu varijable pozitivno koreliraju s drugim varijablama istog konstrukta [312], dok diskriminantna valjanost predstavlja mjeru koliko se neki konstrukt doista razlikuje od drugih konstrukata, odnosno odgovara na pitanje koliko neki konstrukt

korelira s drugim konstruktima i koliko se pojedina varijabla koja opisuje jedan konstrukt razlikuje od varijabli koje opisuju drugi konstrukt [313].

Straub i suradnici [306] te Petter i suradnici [312] smatraju kako su konvergentna i diskriminantna valjanost latentnog konstrukta osigurane primjenom metode sortiranja karata. Drugim riječima, ukoliko su eksperti konzistentno svrstali čestice u odgovarajuće konstrukte smatra se da se postigla konvergentna valjanost određenog konstrukta, te diskriminantna valjanost u odnosu na druge konstrukte [302], [306], [199], a one čestice kod kojih se eksperti ne slože isključuju se iz upotrebe u mjernom instrumentu.

Za procjenu pouzdanosti procedure sortiranja korištene su dvije mjerne metode*: Fleiss Kappa koeficijent* [314] i *omjer pogodaka* (engl. *Hit Ratio*) [302]. **Fleiss Kappa koeficijent** predstavlja koeficijent slaganja među ekspertima kada u procjeni sudjeluju više od dva eksperta gdje se jačina slaganja određuje prema vrijednostima iz Tablice 5.2.

Tablica 5.2. Referentne vrijednosti Kappa koeficijenta

Vrijednost Kappa koeficijenta	Jačina slaganja
< 0,20	Slaba
0,21 – 0,40	Prihvatljiva
0,41 – 0,60	Umjerena
0,61 – 0,80	Dobra
0,81 – 1,00	Vrlo dobra

Izvor: [315], [316]

Omjer pogodaka (engl. *Hit Ratio*) pokazuje koliko je manifestnih varijabli pridruženo ciljanom latentnom konstruktu od strane eksperata [302], odnosno u ovom konkretnom istraživanju, koliko je čestica pridruženo ciljanim čimbenicima odnosno koliko je čimbenika pridruženo ciljanim kategorijama. Omjer pogodaka, za koji u literaturi ne postoji eksplicitno definirana referentna vrijednost [311], računa se kao kvocijent broja manifestnih varijabli koje su svi eksperti pridružili ciljanim latentnim konstruktima i ukupnog broja mogućih pridruživanja manifestnih varijabli po svim uključenim ekspertima. Veći postotak manifestnih varijabli koje su smještene u ciljane konstrukte predstavlja veći stupanj postizanja međusobnog slaganja među ekspertima [302].

Za mjerne instrumente koji imaju veliki postotak „ispravnih" svrstavanja može se reći da imaju velik stupanj konstruktne valjanosti te visok potencijal za dobru pouzdanost. Čestice su kodirane na semantičkoj ordinalnoj skali od 5 stupnjeva. Oznake odgovora za čestice koje mjere

razinu percepcije sudionika istraživanja po pitanju čimbenika kulture informacijske sigurnosti kretale su se u rasponu od „*1 - u potpunosti se ne slažem*" do „*5 - u potpunosti se slažem*" te dodatnog odgovora „*n/p - nije primjenjivo u mojoj organizaciji*" u slučaju da neka od čestica nije bila primjenjiva za pojedinu organizaciju. Dodatno, oznake odgovora za čestice vezane uz različite oblike sigurnosnih praksi kretale su se, ovisno o vrsti čestice, od „*1 - u potpunosti se ne slažem*" do „*5 - u potpunosti se slažem*" ili od „*1 – uopće ne*" do „*5 – vrlo često*" ili pak od „*1 – 0 puta*" do „*5 – 4 i više puta*". Kako bi se izradio okvir kulture informacijske sigurnosti te provjerila povezanost kulture informacijske sigurnosti i primjene dobrih sigurnosnih praksi u organizaciji, mjerni instrument sadrži osim navedenog i nekoliko pitanja o objektivnim pokazateljima primjene implementiranih mjera informacijske sigurnosti u organizaciji (primjerice, pojavi incidentnih situacija ili kampanjama podizanja svijesti putem poruka elektroničke pošte u kojima se zaposlenici upozoravaju na različite oblike sigurnosnih prijetnji).

5.3.3. Testiranje mjernog instrumenta

Testiranje odnosno validacija mjernog instrumenta provedena je uz pomoć empirijskog istraživanja što obuhvaća provjeru sadržajne i konstruktne valjanosti te pouzdanosti [306]. Sadržajna i konstruktna valjanost utvrđena je u prethodnom koraku razvoja mjernog instrumenta, putem pregleda literature i procjenom eksperata, dok se u ovom koraku utvrdila pouzdanost mjernog instrumenta te konačna struktura čestica koje čine mjerni instrument putem faktorske analize.

5.3.3.1. Prikupljanje podataka

Za potrebu provedbe validacije mjernog instrumenta u smislu interne konzistentnosti, ali ujedno i validacije konceptualnog okvira i testiranja druge hipoteze u sljedećoj fazi istraživanja, formiran je uzorak na kojem će se provesti empirijsko istraživanje na način da se pokušalo identificirati sve organizacije koje čine operatore ključnih usluga u kontekstu kritične nacionalne infrastrukture Republike Hrvatske, sukladno Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i pružatelja digitalnih usluga [219] te se zatim formirao slučajni uzorak tih organizacija. Nakon formiranja uzorka organizacija, poveznica na online anketni upitnik se elektroničkim putem proslijedila na zaposlenike organizacija koji su korisnici informacijskog sustava. Istraživanje se provodilo na temelju dobrovoljnog i anonimnog sudjelovanja sudionika bez prikupljanja osobnih podataka, a dodatna prednost online anketnog upitnika u odnosu na ostale metode prikupljanja podataka su minimalni troškovi provođenja ovakvog istraživanja te smanjeno vrijeme potrebno za implementaciju [301]. U ovoj fazi

istraživanja djelomično je ostvaren drugi postavljeni cilj istraživanja, dok je njegovo ostvarenje u potpunosti postignuto u sljedećoj fazi, nakon procjene pouzdanosti mjernog instrumenta.

5.3.3.2. Pouzdanost

Podaci dobiveni empirijskim istraživanjem poslužili su za konačnu validacija mjernog instrumenta u smislu **pouzdanosti** (engl. *Reliability*), čime se utvrđuje opseg u kojem se rezultati istraživanja mogu ponoviti tijekom vremena ili kroz različite grupe sudionika [306].

Za procjenu pouzdanosti mjernog instrumenta koristio se Cronbachov α (alfa) koeficijent kao mjera koja određuje unutarnju konzistentnost ili prosječnu povezanost čestica mjernog instrumenta (manifestne varijable) koje mjere pojedini čimbenik (latentne varijable) [317]. Vrijednost Cronbachovog alfa koeficijenta može poprimiti vrijednosti od 0 do 1 gdje nizak Cronbachov alfa koeficijent upućuje na to da varijable mogu biti toliko heterogene da slabo predstavljaju konstrukt, a općenito prihvaćenom donjom razinom Cronbachovog alfa koeficijenta smatra se vrijednost 0,70 [306], [300], [318].

5.3.3.3. Faktorska analiza

Kako bi se dodatno ispitala valjanost i pouzdanost mjernog instrumenta, u sklopu testiranja mjernog instrumenta, a nakon provedenog prikupljanja podataka putem empirijskog istraživanja, provedena je i faktorska analiza za svaku pojedinu kategoriju kako bi se statistički utvrdio broj čimbenika (faktora) koji čine pojedinu kategoriju kako mjernog instrumenta tako i konceptualnog okvira koji dijeli njegovu strukturu, budući da se faktorska analiza može koristiti za procjenu robusnosti grupe pitanja u mjernom instrumentu, identificirajući na taj način klastere međusobno povezanih čestica [319]. Validacijom mjernog instrumenta potvrdom njegove valjanosti i pouzdanosti ostvario se drugi postavljeni cilj ovog istraživanja te jednim dijelom i treći postavljeni cilj istraživanja.

Cilj faktorske analize je utvrđivanje temeljnih dimenzija, čimbenika odnosno faktora kojima bi se mogla otkriti struktura nekog nepoznatog ili nedovoljno poznatog područja [300]. Faktorska analiza sastoji se od niza statističkih metoda, čiji je temeljni cilj pojednostaviti korelacijske odnose između brojnih varijabli kako bi se otkrilo postoji li kakva „struktura” u promatranim podacima. Dvije su osnovne vrste faktorske analize, konfirmatorna i eksploratorna. Tako se konfirmatorna faktorska analiza bavi potvrđivanjem ili opovrgavanjem postojećih hipoteza o odnosima između varijabli [319] dok, s druge strane, eksploratorna faktorska analiza služi za otkrivanje temeljnih faktora u nekom području kada broj i struktura faktora nisu unaprijed

poznati [300]. Drugim riječima, eksploratorna faktorska analiza ne pretpostavlja *a priori* postojanje modela, već istraživač istražuje moguće faktore, postoji li njihova međusobna povezanost te koje promatrane varijable najbolje mjere koji faktor. U konačnici je cilj identificirati najmanji broj faktora koji objašnjavaju većinu varijanci u promatranim varijablama [320]. Eksploratorna faktorska analiza posebno je korisna kada je teorijski temelj za konstrukciju modela slab odnosno u slučajevima nedostatka dovoljno detaljne teorije o odnosu varijabli prema temeljnim konstruktima [318].

Upravo je to jedan od glavnih razloga zašto je u ovom istraživanju korištena eksploratorna faktorska analiza, a ne konfirmatorna jer, iako su manifestne varijable (čestice mjernog instrumenta) koje su se koristile u ovom istraživanju bile identificirane na temelju pregleda relevantne literature i prethodnih istraživanja, te manifestne varijable dolaze iz više različitih izvora i mjere različite razine latentnih varijabli što može utjecati na valjanost i pouzdanost mjernog instrumenta budući da, kao što je navedeno u prethodnim poglavljima ove disertacije, ne postoji međusobni konsenzus istraživanja oko toga koji čimbenici čine kulturu informacijske sigurnosti.

Pregledom relevantne literature vezano uz formiranje uzorka u svrhu korištenja faktorske analize, utvrđeno je da nema konsenzusa oko toga koliki je dostatni broj opservacija potreban za provođenje faktorske analize već se mogu pronaći samo generalne smjernice [321] koje se baziraju ili na ukupnoj veličini seta podataka ili na omjeru opservacija (broja sudionika) i broja varijabli. Tako se za minimalnu veličinu seta podataka uzima 100 opservacija [322], [321] odnosno, prema Brewetonu i Millwardu [319] potrebno je minimalno tri puta više sudionika od broja varijabli, prema Hairu [322] pet puta više sudionika od broja varijabli dok Cattell [323] navodi kako se taj broj kreće između tri i šest puta više sudionika od broja varijabli, a za Fielda [307] čak 10 do 15 puta više.

Za prethodnu procjenu valjanosti i mogućnosti provođenja faktorske analize korišteni su *Kaiser-Meyer-Olkin (KMO) mjera adekvatnosti uzorka* i *Bartlettov test sfericiteta*. KMO poprima vrijednosti između 0 i 1, a vrijednosti KMO-a iznad 0,6 smatraju se prihvatljivima dok su vrijednosti iznad 0,9 izvrsne [307]. Bartlettov test sfericiteta mora biti značajan na razini $p < 0.001$ što znači da postoje adekvatne veze (korelacije) između varijabli uključenih u analizu koje su potrebne ako se očekuje da promatrane varijable opisuju istu latentnu varijablu [307]. Međutim, ta korelacija ne smije biti prevelika, inače može doći do multikolinearnosti koja može

uzrokovati probleme u faktorskoj analizi na način da postane nemoguće otkriti jedinstveni doprinos pojedinom faktoru od strane varijabli koje visoko koreliraju [307].

Iz tog razloga, u prvom koraku faktorske analize napravljena je korelacijska matrica manifestnih varijabli (čestica) te identificirani parovi varijabli koji visoko koreliraju. Kao granica uzeta je vrijednost 0.8 [307] te, sukladno tome uklonjena po jedna varijabla iz visokokorelirajućih parova, kako bi se smanjila multikolinearnost. Ne postoji statistički način za određivanje koju varijablu iz tog para treba ukloniti već je to stvar interpretacije istraživača [324].

Eksploratorna faktorska analiza mora slijediti dva bitna koraka za stvaranje odgovarajućeg rješenja koje objašnjava odgovarajući broj faktora koji predstavljaju konstrukt: (1) ekstrakciju faktora i (2) rotaciju i interpretaciju faktora [325]. Ekstrakcija faktora želi otkriti faktore na temelju određene metode i kriterija za utvrđivanje adekvatnosti broja faktora, dok rotacija i interpretacija faktora ima za cilj poboljšati interpretaciju određenog faktorskog rješenja [326].

Postoji više metoda ekstrakcije faktora od kojih se najčešće koriste analiza glavnih komponenti (engl. *Principal Component Analysis - PCA*) i analiza zajedničkih faktora (engl. *Common Factor Analysis - CFA*), koja se još naziva i analiza glavnih faktora (engl. *Principal Factor Analysis - PFA*) ili faktoriranje glavnih osi (engl. *Principal Axis Factoring - PAF*) [327]. Analiza glavnih komponenti traži linearnu kombinaciju varijabli tako da se iz varijabli izdvaja maksimalna varijanca nakon čega se uklanja ta varijanca i traži druga linearna kombinacija koja objašnjava većinu varijance. S druge strane, analiza zajedničkih faktora traži najmanji broj faktora koji mogu objasniti zajedničku varijancu skupa varijabli [327]. Drugim riječima, osnovna razlika između ove dvije metode leži u činjenici da se u analizi glavnih komponenti analiziraju sve varijance u manifestnim varijablama dok se u analizi zajedničkih faktora analizira samo zajednička varijanca, odnosno pokušavaju se procijeniti i ukloniti varijance nastale zbog pogreške i varijance koje su jedinstvene za svaku varijablu [326]. U konačnici, ne postoji jedinstveno pravilo oko toga koju metodu ekstrakcije koristiti, što potvrđuje analiza slučajeva korištenja eksploratorne faktorske analize koju su proveli Osborne i Costello [327] te zaključili da ne postoji optimalni postupak ekstrakcije već istraživač sam odabire najprikladniju metodu u pojedinačnom slučaju.

Za određivanje broja faktora koji najbolje opisuju odnos između varijabli postoji nekoliko kriterija od kojih su najpoznatiji sljedeći [322]:

- **A priori kriterij** kod kojeg istraživač prije same analize zna koliko faktora želi dobiti u analizi. Ovaj pristup ima smisla kod testiranja teorija ili hipoteza o broju faktora koje je potrebno dobiti analizom, kao i kod pokušaja ponavljanja nekog istraživanja kod kojeg je poznat rezultat po pitanju broja faktora.

- **Kriterij latentnog korijena** (engl. *Latent root criterion*) koji se naziva još i Kaiserovo pravilo [328], a temelji se na pretpostavci da se jedino one varijable koje imaju svojstvenu vrijednost (engl. *Eigenvalue*) većom od 1 mogu smatrati značajnima, a sve one manje od 1 se odbacuju. Ovo je ujedno i najčešće korištena tehnika.

- **Kriterij postotka varijance** koji se temelji na postizanju određenog kumulativnog postotka ukupne varijance koji čine uzastopne varijable. Svrha ovog pristupa je osigurati praktičnu značajnost dobivenih faktora osiguravajući da oni objašnjavaju barem određeni iznos varijance. Ne postoji generalno pravilo koliki bi postotak varijance trebao biti minimalno postignut, ali se za prirodne znanosti očekuje postizanje barem 95%-tnog iznosa, dok je za društvene znanosti postotak od 60% ukupne varijance, a ponekad i manje, prihvatljivo.

- **Scree test**, koji se još naziva i Catellov test [329], predstavlja grafički prikaz odnosa svojstvenih vrijednosti i broja faktora po redoslijedu izvlačenja varijabli. Na dijagramu se pronađe prijelomna točka gdje se svojstvene vrijednosti prestaju naglo smanjivati i počne se formirati ravna linija te se za broj faktora uzima broj iznad prijelomne točke.

- **Paralelna analiza** predstavlja metodu kojom se određuje broj faktora na način da se generira velik broj simuliranih setova podataka s nasumičnim vrijednostima za isti broj varijabli i veličinu uzorka kao i originalni podaci. Nakon toga se na simuliranim podacima napravi faktorska analiza te se svojstvene vrijednosti simuliranih podataka uprosječe i uspoređuju redom s dobivenim svojstvenim vrijednostima originalnih podataka. Svi faktori koji imaju svojstvenu vrijednost veću od prosječne simulirane svojstvene vrijednosti ostaju u daljnjoj analizi dok se drugi odbacuju.

Sljedeći koraci obuhvaćaju izradu tablice komunaliteta (engl. *Communalities*) odnosno proporcija zajedničke varijance koji neka varijabla dijeli s drugim varijablama i faktorske matrice (engl. *Factor Matrix*) koja prikazuje faktorska opterećenja [322]. Faktorska opterećenja (engl. *Factor Loading*) ukazuju na važnost pojedine varijable za pojedini faktor odnosno određuju stupanj u kojem se varijable vežu na te faktore [307]. U idealnom slučaju svaki faktor

bit će reprezentiran varijablama koje imaju visoko faktorsko opterećenje samo za jedan faktor. Međutim, to u praksi gotovo nikad nije tako te je češća situacija da jedna varijabla ima faktorsko opterećenje srednje razine za više faktora gdje se ta pojava naziva unakrsno opterećenje (engl. *Cross-Loading*) [322].

U većini slučajeva, početno faktorsko rješenje u vidu dobivene faktorske matrice ne pruža odgovarajuću interpretaciju što znači da je rezultate ekstrakcije faktora bez upotrebe rotacije faktora u pravilu teško protumačiti bez obzira na to koja se metoda ekstrakcije koristi [326]. Iz tog razloga, dobiveni faktori trebaju se transformirati odnosno rotirati kako bi se dobila jednostavna, a time i lako interpretabilna struktura faktora, u kojoj samo manji broj manifestnih varijabli ima visoke i srednje visoke korelacije s pojedinim faktorom dok sve ostale varijable imaju niske ili nulte korelacije s tim faktorom [300]. Rotacija faktora se koristi za poboljšanje interpretabilnosti i znanstvene korisnosti rješenja, a ne za poboljšanje kvalitete matematičkog temelja između promatrane i reproducirane korelacijske matrice [326] jer rotacija ne mijenja temeljno rješenje, već daje obrazac faktorskih opterećenja na način koji je lakše interpretirati [325].

Dvije osnovne skupine rotacija su ortogonalne (engl. *Orthogonal*) i kosokutne (engl. *Oblique*) [326] gdje su češće korištene ortogonalne metode rotacije koje su poželjna metoda kad je cilj istraživanja smanjenje podataka ili na manji broj varijabli ili na niz nekoreliranih mjera za naknadnu upotrebu u drugim multivarijantnim tehnikama [322]. Najčešće korištena metoda ortogonalne rotacije je Varimax rotacija čiji je cilj pojednostaviti faktore maksimizacijom varijance opterećenja unutar faktora gdje je onda tumačenje faktora lakše jer je očito koje se varijable s njim povezuju [326].

Ne postoje definirana pravila koja bi vodila istraživača pri odabiru određene ortogonalne ili kosokutne rotacijske tehnike [322] pa mnogi istraživači provode i ortogonalne i kosokutne rotacije, a zatim izvještavaju o najjasnijoj i najlakšoj za interpretaciju [325].

Za ekstrakciju faktora u ovom istraživanju primijenila se metoda analize zajedničkih faktora s ortogonalnom Varimax rotacijskom metodom gdje je ortogonalna Varimax rotacijska metoda odabrana iz razloga što ova metoda pokušava identificirati manji broj varijabli s visokim opterećenjem na svaki faktor, što rezultira pojednostavljenom interpretacijom rezultata [320] te je ujedno najčešći izbor istraživača [327].

Iz daljnje analize uklonjene su manifestne varijable koje imaju faktorsko opterećenje manje od 0,3 [330], [307], [322] te se izračunalo unakrsno opterećenje za sve varijable koje imaju opterećenje u više od jednog faktora. Unakrsno opterećenje računa se na način da se kvadriraju faktorska opterećenja varijabli koje reprezentiraju isti faktor te se izračuna omjer dvaju vrijednosti, odnosno podijeli se veća vrijednost s manjom [322]. Odluka o daljnjem postupanju s unakrsnim opterećenjem temelji se na dobivenoj vrijednosti omjera te sljedećeg pravila [322]:

- ako je omjer u rasponu od 1,0 do 1,5, radi se o problematičnom unakrsnom opterećenju te je varijabla s manjim faktorskim opterećenjem dobar kandidat za isključivanje iz daljnje analize kako bi se postigla jednostavna struktura,
- ako je omjer u rasponu od 1,5 do 2,0, radi se o potencijalnom unakrsnom opterećenju te se isključivanje varijable temelji na interpretaciji rezultirajućih faktora, te
- ako je omjer veći od 2.0, radi se o zanemarujućem unakrsnom opterećenju gdje se manje faktorsko opterećenje, iako značajno, može zanemariti u svrhu interpretacije.

Nakon određivanja faktora i broja manifestnih varijabli koje opisuju te faktore, za svaki faktor izračunata je i analizirana unutarnja konzistentnost putem Cronbachovog alfa koeficijenta, te su uklonjeni oni faktori čiji je iznos koeficijenta bio ispod predviđenog praga od 0,7 [306], [300]. Dobro definiran faktor trebao bi se sastojati od manifestnih varijabli koje imaju visoko faktorsko opterećenje za taj faktor, a što je veći broj manifestnih varijabli taj faktor će biti pouzdaniji za buduća istraživanja. Međutim, broj manifestnih varijabli po pojedinom faktoru ne bi trebao biti manji od tri [319], [321], [323], [331], [332].

U konačnici, dobivene faktore potrebno je imenovati radi lakšeg korištenja u budućim istraživanjima. Prilikom imenovanja faktora, autor ovog istraživanja vodio se razmišljanjem, koje je predložio Hair [322] da se faktorima dodijeli logično ime koje predstavlja temeljnu prirodu faktora, čime se obično olakšava prezentacija i razumijevanje faktorskog rješenja.

5.4. Validacija okvira i analiza prikupljenih podataka

Završna, **četvrta faza** obuhvaća analizu prikupljenih podataka nakon provedenog empirijskog istraživanja kao i analizu povezanosti kulture informacijske sigurnosti s primjenom implementiranih mjera informacijske sigurnosti u organizaciji. Na samom početku korištena je deskriptivna statistička analiza pomoću koje su ispitani sumarni opisi distribucija kvantitativnih varijabli nakon čega je slijedila validacija predloženog okvira.

Konačni cilj ovog istraživanja je dobiti validiranu strukturu okvira za procjenu i unapređenje kulture informacijske sigurnosti koji će omogućiti interpretaciju pojedinih čimbenika tog okvira. Ovdje je bitno naglasiti kako se sam radni okvir za procjenu i unapređenje kulture informacijske sigurnosti temelji na validiranom mjernom instrumentu i dijeli njegovu strukturu. To znači da mjerni instrument čine manifestne varijable (čestice) kojima se opisuju latentne varijable prve razine (čimbenici) te latentne varijable druge razine (kategorije) koje su opisane tim čimbenicima. Upravo spomenuti čimbenici i kategorije iz mjernog instrumenta sastavni su dijelovi okvira za procjenu i unapređenje kulture informacijske sigurnosti te se validacijom mjernog instrumenta formira konačna konstrukcija okvira sa svim pripadajućim kategorijama i čimbenicima, čime je djelomično validiran i sam okvir. Potpuna validacija predloženog okvira provedena je nakon testiranja hipoteze H2, gdje je, na temelju pitanja o objektivnim pokazateljima primjene implementiranih mjera informacijske sigurnosti u organizaciji u sklopu mjernog instrumenta, analizirana povezanost kulture informacijske sigurnosti s primjenom implementiranih mjera informacijske sigurnosti, čime se nastojala pokazati primjenjivost okvira u praksi. Hipoteza H2 testirala se korelacijskom analizom koristeći parametrijsku metodu izračuna Pearsonovog koeficijenta korelacije, kao i neparametrijsku metodu izračuna Spearmanovog rho koeficijenta. Konačnom validacijom okvira postignut je i treći postavljeni cilj istraživanja testiranje hipoteze H1.

6. REZULTATI ISTRAŽIVANJA

Ovo poglavlje predstavlja konačne rezultate istraživanja provedenog u sklopu izrade doktorske disertacije koje se sastojalo od teoretskog i empirijskog dijela čiji su rezultati prikazani putem četiri identificirana koraka metodologije istraživanja opisane u prethodnom poglavlju.

6.1. Identificirani čimbenici kulture informacijske sigurnosti

Tijekom prve faze istraživanja napravljen je upit u citatnu bazu *Web of Science (WoS)* koji je imao sljedeći format: *TITLE: ((secur* AND ("efficien*" OR "effectiv*" OR "success*" OR "culture")) OR (organi* AND ("secur*" OR "culture"))) AND TOPIC: ("information systems security" OR "information security" OR "organizational culture")*. Rezultat ovog upita bilo je preko dvije tisuće članaka gdje su po naslovu odabrani oni koji bi mogli biti relevantni za ovo istraživanje. Kako bi se nadopunila dobivena lista potencijalno relevantnih članaka pretraživanje po istim ključnim riječima uslijedilo je na dodatnim bazama podataka - *Science Direct, Emerald Insight, Springer Link, IEEE Xplore Digital Library* i *Google Scholar*. Nakon uklanjanja duplikata i radova koji nisu bili na engleskom jeziku, došlo se do konačne brojke od oko 250 jedinstvenih radova koji su bili potencijalno relevantni za ovo istraživanje. Nakon čitanja sažetka i brze provjere sadržaja članaka, došlo se do konačne brojke od oko stotinjak relevantnih radova koji su detaljno pročitani kako bi se definirali ključni čimbenici kulture informacijske sigurnosti koji bi činili temelj predložene teme istraživanja.

Tablica 6.1. u nastavku prikazuje sumarni pregled čimbenika kulture informacijske sigurnosti prepoznatih u identificiranoj literaturi, iz koje je vidljiv spomenuti nedostatak konsenzusa oko toga koji konkretni čimbenici čine kulturu informacijske sigurnosti. Ovime je postignut prvi cilj istraživanja.

Tablica 6.1. Identificirani čimbenici kulture informacijske sigurnosti na temelju pregleda literature

Rbr.	Čimbenik	Referenca
1.	Podrška rukovodstva	[74]; [162]; [79]; [88]; [289]; [333]; [198]; [293]; [68]; [253]; [6]; [138]; [258]; [140]; [160]; [290]; [291]; [254]; [15]; [264]; [250]; [192]; [257]; [7]; [288]; [127]; [266]; [334]; [151]; [184]; [288]; [270]; [197]; [252]; [197]; [335]; [336]; [5]; [246]; [261]; [248]; [75]; [256]; [141]; [24]
2.	Uspostavljene sigurnosne politike i procedure	[74]; [245]; [17]; [164]; [293]; [68]; [140]; [160]; [80]; [294]; [290]; [291]; [139]; [292]; [254]; [15]; [54]; [164]; [264]; [250]; [192]; [257]; [7]; [288]; [334]; [249]; [151]; [184]; [270]; [252]; [197]; [335]; [336]; [17]; [5]; [246]; [265]; [261]; [256]; [136]; [337]; [161]; [10]
3.	Svijest o informacijskoj sigurnosti	[17]; [164]; [333]; [140]; [160]; [290]; [291]; [139]; [292]; [254]; [15]; [59]; [250]; [192]; [257]; [188]; [7]; [266]; [334]; [249]; [151]; [184]; [270]; [197]; [252]; [336]; [17]; [5]; [246]; [265]; [261]; [266]; [256]; [136]; [337]; [338]
4.	Obuka	[74]; [245]; [164]; [289]; [293]; [68]; [253]; [6]; [138]; [258]; [17]; [290]; [291]; [139]; [292]; [254]; [15]; [264]; [257]; [188]; [288]; [334]; [249]; [184]; [288]; [252]; [336]; [254]; [5]; [261]; [136]; [337]
5.	Odgovornost	[74]; [293]; [68]; [8]; [253]; [6]; [138]; [258]; [290]; [291]; [139]; [292]; [266]; [249]; [252]; [261]; [136];
6.	Analiza i upravljanje rizicima	[245]; [140]; [160]; [290]; [291]; [139]; [292]; [254]; [15]; [264]; [257]; [334]; [249]; [184]; [252]; [246]; [337]
7.	Usklađenost	[245]; [8]; [254]; [15]; [54]; [250]; [192]; [257]; [334]; [249]; [184]; [270]; [197]; [252]; [336]; [136];
8.	Povjerenje	[245]; [140]; [160]; [17]; [80]; [294]; [290]; [291]; [139]; [292]; [257]; [334]; [249]; [252]; [335]; [256]
9.	Etika i etičko ponašanje	[74]; [245]; [140]; [160]; [290]; [291]; [139]; [292]; [254]; [15]; [264]; [334]; [249]; [184]; [252]; [246]
10.	Upravljanje promjenama	[245]; [253]; [6]; [138]; [258]; [17]; [80]; [294]; [290]; [291]; [59]; [257]; [249]; [252]; [335]
11.	Edukacija	[245]; [164]; [293]; [68]; [290]; [291]; [139]; [292]; [264]; [257]; [249]; [184]; [337]
12.	Budžet	[198]; [293]; [68]; [140]; [160]; [290]; [291]; [139]; [292]; [250]; [192]; [246]
13.	Sigurnosno ponašanje	[333]; [59]; [257]; [7]; [334]; [197]; [252]; [265]; [256]
14.	Znanje	[333]; [261]; [59]; [257]; [334]; [13]; [252]; [256]
15.	Resursi	[74]; [253]; [6]; [138]; [258]; [257]; [337]
16.	Uvjerenja	[334]; [252]; [5]; [256]; [136]

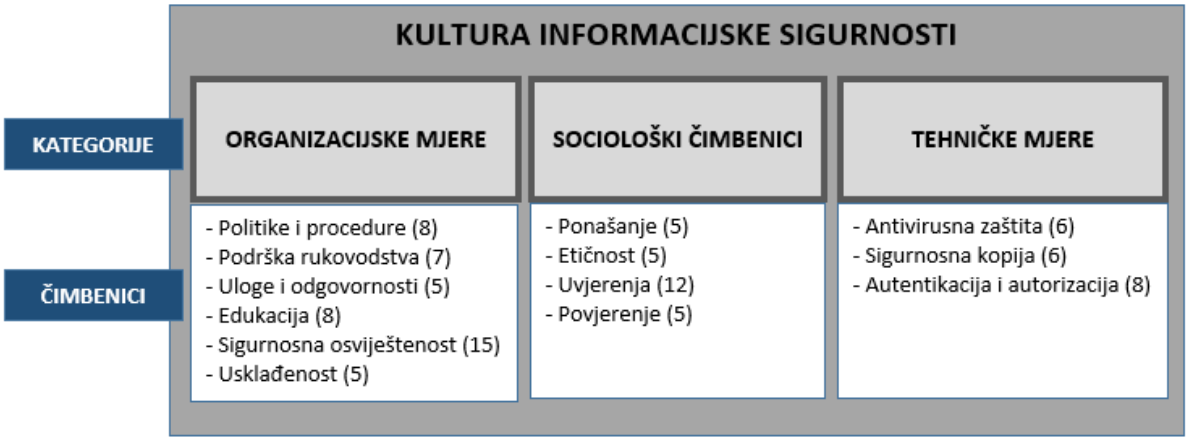
Tablica 6.1. Identificirani čimbenici kulture informacijske sigurnosti na temelju pregleda literature (nastavak)

Rbr.	Čimbenik	Referenca
17.	Upravljanje informacijskom sigurnošću	[17]; [80]; [294]; [151]; [254]
18.	Tehnologija	[250]; [192]; [257]; [252]
19.	Uključenost zaposlenika	[289]; [5]; [256]; [136]
20.	Sustav nagrađivanja	[289]; [5]; [261]; [136]
21.	Organizacijska struktura	[74]; [261]; [59]
22.	Nadzor i revizija	[74]; [245]; [249]
23.	Upravljanje incidentima	[245]; [54]; [249]
24.	Privatnost	[245]; [294]

Izvor: *vlastiti prikaz*

6.2. Konceptualni okvir

Kako je već navedeno u teoretskom dijelu ove disertacije, u potpoglavlju 3.3., relevantna istraživanja navode kako je za primjerenu razinu informacijske sigurnosti u organizacijama potreban holistički, višedimenzionalni pristup [9], [4] sastavljen od različitih glavnih komponenti. Tako Panguluri i suradnici [10] navode kako su te glavne komponente: tehničke mjere, ljudi i procesi. Yildrim [4] kao tri komponente takvog holističkog pristupa vidi tehnologiju, ljude i edukaciju, a AlHogail i Mirza [339] ljude, organizaciju i tehnologiju. Na temelju tih zaključaka te identificiranih čimbenika kulture informacijske sigurnosti u prethodnoj fazi, predloženi konceptualni okvir za evaluaciju i uspostavu kulture informacijske sigurnosti, sastavljen od tri latentne varijable druge razine odnosno kategorije te trinaest latentnih varijabli prve razine odnosno čimbenika koje su mjerene uz pomoć manifestnih varijabli (čestice mjernog instrumenta odnosno pitanja iz anketnog upitnika, čiji je broj po pojedinom konstruktu naveden u zagradi) prikazan je na Slici 6.1.



Slika 6.1. Konceptualni okvir kulture informacijske sigurnosti

Izvor: *vlastiti prikaz*

Prilikom odabira koje čimbenike iz Tablice 6.1. uključiti u predloženi konceptualni okvir kulture informacijske sigurnosti, autor ove disertacije vodio se primjenom nekoliko načela. Kao prvo, u principu su uzeti čimbenici koji su najčešće citirani u literaturi. Međutim, budući da su ciljani sudionici u ovom istraživanju svi zaposlenici odabranih organizacija koji su korisnici informacijskog sustava, čimbenici za koje je procijenjeno da prosječni zaposlenik nema dovoljno informacija kako bi mogao adekvatno odgovoriti (primjerice, čimbenici kao što su „analiza i upravljanje rizicima", „upravljanje promjenama" ili „budžet") nisu uzeti u obzir. Istraživanja u kojima su ti čimbenici bili uključeni za sudionike su uglavnom imali predstavnike rukovodstva ili zaposlenike IT odjela odnosno odjela za sigurnost koji su uključeni u ove aktivnosti te shodno tome mogu pružiti adekvatne informacije.

Zbog činjenice da su najčešće navođeni kao ključni čimbenici kulture informacijske sigurnosti, u konceptualni okvir uključeni su sljedeći čimbenici: „politike i procedure" [74], [245], [17], [164], [293], [68], [140], [160], [80], [294], [290], [291], [139], [292], [254], [15], [54], [164], [264], [250], [192], [257], [7], [288], [334], [249], [151], [184], [270], [252], [197], [335], [336], [17], [5], [246], [265], [261], [256], [136], [337], [161], [10], „podrška rukovodstva" [74], [162], [79], [88], [289], [333], [198], [293], [68], [253], [6], [138], [258], [140], [160], [290], [291], [254], [15], [264], [250], [192], [257], [7], [288], [127], [266], [334], [151], [184], [288], [270], [197], [252], [197], [335], [336], [5], [246], [261], [248], [75], [256], [141], [24], „sigurnosna osviještenost" [17], [164], [333], [140], [160], [290], [291], [139], [292], [254], [15], [59], [250], [192], [257], [188], [7], [266], [334], [249], [151], [184], [270], [197], [252], [336], [17], [5], [246], [265], [261], [266], [256], [136], [337], [338], „uloge i odgovornosti"

[74], [293], [68], [8], [253], [6], [138], [258], [290], [291], [139], [292], [266], [249], [252], [261], [136], „usklađenost“ [245], [8], [254], [15], [54], [250], [192], [257], [334], [249], [184], [270], [197], [252], [336], [136] i „povjerenje“ [245], [140], [160], [17], [80], [294], [290], [291], [139], [292], [257], [334], [249], [252], [335], [256]. Također su uzeti i čimbenici „obuka“ [74], [245], [164], [289], [293], [68], [253], [6], [138], [258], [17], [290], [291], [139], [292], [254], [15], [264], [257], [188], [288], [334], [249], [184], [288], [252], [336], [254], [5], [261], [136], [337] i „edukacija“ [245], [164], [293], [68], [290], [291], [139], [292], [264], [257], [249], [184], [337], ali spojeni u jedan, zajednički čimbenik pod nazivom „edukacija“ iz razloga što je često teško napraviti jasnu razliku gdje prestaje edukacija, a počinje obuka te se iz tog razloga ta dva pojma često i zajedno spominju u literaturi, kako je objašnjeno u potpoglavlju 3.5.4. Dodatno, uzeti su i čimbenici „etika“ [74], [245], [140], [160], [290], [291], [139], [292], [254], [15], [264], [334], [249], [184], [252], [246], koja predstavlja etičke aspekte ponašanja zaposlenika unutar organizacije te „ponašanje“, koje predstavlja cjelokupno sigurnosno ponašanje zaposlenika unutar organizacije budući da ponašanje zaposlenika u praksi pokazuje pridržavaju li se zaposlenici onog što znaju odnosno onog na što su upozoreni u organizaciji po pitanju informacijske sigurnosti. U konačnici, čimbenikom „uvjerenja“ [334], [252], [5], [256], [136] obuhvaćeni su osobni stavovi zaposlenika po pitanju informacijske sigurnosti i pripadajuće prakse u postupanju s takvim pitanjima.

Nadalje, iz Tablice 6.1. vidljivo je kako svi čimbenici nisu jednake razine detalja pa tako neki čimbenici predstavljaju jednoznačno određeni koncept (primjerice „politike i procedure”) dok drugi predstavljaju složeni višeslojni koncept (primjerice „upravljanje informacijskom sigurnošću”) koji sam može predstavljati jednu kategoriju. Tako je čimbenik „tehničke mjere” [250], [192], [257], [252] autor ove disertacije prilikom izrade konceptualnog okvira preuzeo kao kategoriju umjesto kao čimbenik, a kao čimbenike uzeo antivirusnu zaštitu, sigurnosnu kopiju te autentikaciju i autorizaciju. Ti čimbenici su uzeti u obzir iz razloga što predstavljaju neke od osnovnih tehničkih kontrola koje današnje organizacije imaju implementirane, a koje pokrivaju tri osnovna svojstva sigurnosti informacija, odnosno očuvanje njihove povjerljivosti, integriteta i dostupnosti. U potpoglavlju 3.5.7. opisano je više od ove odabrane tri tehničke mjere odnosno čimbenika, međutim, mjere kao što su sustavi za otkrivanje/sprečavanje upada (IDS/IPS sustav) ili sustav za upravljanje sigurnosnim informacijama i događajima (SIEM sustav) predstavljaju napredne tehničke sigurnosne mjere koje ne moraju nužno biti implementirane u promatranim organizacijama, a ako i jesu, vjerojatno prosječni zaposlenik nema dovoljno informacija kako bi mogao adekvatno odgovoriti na pitanja povezana s tim

mjerama. S druge strane, antivirusni sustav, sigurnosna kopija te neki oblik autentikacije i autorizacije trebali bi, u pravilu, biti prisutni u svim današnjim organizacijama, a napose u organizacijama koje predstavljaju nacionalnu kritičnu infrastrukturu odnosno operatore ključnih usluga te zaposlenici tih organizacija upoznati s tim mjerama jer se redovno susreću s istima. U konačnici, oni prepoznati čimbenici koji su identificirani od svega nekoliko autora također nisu uzeti u obzir kako bi se očekivani okvir za procjenu i unapređenje kulture informacijske sigurnosti mogao fokusirati na ključne čimbenike kulture informacijske sigurnosti te kako bi mjerni instrument koji čini temelj tog okvira bio što primjereniji za praktičnu upotrebu.

6.3. Mjerni instrument za procjenu i unapređenje kulture informacijske sigurnosti

Za potrebe validacije definiranog konceptualnog okvira kulture informacijske sigurnosti, u sklopu ovog istraživanja, razvijen je novi mjerni instrument. U svrhu validacije mjernog instrumenta korišten je online upitnik, koji predstavlja brz, učinkovit i povoljan način prikupljanja potrebnih informacija od ciljane populacije. Kako bi se razvio mjerni instrument s dobrim psihometrijskim karakteristikama, slijeđen je pristup koji su predložili Moore i Benbasat [302], kako je opisano u potpoglavlju 5.3.

Prvo je, na temelju pregleda dosadašnjih istraživanja, kreiran skup čestica mjernog instrumenta koje predstavljaju manifestne varijable samog okvira. U početnoj fazi izdvojeno je ukupno 105 čestica od čega 95 čestica opisuje predloženih 13 čimbenika, a 10 čestica odnosilo se na mjerenje stvarnog stanja implementiranih kontrola dobre prakse informacijske sigurnosti u organizacijama koje će poslužiti za potvrđivanje ili odbacivanje hipoteze H2. Popis svih čestica mjernog instrumenta nalazi se u Prilogu 1., čime je djelomično ostvaren drugi cilj istraživanja. Da bi se drugi cilj istraživanja ostvario u potpunosti, potrebno je provjeriti valjanost i pouzdanost izrađenog mjernog instrumenta.

Nakon što je izrađen inicijalni popis čestica mjernog instrumenta sljedeći korak bila je validacija predloženog mjernog instrumenta koja je uključivala provjeru valjanosti i pouzdanosti mjernog instrumenta, prvo pomoću ekspertnog mišljenja te potom, nakon provođenja empirijskog istraživanja, putem faktorske analize. Provjera valjanosti uključivala je procjenu sadržajne i konstruktne valjanosti i to, ne samo manifestnih varijabli (čestica mjernog instrumenta) već i latentnih varijabli prve i druge razine (čimbenika i kategorija). U tu svrhu,

putem poslovne društvene mreže LinkedIn kontaktirano je 15 eksperata s ciljem njihovog uključivanja u validaciju mjernog instrumenta. U kontekstu ovog istraživanja pod pojmom „eksperti" podrazumijevaju se certificirani profesionalci iz područja informacijske sigurnosti ili revizije informacijskih sustava, odnosno osobe koje posjeduju stručne certifikate CISM (engl. *Certified Information Security Manager*), CISA (engl. *Certified Information Systems Auditor*) ili CISSP (engl. *Certified Information Systems Security Professional*). Ti certifikati odabrani su iz razloga što su neovisni o dobavljaču (engl. *Vendor-neutral*) te zahtijevaju, uz polaganje stručnog ispita kojim se dokazuje znanje iz predmetnog područja, i određeni broj godina radnog iskustva u predmetnoj domeni, a standardizacija obaveznog ispita jamči da svi eksperti imaju isto tumačenje određenih pojmova.

Nakon inicijalnog kontakta putem poslovne društvene mreže LinkedIn, autor ovog istraživanja je poslao ekspertima elektroničku poruku s opisom istraživanja i uputama za evaluaciju (Prilog 2.) u čijem je privitku bila tablica u Microsoft Excel datoteci s nekoliko listova putem koje su eksperti trebali napraviti procjenu sadržajne i konstruktne valjanosti. Eksperti su trebali pažljivo pročitati svaku česticu te ju prema potrebi preformulirati, te nakon toga svakoj od navedenih čestica procijeniti važnost pojedine čestice na način da joj dodijele jednu od ponuđenih vrijednosti (0 – ne mogu odrediti, 1 – obavezna, 2 – poželjna, 3 – nepotrebna). Eksperti su bili u mogućnosti, osim drugačijeg formuliranja postojećih čestica, formirati dodatne čestice. U sklopu ovog dijela eksperti su predložili bolju formulaciju za ukupno 9 čestica od kojih se 4 odnosilo na čestice kojima se mjeri kultura informacijske sigurnosti, a 5 na čestice kojima se mjeri stvarno stanje u organizaciji po pitanju implementiranih mjera dobre prakse. Ujedno, eksperti su predložili dvije dodatne čestice kojima se mjeri stvarno stanje u organizaciji („*U mojoj organizaciji postoji interna funkcija (jedna ili više osoba ili odjel) zadužena za informacijsku sigurnost*" i „*U zadnjih 12 mjeseci prijavio/la sam incident informacijske sigurnosti ili sumnju na isti*") čime ukupni broj čestica koje mjere stvarno stanje u organizaciji po pitanju implementacije mjera dobre prakse iznosi 12.

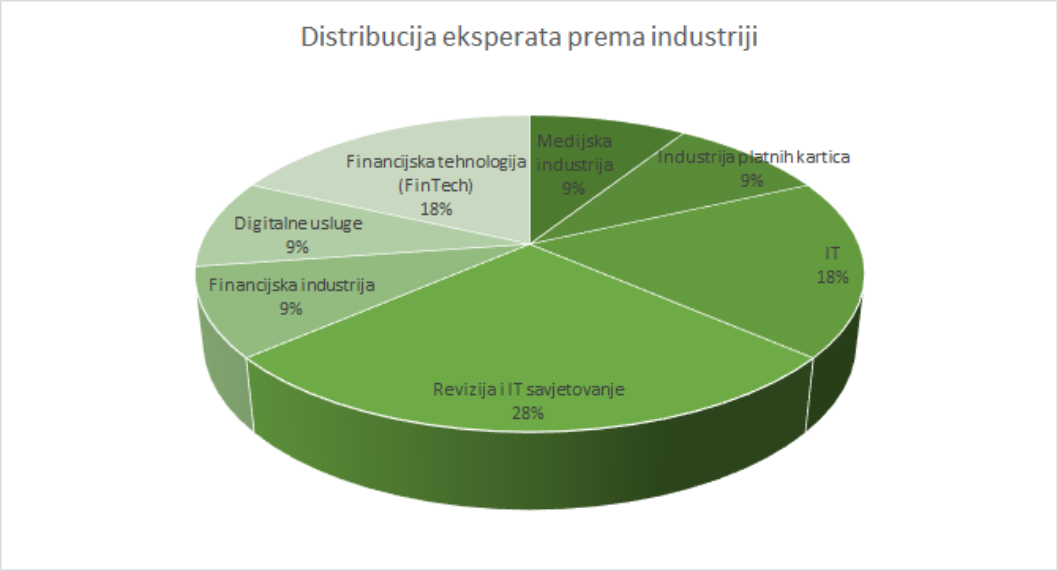
Nakon provjere i formulacije čestica te određivanja njihove važnosti, svaku od čestica bilo je potrebno smjestiti u jedan od ponuđenih 13 čimbenika (metoda zatvorenog sortiranja karata) [302]. Kako se ne bi utjecalo na mišljenje eksperata u pogledu razvrstavanja po čimbenicima, sve čestice bile su sortirane abecednim redom. Nakon što se izradila procjena za čestice (manifestne varijeble), istu proceduru bilo je potrebno primijeniti i na latentne varijable, odnosno odrediti važnost pojedinog čimbenika i kategorije te smjestiti svaki čimbenik u jednu od ponuđene tri kategorije.

Od kontaktiranih 15 eksperata ukupno je njih 11 vratilo ispunjenu tablicu, od čega je ženskog spola bilo njih 5 (45%), a muškog 6 (55%). Što se tiče radnog iskustva, najviše eksperata (njih 7 odnosno 64%) ima od 5 do 9 godina radnog iskustva, dok su 2 eksperta bila sa više od 20 godina radnog iskustva, a sveukupno 7 eksperata ima radno iskustvo u informacijskoj sigurnosti od 5 do 14 godina. Kao što je vidljivo iz Tablice 6.2., svi eksperti posjeduju barem jedan profesionalni certifikat iz područja upravljanja informacijskom sigurnošću (CISM, CISSP) ili revizije informacijskih sustava (CISA) dok dvoje eksperata, uz CISM certifikat, posjeduju i CISSP odnosno CISA certifikat. Eksperti su ravnomjerno raspoređeni po različitim industrijama iz kojih dolaze gdje najviše eksperata (3) dolazi iz industrije revizije i IT savjetovanja (Grafikon 6.1.).

Tablica 6.2. Odabrani demografski podaci o ekspertima koji su sudjelovali u istraživanju

Spol	**Certifikat iz područja informacijske sigurnosti ili revizije informacijskih sustava**	**Ukupno radno iskustvo (ukupno godina radnog staža)**	**Radno iskustvo u području informacijske sigurnosti**	**Radno iskustvo u području revizije informacijskih sustava**
M	CISM, CISSP	25	10	0
M	CISA	5	4	4
Ž	CISA	7	< 1	6
Ž	CISA	9	9	9
M	CISA	8	3	4
M	CISA	20	12	12
Ž	CISA	5	5	5
M	CISA	12	11	11
M	CISA	6	6	6
Ž	CISM	12	12	6
Ž	CISA, CISM	9	4	3

Izvor: *vlastiti prikaz*



Grafikon 6.1. Distribucija eksperata prema industriji u kojoj su zaposleni

Izvor: *vlastiti prikaz*

Za procjenu sadržajne valjanosti izračunati su omjer sadržajne valjanosti (engl. *Content Validity Ratio - CVR*) i prosječna vrijednosti relativne važnosti (engl. *Averaged value of relative importance - AVRI*) kako je opisano u potpoglavlju 5.3. Na temelju dobivenih rezultata iz mjernog instrumenta isključene su čestice koje su imale vrijednost CVR < 0,59 kolika je minimalna vrijednost potrebna za 11 eksperata prema Lawsheovom kriteriju [308] kao i one čestice koje su imale AVRI > 2. Isti princip primijenjen je i na čimbenike i kategorije. Ukupno 56 od 95 čestica imalo je CVR = 1 što, prema mišljenju eksperta, znači da su obavezne u predloženom mjernom instrumentu. S druge strane, 9 čestica je imalo CVR < 0,59 i/ili AVRI > 2 zbog čega su isključene iz mjernog instrumenta. Detaljni prikaz isključenih čestica prikazan je u Prilogu 1. Što se tiče čimbenika, ukupno 8 od 13 čimbenika imalo je CVR = 1 što, prema mišljenju eksperata, znači da su obavezni u predloženom mjernom instrumentu dok je, s druge strane, jedan čimbenik (etika) imao CVR < 0,59 zbog čega je taj čimbenik isključen iz mjernog instrumenta. Što se tiče kategorija, sve tri su jednoglasno proglašene obaveznima od strane eksperata, čime je djelomično potvrđena hipoteza H1 gdje će se hipoteza dodatno testirati formiranjem konačne strukture predloženog okvira temeljem provedbe faktorske analize. Tablica 6.3. prikazuje broj manifestnih i latentnih varijabli prije i nakon provjere sadržajne valjanosti.

Tablica 6.3. Broj manifestnih i latentnih varijabli prije i nakon izračuna CVR i AVRI

	Manifestne varijable (čestice)	Latentne varijable prve razine (čimbenici)	Latentne varijable druge razine (kategorije)
Početni broj	95	13	3
CVR < 0,59	8	1	-
AVRI	1 (4*)	-	-
Ostalo	4	-	-
Ukupan broj	**82**	**12**	**3**

CVR - omjer sadržajne valjanosti; AVRI – prosječna vrijednost relativne valjanosti; Ostalo – čestice koje zadovoljavaju CVR i AVRI kriterije, ali su isključene zbog isključivanja pripadajućeg čimbenika

**ukupno 4 čestice nemaju zadovoljavajući AVRI od čega 3 nemaju niti CVR te su već ubrojane*

Izvor: *vlastiti prikaz*

U sljedećem koraku, na temelju podataka dobivenih od eksperata metodom zatvorenog sortiranja karata, napravio se izračun **omjera pogodaka** (engl. *Hit Ratio*) kao indikatora koliko je varijabli smješteno u ciljanu grupu od strane eksperata [311] i **Fleiss Kappa koeficijenta,** kao mjere slaganja između više od dva eksperta [314], kako je opisano u potpoglavlju 5.3.2. Potrebno je napomenuti da, budući da su eksperti sadržajnu i konstruktnu valjanost radili u jednom potezu, sortirali su i čestice i čimbenike kojima je naknadno utvrđen nezadovoljavajući CVR ili AVRI. Međutim, te čestice i čimbenici nisu uzete u obzir prilikom analize konstruktne valjanosti. Također, potrebno je napomenuti kako su, kao posljedica analize podataka prikupljenih metodom zatvorenog sortiranja karata, pojedine srodne latentne varijable prve razine (čimbenici) spojene dok je čimbenik „povjerenje", iako je i u literaturi i od strane eksperata prepoznat kao važan, isključen iz daljnje analize zbog toga što nije postignut konsenzus eksperata odnosno nijedna čestica nije većinski svrstana u ovaj čimbenik.

Čimbenici „politike i procedure" i „uloge i odgovornosti" spojeni su u novi čimbenik „politike i uloge" budući da se politika informacijske sigurnosti može definirati i kao „*izjava o ulogama i odgovornostima zaposlenika da čuvaju informacijske i tehnološke resurse svojih organizacija*" [77]. Isto tako čimbenici „edukacija" i „sigurnosna osviještenost" spojeni su u novi čimbenik „edukacija i osviještenost" budući da se često sigurnosna edukacija, obuka i osviještenost navode zajedno te ih je teško poimence razlikovati, kao što je istaknuto u potpoglavlju 3.5.4. U prilog tome govore dva primjera čestica koje su eksperti ravnomjerno rasporedili između postojećih kategorija „edukacija" i „sigurnosna osviještenost". Tako je

česticu „*Svi zaposlenici su educirani o potrebi zaključavanja svojih računala kad napuštaju svoje radno mjesto*” 4 eksperta smjestilo u čimbenik „edukacija”, 4 u čimbenik „sigurnosna osviještenost”, 2 u „ponašanje” te 1 u „uloge i odgovornosti”, a česticu „*Svi zaposlenici u mojoj organizaciji pravovremeno su obaviješteni o prijetnjama informacijske sigurnosti putem elektroničke pošte ili na neki drugi način*” 5 eksperata je smjestilo u čimbenik „edukacija”, 5 u „sigurnosnu osviještenost” te 1 ekspert u čimbenik “usklađenost”. Spajanjem čimbenika „edukacija” i „sigurnosna osviještenost” dobiva se rezultat da je 8 od 11 eksperata u prvom slučaju i 10 od 11 eksperata u drugom slučaju, smjestio česticu u ciljani čimbenik.

Manifestne varijable koje su bile smještene u pripadajuću latentnu varijablu prve razine dobile su oznake prema toj varijabli. Tako su manifestne varijable koje opisuju latentnu varijablu „Politike i uloge“ nosile oznake POL1 do POL12, manifestne varijable koje opisuju latentnu varijablu „Podrška rukovodstva“ oznake MNG1 do MNG7, manifestne varijable koje opisuju latentnu varijablu „Edukacija i osviještenost“ oznake EDU1 do EDU19, manifestne varijable koje opisuju latentnu varijablu „Usklađenost“ oznake CMP1 do CMP4, manifestne varijable koje opisuju latentnu varijablu „Ponašanje“ oznake BHV1 do BHV4, manifestne varijable koje opisuju latentnu varijablu „Uvjerenja“ oznake BLF1 do BLF6, manifestne varijable koje opisuju latentnu varijablu „Antivirusna zaštita“ oznake AV1 do AV5, manifestne varijable koje opisuju latentnu varijablu „Sigurnosna kopija“ oznake BCK1 do BCK4, a manifestne varijable koje opisuju latentnu varijablu „Autentikacija i autorizacija“ nosile su oznake AA1 do AA6. Popis svih manifestnih varijabli prije i nakon validacije od strane eksperata prikazani su u Tablici 9.1. u Prilogu 1.

One manifestne varijable kod kojih nije postignut konsenzus kod eksperata u smislu većinskog svrstavanja u određenu latentnu varijablu, isključene su iz daljnje analize, čime je broj manifestnih varijabli nakon računanja Fleiss Kappa koeficijenta i omjera pogodaka smanjen sa 82 na 67, dok je broj latentnih varijabli prve razine smanjen za 1, a broj latentnih varijabli druge razine ostao isti, kao što je vidljivo u Tablici 6.4.

Tablica 6.4. Broj manifestnih i latentnih varijabli prije i nakon izračuna Fleiss Kappa koeficijenta i omjera pogodaka

	Početni broj	Nakon izračuna CVR i AVRI	Nakon izračuna FK i HR
Manifestne varijable (čestice)	95	82	67
Latentne varijable prve razine (čimbenici)	13	12	11
Latentne varijable druge razine (kategorije)	3	3	3
CVR - omjer sadržajne valjanosti; AVRI – prosječna vrijednost relativne valjanosti; FK – Fleiss Kappa koeficijent; HR – omjer pogodaka			

Izvor: *vlastiti prikaz*

Prilikom izračuna Fleiss Kappa[8] koeficijenta i omjera pogodaka, sva svrstavanja manifestnih varijabli u neku od latentnih varijabli prvog reda koje su isključene iz daljnje analize u prethodnim koracima, stavljena su u kategoriju „Ostalo". Kao što je vidljivo iz Tablice 6.5. vrijednost Fleiss Kappa koeficijenta iznosi 0,51 što se smatra umjerenom jačinom slaganja između eksperata [315], [316]. To je ujedno potvrđeno i izračunom omjera pogodaka gdje je najmanji omjer pogodaka za čimbenik „ponašanje" u iznosu od 45%, a najveći za čimbenik „sigurnosna kopija" u iznosu od 89%. Budući da u literaturi ne postoji striktni dogovor oko razina kvalitete omjera pogodaka, ukupni omjer pogodaka od 73% može se smatrati prihvatljivim.

Isti izračun ponovljen je i za latentne varijable (čimbenike) gdje, kao što je vidljivo iz Tablice 6.6., vrijednost Fleiss Kappa koeficijenta iznosi 0,78 što se smatra dobrom jačinom slaganja između eksperata [315], [316]. To je ujedno potvrđeno i izračunom omjera pogodaka gdje omjer pogodaka za kategoriju „organizacijske mjere" iznosi 85%, za preostale dvije kategorije 100%. Ukupni omjer pogodaka od 95% može se smatrati prihvatljivim.

[8] Vrijednost Fleiss' Kappa koeficijenta izračunata je pomoću formula Dr. Charlesa Zaiontza, autora web stranice *Real Statistics Using Excel* (http://www.real-statistics.com/reliability/fleiss-kappa/)

Tablica 6.5. Izračun omjera pogodaka i Fleiss Kappa koeficijenta za manifestne varijable

		STVARNI ČIMBENICI											
		POLITIKE I ULOGE	PODRŠKA RUKOVODSTVA	EDUKACIJA I OSVIJEŠTENOST	USKLAĐENOST	PONAŠANJE	UVJERENJA	ANTIVIRUSNA ZAŠTITA	SIGURNOSNA KOPIJA	AUTENTIKACIJA I AUTORIZACIJA	Ostalo	Broj svrstavanja	Omjer pogodaka
CILJANI ČIMBENICI	POLITIKE I ULOGE	101	4	13	3	3	5	0	0	0	3	**132**	*0,77*
	PODRŠKA RUKOVODSTVA	6	65	2	0	3	0	0	0	0	1	**77**	*0,84*
	EDUKACIJA I OSVIJEŠTENOST	12	1	156	2	12	12	2	0	1	11	**209**	*0,75*
	USKLAĐENOST	6	1	2	31	1	3	0	0	0	0	**44**	*0,70*
	PONAŠANJE	5	0	12	0	20	4	0	0	0	3	**44**	*0,45*
	UVJERENJA	5	3	10	1	7	33	0	0	0	7	**66**	*0,50*
	ANTIVIRUSNA ZAŠTITA	0	0	1	1	0	6	46	0	0	1	**55**	*0,84*
	SIGURNOSNA KOPIJA	2	0	3	0	0	0	0	39	0	0	**44**	*0,89*
	AUTENTIKACIJA I AUTORIZACIJA	10	0	4	3	1	0	0	0	46	2	**66**	*0,70*
Fleiss Kappa = 0,51		Ukupan broj svrstavanja: 737				Ukupan broj pogodaka: 537				**Ukupan omjer pogodaka: 0,73**			

Izvor: *vlastiti prikaz*

Tablica 6.6. Izračun omjera pogodaka i Fleiss Kappa koeficijenta za latentne varijable

		STVARNE KATEGORIJE					
		ORGANIZACIJSKE MJERE	SOCIOLOŠKI ČIMBENICI	TEHNIČKE MJERE	Ostalo	Broj svrstavanja	Omjer pogodaka
CILJANE KATEGORIJE	ORGANIZACIJSKE MJERE	56	8	2	0	**66**	*0,85*
	SOCIOLOŠKI ČIMBENICI	0	22	0	0	**22**	*1,00*
	TEHNIČKE MJERE	0	0	33	0	**33**	*1,00*
Fleiss Kappa = 0,78		**Ukupan broj svrstavanja: 121**		**Ukupan broj pogodaka: 111**	**Ukupan omjer pogodaka: 0,95**		

Izvor: *vlastiti prikaz*

Ovime je, uz prethodno ispitanu sadržajnu valjanost, ispitana i konstruktna valjanost mjernog instrumenta gdje je također, za varijable koje su konzistentno svrstavane u određene čimbenike odnosno kategorije postignuta i konvergentna valjanost varijable s određenim konstruktom, te diskriminantna valjanost prema drugima konstruktima [306].

Pouzdanost mjernog instrumenta u vidu izračuna Cronbachovog alfa koeficijenta unutarnje konzistentnosti, izračunat će se nakon provedbe eksploratorne faktorske analize u sklopu empirijskog istraživanja kojom će se utvrditi točan broj konstrukata unutar svake od tri kategorije.

6.3.1. Prikupljanje podataka

Od konačnog skupa sadržajno i konstruktno valjanih manifestnih varijabli, njih 67 je oblikovano u čestice mjernog instrumenta namijenjenog procjeni percepcije aspekata kulture informacijske sigurnosti dok je preostalih 12 manifestnih varijabli oblikovano u objektivne metrike namijenjene mjerenju stvarnog stanja u organizaciji po pitanju implementacije mjera dobre prakse informacijske sigurnosti.

Za potrebe ovog istraživanja mjerni instrument je izrađen pomoću alata LimeSurvey za izradu online upitnika čija je prilagođena verzija dostupna na web stranicama Sveučilišnog računalnog centra[9]. Slike ekrana izrađenog mjernog instrumenta u alatu LimeSurvey prikazani su u Prilogu 4. Pitanja u anketnom upitniku koja predstavljaju čestice mjernog instrumenta bila su formulirana kao izjavne rečenice s ponuđenim odgovorima gdje su se sudionici, u 67 pitanja koja su mjerila njihovu percepciju, mogli pozicionirati na ordinalnoj semantičkoj skali od „*1 - u potpunosti se ne slažem*" do „*5 - u potpunosti se slažem*" te dodatnog odgovora „*n/p - nije primjenjivo u mojoj organizaciji*" u slučaju da neko od pitanja nije bilo primjenjivo za pojedinu organizaciju. Ljestvica od pet stupnjeva koja se najčešće koristi, smatra se najprimjerenijom što se tiče osjetljivosti odnosno sposobnosti diferenciranja čovjeka kao procjenjivača [300]. Iako je ta ljestvica ordinalna, ona se može smatrati i intervalnom ako se polazi od pretpostavke da su intervali na skali jednaki [340]. Za preostalih 12 pitanja vezanih uz različite oblike sigurnosnih praksi, ponuđeni odgovori bili su od „*1 – uopće ne*" do „*5 – vrlo često*" za 6 pitanja odnosno od „*1 – 0 puta*" do „*5 – 4 i više puta*" za 2 pitanja, dok su 4 pitanja dijelila strukturu prvih 67 pitanja, od „*1 - u potpunosti se ne slažem*" do „*5 - u potpunosti se slažem*". Popis svih čestica nalazi se u Prilogu 1. Mjerni instrument je dodatno sadržavao 7 demografskih pitanja

[9] https://limesurvey.srce.hr/

koja su uključivala podatke o spolu, dobi, stupnju obrazovanja, radnom iskustvu u trenutnoj organizaciji, ukupnom radnom iskustvu te veličini organizacije i sektoru u kojem je sudionik zaposlen. Ljestvice za odgovore na demografska pitanja napravljene su po uzoru na statističke ljetopise Državnog zavoda za statistiku Republike Hrvatske[10]. Nakon formiranja strukture mjernog instrumenta u online formi probna verzija upitnika poslana je na pet osoba iz različitih struka kako bi se provjerila razumljivost pitanja, snalaženje u online okruženju i, ono najvažnije, trajanje same ankete, kako bi se moglo navesti okvirno trajanje u sam opis istraživanja.

Mjerni instrument izrađen je na način da nije prikupljao nikakve osobne informacije (uključujući ni IP adresu s koje se pristupalo online upitniku) te se mogla jamčiti anonimnost i povjerljivost odgovora sudionika budući da odgovore nije bilo moguće povezati s pojedinim sudionikom. Sudjelovanje u ovom istraživanju bilo je na dobrovoljnoj bazi te je u bilo kojem trenutku bilo moguće odustati od ispunjavanja upitnika, što je i navedeno sudionicima u samom opisu istraživanja. Sudionici ovog istraživanja bili su definirani kao zaposlenici organizacija koje su prepoznate kao operatori ključnih usluga, sukladno Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/2018) [219], koji koriste informacijski sustav organizacije.

Veliki problem s kojim se autor ovog istraživanja susreo prilikom provedbe empirijskog istraživanja ležao je u činjenici da je, kako bi se odredio statistički značajan uzorak sudionika, bilo potrebno imati informaciju o veličini i karakteristikama cijele populacije. Budući da spomenuti Zakon ne navodi eksplicitno o kojim se točno organizacijama radi, već samo u svom Prilogu I. navodi sektore koji predstavljaju ključne usluge te kriterije za određivanje operatora tih ključnih usluga, autor ovog istraživanja poslao je svim nadležnim sektorskim tijelima definiranim tim Zakonom, Zahtjev za pristup informacijama, sukladno Zakonu o pravu na pristup informacijama (NN 25/13, 85/15) [341], u kojem se tražio popis operatora ključnih usluga za pojedini sektor. Tako je 18. siječnja 2019. godine poslano ukupno 8 Zahtjeva za pristup informacijama na ukupno 6 nadležnih sektorskih tijela[11]. Kao što je vidljivo u Prilogu 3., odgovori na poslane Zahtjeve za pristup informacijama zaprimljeni su u periodu od 22. siječnja do 19. lipnja 2019., gdje su svi zahtjevi, osim zahtjeva upućenog nadležnom tijelu za

[10] https://www.dzs.hr/Hrv/Publication/stat_year.htm

[11] Dva sektorska tijela nadležna su za po dva sektora: Ministarstvo zaštite okoliša i energetiku za energetski sektor i sektor opskrbe vodom za piće i njezinu distribuciju, a Središnji državni ured za razvoj digitalnog društva za sektor digitalne infrastrukture i sektor poslovnih usluga za državna tijela.

sektor bankarstva, odbijeni, pozivajući se na članak 40. Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga kojim je predviđena mogućnost ograničavanja pristupa podacima o popisu operatora ključnih usluga od strane nadležnog tijela.

Budući da autor ovog istraživanja nije bio u mogućnosti dobiti popis operatora ključnih usluga za pojedini sektor, osim sektora bankarstva, čime bi se odredila cijela ciljana populacija, nije bilo moguće provesti statistički nasumično uzorkovanje već se morala primijeniti jedna od metoda neprobabilističkog uzorkovanja, čime se smanjuje mogućnost generalizacije rezultata, što je ujedno i najveće ograničenje ovog istraživanja. Kao metoda prikupljanja podataka uzeta je metoda neprobabilističkog uzorkovanja pod nazivom metoda snježne grude (engl. *Snowball sampling*) u kojoj su sudionici zamoljeni da proslijede poveznicu na anketni upitnik drugim potencijalnim sudionicima kako bi se postigla maksimalna moguća veličinu uzorka. Istraživači koriste ovu tehniku kad trebaju identificirati ljude koje je iz nekog razloga teško pronaći [310]. Prilikom uzorkovanja metodom snježne grude, istraživač prikuplja podatke o nekolicini pripadnika ciljane populacije koje sam može locirati, a zatim od tih osoba traži pomoć u pronalasku ostalih članova te populacije za koje sami znaju [342]. Odakle i dolazi naziv metode budući da se sudionici istraživanja akumuliraju tijekom vremena [319], a povećanjem uzorka, prikuplja se dovoljno podataka koji su upotrebljivi za daljnju analizu. Ponekad se izraz *lančano uzorkovanje* (engl. *Chain Referral*) koristi u odnosu na uzorkovanje snježne grude i druge slične tehnike u kojima se uzorak razvija i raste iz početne selekcije. Općenita mana neprobabilističkih tehnika uzorkovanja je da nijedna od njih ne osigurava da će rezultirajući uzorak biti reprezentativan za populaciju koja je uzorkovana [342], ali su takve metode ponekad nužne da bi se provelo istraživanje [319].

Prikupljanje sudionika iz opsega istraživanja metodom snježne grude započelo je slanjem elektroničke poruke s kratkim opisom istraživanja u kojoj se potencijalne sudionike istraživanja zamolilo za povratnu informaciju ukoliko su zainteresirani za sudjelovanje u predmetnom istraživanju, na generičke (info, upiti, about i sl.) adrese elektroničke poruke objavljene na službenim stranicama organizacija za koje se sa sigurnošću znalo da predstavljaju operatore ključnih usluga (Prilog 4.). Iako je službena potvrda identificiranih operatora ključnih usluga stigla jedino od nadležnog sektorskog tijela za sektor bankarstva, za neke operatore ključnih usluga iz drugih sektora autor je također saznao, bilo putem jedinstvene definicije operatora za pojedini sektor iz Priloga I. Zakona o kibernetičkoj sigurnosti, bilo putem sudjelovanja na formalnim i neformalnim sastancima strukovnih udruga vezanih uz informacijsku sigurnost i osobnih kontakata. Ukoliko bi se dobio pozitivan odgovor na poziv za sudjelovanje u

istraživanju, poslana je druga poruka elektroničke poruke u kojoj se nalazila poveznica na online upitnik, a koja je bila namijenjena prosljeđivanju na druge kolege iz organizacije (Prilog 4.). Budući da, na ovakav način prikupljanja mogućih sudionika, usko grlo predstavlja ulazna točka (generička adresa elektroničke pošte koja je često, uslijed javne dostupnosti, zatrpana raznim oblicima neželjene pošte, odnosno osoba koja provjerava dolaznu elektroničku poštu), isti je upit poslan još dva puta u razmaku od nekoliko tjedana. Usporedo s tim, autor ovog istraživanja putem poslovne društvene mreže LinkedIn, s istim upitom kontaktirao je neke od osoba iz čijih se profila na društvenoj mreži vidjelo da rade u organizacijama od interesa za ovo istraživanje. Prikupljanje podataka putem online upitnika trajalo je od 01.11.2019. do 31.01.2020. godine te je u tom periodu sudjelovalo ukupno 506 sudionika, od čega je 240 sudionika u potpunosti ispunilo upitnik dok je djelomično ispunilo njih 266. Naknadnim uvidom u 240 u potpunosti ispunjenih upitnika utvrđeno je kako je kod jednog sudionika u svim odgovorima bila odabrana opcija „nije primjenjivo" zbog čega je isključena i ta opservacija te je za daljnju analizu korišten set od 239 odgovora.

6.3.2. Rezultati faktorske analize

Uzevši u obzir da je ukupan broj pitanja u anketnom upitniku bio 79 (67 vezano za percepciju zaposlenika o čimbenicima kulture informacijske sigurnosti i 12 vezano za stvarno stanje u organizaciji po pitanju implementiranih mjera dobre prakse), ukupan broj od 239 u potpunosti ispunjenih upitnika zadovoljava kriterij od minimalno tri puta više opservacija od manifestnih varijabli [319], [323].

Za procjenu valjanosti i mogućnosti provođenja faktorske analize, u sljedećem koraku korišteni su Kaiser-Meyer-Olkin (KMO) mjera adekvatnosti uzorka i Bartlettov test sfericiteta.

Kako bi se dodatno ispitala valjanost mjernog instrumenta i potvrdila konstruktna i konvergentna valjanost radnog okvira za procjenu i unapređenje kulture informacijske sigurnosti, napravljena je eksploratorna faktorska analiza posebno za svaku od 3 kategorije, koje su bile potvrđene kao nužne od strane eksperata u ranijim koracima ovog istraživanja. Faktorska analiza je rađena u programskom alatu IBM SPSS Statistics v26, a za ekstrakciju faktora odabrana je metoda Principal axis factoring i Varimax ortogonalna rotacija.

6.3.2.1. Kategorija Organizacijske mjere

U prvom koraku napravljena je korelacijska matrica te su identificirani parovi manifestnih varijabli koji visoko koreliraju. Kao granica je uzeta vrijednost 0,8 [307] te je uklonjena po

jedna manifestna varijabla iz visokokorelirajućih parova, kako bi se smanjila multikolinearnost. Ne postoji statistički način za određivanje koju manifestnu varijablu iz tog para treba ukloniti već je to stvar interpretacije istraživača [324]. Tablica 6.7. prikazuje korelacijsku matricu za čestice iz kategorije *Organizacijske mjere* s označenim parovima manifestnih varijabli koje visoko koreliraju dok Tablica 6.8. detaljnije prikazuje te parove varijabli s obrazloženjem koje od njih se isključuju iz daljnjeg istraživanja.

Tablica 6.7. Korelacijska matrica za manifestne varijable iz kategorije *Organizacijske mjere*

	POL1	POL2	POL3	POL4	POL5	POL6	POL7	POL8	POL9
POL1	1,000	0,797	0,792	0,738	0,642	0,672	0,512	0,477	0,548
POL2	0,797	1,000	0,892	0,758	0,738	0,741	0,614	0,528	0,519
POL3	0,792	0,892	1,000	0,771	0,708	0,739	0,566	0,555	0,550
POL4	0,738	0,758	0,771	1,000	0,662	0,709	0,641	0,560	0,508
POL5	0,642	0,738	0,708	0,662	1,000	0,785	0,555	0,458	0,513
POL6	0,672	0,741	0,739	0,709	0,785	1,000	0,617	0,473	0,536
POL7	0,512	0,614	0,566	0,641	0,555	0,617	1,000	0,710	0,433
POL8	0,477	0,528	0,555	0,560	0,458	0,473	0,710	1,000	0,397
POL9	0,548	0,519	0,550	0,508	0,513	0,536	0,433	0,397	1,000
POL10	0,679	0,690	0,695	0,693	0,654	0,673	0,664	0,585	0,668
POL11	0,620	0,655	0,650	0,636	0,665	0,683	0,535	0,482	0,647
POL12	0,540	0,510	0,612	0,478	0,494	0,560	0,369	0,395	0,463
MNG1	0,648	0,662	0,673	0,628	0,558	0,636	0,557	0,510	0,481
MNG2**	0,172	0,144	0,113	0,126	0,034	0,143	0,067	0,050	0,112
MNG3	0,472	0,511	0,539	0,548	0,467	0,501	0,442	0,399	0,480
MNG4	0,473	0,529	0,545	0,540	0,506	0,525	0,532	0,453	0,446
MNG5	0,564	0,629	0,642	0,592	0,559	0,583	0,498	0,524	0,456
MNG6	0,485	0,530	0,540	0,541	0,512	0,547	0,481	0,449	0,432
MNG7	0,540	0,615	0,612	0,605	0,526	0,566	0,519	0,493	0,479
EDU1	0,197	0,206	0,227	0,170	0,261	0,293	0,232	0,179	0,231
EDU2	0,402	0,450	0,467	0,390	0,447	0,429	0,393	0,381	0,341
EDU3	0,440	0,474	0,447	0,460	0,427	0,442	0,501	0,466	0,376
EDU4	0,509	0,556	0,520	0,538	0,552	0,554	0,572	0,475	0,438
EDU5	0,544	0,580	0,528	0,538	0,538	0,535	0,560	0,457	0,489
EDU6	0,488	0,551	0,516	0,474	0,527	0,500	0,490	0,387	0,446
EDU7	0,475	0,514	0,470	0,498	0,529	0,497	0,462	0,408	0,422
EDU8	0,582	0,546	0,554	0,519	0,517	0,573	0,525	0,505	0,479
EDU9	0,691	0,644	0,632	0,630	0,552	0,564	0,518	0,426	0,493
EDU10	0,444	0,351	0,390	0,284	0,370	0,328	0,286	0,307	0,329
EDU11	0,422	0,399	0,419	0,271	0,391	0,358	0,267	0,280	0,164
EDU12**	0,225	0,193	0,222	0,186	0,190	0,223	0,086	0,190	0,191
EDU13	0,234	0,228	0,209	0,237	0,245	0,202	0,161	0,184	0,223
EDU14	0,557	0,569	0,543	0,542	0,530	0,570	0,480	0,416	0,376

Tablica 6.7. Korelacijska matrica za manifestne varijable iz kategorije *Organizacijske mjere* (nastavak)

	POL1	POL2	POL3	POL4	POL5	POL6	POL7	POL8	POL9
EDU15	0,512	0,583	0,542	0,613	0,478	0,550	0,541	0,489	0,482
EDU16	0,682	0,665	0,659	0,669	0,572	0,625	0,640	0,524	0,559
EDU17	0,603	0,651	0,647	0,566	0,573	0,633	0,524	0,444	0,528
EDU18	0,413	0,466	0,467	0,402	0,477	0,500	0,341	0,304	0,451
EDU19	0,448	0,498	0,543	0,457	0,503	0,549	0,385	0,329	0,413
CMP1	0,446	0,476	0,493	0,447	0,532	0,480	0,362	0,415	0,374
CMP2	0,569	0,597	0,591	0,605	0,572	0,593	0,550	0,503	0,484
CMP3	0,565	0,602	0,586	0,616	0,574	0,578	0,523	0,502	0,493
CMP4	0,539	0,600	0,579	0,598	0,539	0,556	0,525	0,496	0,486

	POL10	POL11	POL12	MNG1	MNG2**	MNG3	MNG4	MNG5	MNG6
POL1	0,679	0,620	0,540	0,648	0,172	0,472	0,473	0,564	0,485
POL2	0,690	0,655	0,510	0,662	0,144	0,511	0,529	0,629	0,530
POL3	0,695	0,650	0,612	0,673	0,113	0,539	0,545	0,642	0,540
POL4	0,693	0,636	0,478	0,628	0,126	0,548	0,540	0,592	0,541
POL5	0,654	0,665	0,494	0,558	0,034	0,467	0,506	0,559	0,512
POL6	0,673	0,683	0,560	0,636	0,143	0,501	0,525	0,583	0,547
POL7	0,664	0,535	0,369	0,557	0,067	0,442	0,532	0,498	0,481
POL8	0,585	0,482	0,395	0,510	0,050	0,399	0,453	0,524	0,449
POL9	0,668	0,647	0,463	0,481	0,112	0,480	0,446	0,456	0,432
POL10	1,000	0,694	0,513	0,615	0,166	0,500	0,543	0,564	0,558
POL11	0,694	1,000	0,573	0,562	0,114	0,502	0,482	0,557	0,517
POL12	0,513	0,573	1,000	0,529	0,050	0,396	0,383	0,536	0,343
MNG1	0,615	0,562	0,529	1,000	0,149	0,612	0,635	0,720	0,651
MNG2**	0,166	0,114	0,050	0,149	1,000	0,052	0,106	0,117	0,156
MNG3	0,500	0,502	0,396	0,612	0,052	1,000	0,665	0,661	0,657
MNG4	0,543	0,482	0,383	0,635	0,106	0,665	1,000	0,747	0,722
MNG5	0,564	0,557	0,536	0,720	0,117	0,661	0,747	1,000	0,692
MNG6	0,558	0,517	0,343	0,651	0,156	0,657	0,722	0,692	1,000
MNG7	0,599	0,538	0,421	0,745	0,141	0,700	0,716	0,775	0,807
EDU1	0,258	0,344	0,306	0,205	0,042	0,191	0,203	0,213	0,178
EDU2	0,474	0,443	0,392	0,408	0,161	0,456	0,475	0,517	0,513
EDU3	0,556	0,409	0,288	0,407	0,194	0,436	0,469	0,445	0,568
EDU4	0,615	0,525	0,332	0,482	0,205	0,522	0,546	0,519	0,659
EDU5	0,649	0,555	0,337	0,560	0,204	0,543	0,540	0,529	0,667
EDU6	0,547	0,504	0,358	0,491	0,117	0,503	0,490	0,539	0,567
EDU7	0,547	0,440	0,266	0,510	0,084	0,523	0,563	0,590	0,620
EDU8	0,537	0,501	0,391	0,508	0,135	0,429	0,384	0,424	0,538
EDU9	0,585	0,532	0,496	0,593	0,123	0,460	0,448	0,544	0,472
EDU10	0,339	0,348	0,379	0,352	0,022	0,261	0,289	0,259	0,209
EDU11	0,267	0,318	0,508	0,332	-0,090	0,219	0,153	0,296	0,179

Tablica 6.7. Korelacijska matrica za manifestne varijable iz kategorije *Organizacijske mjere* (nastavak)

	POL10	POL11	POL12	MNG1	MNG2**	MNG3	MNG4	MNG5	MNG6
EDU12**	0,122	0,158	0,206	0,232	0,156	0,156	0,095	0,223	0,128
EDU13	0,173	0,257	0,154	0,170	0,023	0,149	0,051	0,145	0,095
EDU14	0,488	0,585	0,408	0,505	0,092	0,423	0,449	0,504	0,436
EDU15	0,594	0,538	0,417	0,556	0,082	0,514	0,571	0,558	0,579
EDU16	0,696	0,629	0,496	0,611	0,109	0,525	0,553	0,577	0,573
EDU17	0,585	0,725	0,516	0,530	0,074	0,426	0,448	0,490	0,467
EDU18	0,456	0,514	0,389	0,390	0,080	0,336	0,282	0,280	0,364
EDU19	0,428	0,555	0,455	0,403	0,022	0,373	0,344	0,379	0,382
CMP1	0,447	0,506	0,405	0,454	0,095	0,420	0,422	0,414	0,451
CMP2	0,617	0,514	0,353	0,514	0,115	0,408	0,475	0,491	0,539
CMP3	0,621	0,546	0,394	0,528	0,190	0,470	0,488	0,537	0,540
CMP4	0,633	0,526	0,380	0,535	0,173	0,507	0,503	0,553	0,571

	MNG7	EDU1	EDU2	EDU3	EDU4	EDU5	EDU6	EDU7	EDU8
POL1	0,540	0,197	0,402	0,440	0,509	0,544	0,488	0,475	0,582
POL2	0,615	0,206	0,450	0,474	0,556	0,580	0,551	0,514	0,546
POL3	0,612	0,227	0,467	0,447	0,520	0,528	0,516	0,470	0,554
POL4	0,605	0,170	0,390	0,460	0,538	0,538	0,474	0,498	0,519
POL5	0,526	0,261	0,447	0,427	0,552	0,538	0,527	0,529	0,517
POL6	0,566	0,293	0,429	0,442	0,554	0,535	0,500	0,497	0,573
POL7	0,519	0,232	0,393	0,501	0,572	0,560	0,490	0,462	0,525
POL8	0,493	0,179	0,381	0,466	0,475	0,457	0,387	0,408	0,505
POL9	0,479	0,231	0,341	0,376	0,438	0,489	0,446	0,422	0,479
POL10	0,599	0,258	0,474	0,556	0,615	0,649	0,547	0,547	0,537
POL11	0,538	0,344	0,443	0,409	0,525	0,555	0,504	0,440	0,501
POL12	0,421	0,306	0,392	0,288	0,332	0,337	0,358	0,266	0,391
MNG1	0,745	0,205	0,408	0,407	0,482	0,560	0,491	0,510	0,508
MNG2**	0,141	0,042	0,161	0,194	0,205	0,204	0,117	0,084	0,135
MNG3	0,700	0,191	0,456	0,436	0,522	0,543	0,503	0,523	0,429
MNG4	0,716	0,203	0,475	0,469	0,546	0,540	0,490	0,563	0,384
MNG5	0,775	0,213	0,517	0,445	0,519	0,529	0,539	0,590	0,424
MNG6	0,807	0,178	0,513	0,568	0,659	0,667	0,567	0,620	0,538
MNG7	1,000	0,195	0,537	0,548	0,659	0,682	0,642	0,608	0,527
EDU1	0,195	1,000	0,431	0,217	0,229	0,287	0,335	0,207	0,302
EDU2	0,537	0,431	1,000	0,606	0,625	0,521	0,673	0,549	0,413
EDU3	0,548	0,217	0,606	1,000	0,825	0,707	0,668	0,607	0,544
EDU4	0,659	0,229	0,625	0,825	1,000	0,832	0,718	0,739	0,615
EDU5	0,682	0,287	0,521	0,707	0,832	1,000	0,720	0,734	0,683
EDU6	0,642	0,335	0,673	0,668	0,718	0,720	1,000	0,649	0,541
EDU7	0,608	0,207	0,549	0,607	0,739	0,734	0,649	1,000	0,556
EDU8	0,527	0,302	0,413	0,544	0,615	0,683	0,541	0,556	1,000
EDU9	0,530	0,323	0,424	0,465	0,534	0,613	0,530	0,567	0,648

Tablica 6.7. Korelacijska matrica za manifestne varijable iz kategorije *Organizacijske mjere* (nastavak)

	MNG7	EDU1	EDU2	EDU3	EDU4	EDU5	EDU6	EDU7	EDU8
EDU10	0,305	0,319	0,252	0,229	0,305	0,343	0,289	0,206	0,329
EDU11	0,207	0,272	0,211	0,189	0,201	0,221	0,223	0,139	0,301
EDU12**	0,180	0,251	0,125	0,057	0,062	0,072	0,096	0,092	0,245
EDU13	0,193	0,198	0,062	0,175	0,143	0,165	0,237	0,126	0,255
EDU14	0,528	0,263	0,440	0,509	0,576	0,542	0,560	0,505	0,543
EDU15	0,655	0,229	0,466	0,595	0,623	0,642	0,635	0,564	0,536
EDU16	0,655	0,266	0,490	0,634	0,696	0,722	0,608	0,616	0,671
EDU17	0,532	0,407	0,477	0,536	0,584	0,625	0,563	0,494	0,557
EDU18	0,374	0,362	0,309	0,379	0,451	0,452	0,507	0,385	0,465
EDU19	0,408	0,384	0,359	0,356	0,431	0,395	0,457	0,378	0,446
CMP1	0,490	0,347	0,434	0,447	0,511	0,528	0,521	0,409	0,463
CMP2	0,604	0,225	0,414	0,594	0,684	0,661	0,575	0,594	0,650
CMP3	0,582	0,210	0,447	0,610	0,698	0,699	0,613	0,626	0,594
CMP4	0,621	0,231	0,483	0,563	0,647	0,651	0,592	0,602	0,598

	EDU9	EDU10	EDU11	EDU12**	EDU13	EDU14	EDU15	EDU16	EDU17
POL1	0,691	0,444	0,422	0,225	0,234	0,557	0,512	0,682	0,603
POL2	0,644	0,351	0,399	0,193	0,228	0,569	0,583	0,665	0,651
POL3	0,632	0,390	0,419	0,222	0,209	0,543	0,542	0,659	0,647
POL4	0,630	0,284	0,271	0,186	0,237	0,542	0,613	0,669	0,566
POL5	0,552	0,370	0,391	0,190	0,245	0,530	0,478	0,572	0,573
POL6	0,564	0,328	0,358	0,223	0,202	0,570	0,550	0,625	0,633
POL7	0,518	0,286	0,267	0,086	0,161	0,480	0,541	0,640	0,524
POL8	0,426	0,307	0,280	0,190	0,184	0,416	0,489	0,524	0,444
POL9	0,493	0,329	0,164	0,191	0,223	0,376	0,482	0,559	0,528
POL10	0,585	0,339	0,267	0,122	0,173	0,488	0,594	0,696	0,585
POL11	0,532	0,348	0,318	0,158	0,257	0,585	0,538	0,629	0,725
POL12	0,496	0,379	0,508	0,206	0,154	0,408	0,417	0,496	0,516
MNG1	0,593	0,352	0,332	0,232	0,170	0,505	0,556	0,611	0,530
MNG2**	0,123	0,022	-0,090	0,156	0,023	0,092	0,082	0,109	0,074
MNG3	0,460	0,261	0,219	0,156	0,149	0,423	0,514	0,525	0,426
MNG4	0,448	0,289	0,153	0,095	0,051	0,449	0,571	0,553	0,448
MNG5	0,544	0,259	0,296	0,223	0,145	0,504	0,558	0,577	0,490
MNG6	0,472	0,209	0,179	0,128	0,095	0,436	0,579	0,573	0,467
MNG7	0,530	0,305	0,207	0,180	0,193	0,528	0,655	0,655	0,532
EDU1	0,323	0,319	0,272	0,251	0,198	0,263	0,229	0,266	0,407
EDU2	0,424	0,252	0,211	0,125	0,062	0,440	0,466	0,490	0,477
EDU3	0,465	0,229	0,189	0,057	0,175	0,509	0,595	0,634	0,536
EDU4	0,534	0,305	0,201	0,062	0,143	0,576	0,623	0,696	0,584
EDU5	0,613	0,343	0,221	0,072	0,165	0,542	0,642	0,722	0,625
EDU6	0,530	0,289	0,223	0,096	0,237	0,560	0,635	0,608	0,563
EDU7	0,567	0,206	0,139	0,092	0,126	0,505	0,564	0,616	0,494

Tablica 6.7. Korelacijska matrica za manifestne varijable iz kategorije *Organizacijske mjere* (nastavak)

	EDU9	EDU10	EDU11	EDU12**	EDU13	EDU14	EDU15	EDU16	EDU17
EDU8	0,648	0,329	0,301	0,245	0,255	0,543	0,536	0,671	0,557
EDU9	1,000	0,339	0,393	0,222	0,165	0,584	0,528	0,683	0,633
EDU10	0,339	1,000	0,466	0,107	0,223	0,341	0,287	0,363	0,401
EDU11	0,393	0,466	1,000	0,199	0,261	0,327	0,262	0,338	0,414
EDU12**	0,222	0,107	0,199	1,000	0,185	0,206	0,104	0,158	0,234
EDU13	0,165	0,223	0,261	0,185	1,000	0,431	0,258	0,277	0,416
EDU14	0,584	0,341	0,327	0,206	0,431	1,000	0,597	0,642	0,748
EDU15	0,528	0,287	0,262	0,104	0,258	0,597	1,000	0,733	0,589
EDU16	0,683	0,363	0,338	0,158	0,277	0,642	0,733	1,000	0,732
EDU17	0,633	0,401	0,414	0,234	0,416	0,748	0,589	0,732	1,000
EDU18	0,507	0,294	0,324	0,238	0,357	0,585	0,470	0,569	0,643
EDU19	0,537	0,321	0,468	0,278	0,319	0,553	0,437	0,571	0,689
CMP1	0,446	0,437	0,382	0,187	0,286	0,484	0,466	0,538	0,551
CMP2	0,567	0,362	0,324	0,204	0,332	0,589	0,635	0,685	0,634
CMP3	0,584	0,304	0,251	0,149	0,286	0,572	0,614	0,694	0,639
CMP4	0,575	0,311	0,270	0,189	0,230	0,522	0,620	0,657	0,581

	EDU18	EDU19	CMP1	CMP2	CMP3	CMP4
POL1	0,413	0,448	0,446	0,569	0,565	0,539
POL2	0,466	0,498	0,476	0,597	0,602	0,600
POL3	0,467	0,543	0,493	0,591	0,586	0,579
POL4	0,402	0,457	0,447	0,605	0,616	0,598
POL5	0,477	0,503	0,532	0,572	0,574	0,539
POL6	0,500	0,549	0,480	0,593	0,578	0,556
POL7	0,341	0,385	0,362	0,550	0,523	0,525
POL8	0,304	0,329	0,415	0,503	0,502	0,496
POL9	0,451	0,413	0,374	0,484	0,493	0,486
POL10	0,456	0,428	0,447	0,617	0,621	0,633
POL11	0,514	0,555	0,506	0,514	0,546	0,526
POL12	0,389	0,455	0,405	0,353	0,394	0,380
MNG1	0,390	0,403	0,454	0,514	0,528	0,535
MNG2**	0,080	0,022	0,095	0,115	0,190	0,173
MNG3	0,336	0,373	0,420	0,408	0,470	0,507
MNG4	0,282	0,344	0,422	0,475	0,488	0,503
MNG5	0,280	0,379	0,414	0,491	0,537	0,553
MNG6	0,364	0,382	0,451	0,539	0,540	0,571
MNG7	0,374	0,408	0,490	0,604	0,582	0,621
EDU1	0,362	0,384	0,347	0,225	0,210	0,231
EDU2	0,309	0,359	0,434	0,414	0,447	0,483
EDU3	0,379	0,356	0,447	0,594	0,610	0,563
EDU4	0,451	0,431	0,511	0,684	0,698	0,647
EDU5	0,452	0,395	0,528	0,661	0,699	0,651

Tablica 6.7. Korelacijska matrica za manifestne varijable iz kategorije *Organizacijske mjere* (nastavak)

	EDU18	EDU19	CMP1	CMP2	CMP3	CMP4
EDU6	0,507	0,457	0,521	0,575	0,613	0,592
EDU7	0,385	0,378	0,409	0,594	0,626	0,602
EDU8	0,465	0,446	0,463	0,650	0,594	0,598
EDU9	0,507	0,537	0,446	0,567	0,584	0,575
EDU10	0,294	0,321	0,437	0,362	0,304	0,311
EDU11	0,324	0,468	0,382	0,324	0,251	0,270
EDU12**	0,238	0,278	0,187	0,204	0,149	0,189
EDU13	0,357	0,319	0,286	0,332	0,286	0,230
EDU14	0,585	0,553	0,484	0,589	0,572	0,522
EDU15	0,470	0,437	0,466	0,635	0,614	0,620
EDU16	0,569	0,571	0,538	0,685	0,694	0,657
EDU17	0,643	0,689	0,551	0,634	0,639	0,581
EDU18	1,000	0,791	0,534	0,470	0,494	0,477
EDU19	0,791	1,000	0,549	0,498	0,473	0,471
CMP1	0,534	0,549	1,000	0,543	0,517	0,503
CMP2	0,470	0,498	0,543	1,000	0,814	0,801
CMP3	0,494	0,473	0,517	0,814	1,000	0,872
CMP4	0,477	0,471	0,503	0,801	0,872	1,000

a. Determinant = 3,804E-18

Izvor: *vlastiti prikaz*

Tablica 6.8. Parovi manifestnih varijabli iz kategorije *Organizacijske mjere* koje visoko koreliraju

Rbr.	**Parovi varijabli koje visoko koreliraju**	**Obrazloženje isključivanja varijable**
1.	*POL2 – Politika informacijske sigurnosti jasno definira ciljeve informacijske sigurnosti moje organizacije** POL3 - Politika informacijske sigurnosti jasno ističe važnost informacijske sigurnosti za organizaciju	Važnost informacijske sigurnosti općenitiji je pojam od ciljeva gdje definirani ciljevi predstavljaju jedan od eksplicitnih pokazatelja važnosti
2.	*MNG6 – Rukovodstvo u mojoj organizaciji sudjeluje u edukacijama, projektima, radionicama podizanja svijesti i ostalim aktivnostima vezanim uz informacijsku sigurnost** MNG7 - U mojoj organizaciji vidljiva je predanost i potpora od strane rukovodstva vezano za informacijsku sigurnost	Sudjelovanje rukovodstva u aktivnostima vezanim uz informacijsku sigurnost jedan je od vidova njihove predanosti i potpore informacijskoj sigurnosti
3.	EDU3 – U mojoj organizaciji podržava se periodično održavanje radionica za zaposlenike na temu informacijske sigurnosti *EDU4 - U mojoj organizaciji svi zaposlenici dobivaju dovoljnu i primjerenu edukaciju o informacijskoj sigurnosti**	Varijabla EDU4 visoko korelira s druge dvije varijable te njenim uklanjanjem rješava se pitanje dva visokokorelirajuća para varijabli

Tablica 6.8. Parovi manifestnih varijabli iz kategorije *Organizacijske mjere* koje visoko koreliraju (nastavak)

Rbr.	Parovi varijabli koje visoko koreliraju	Obrazloženje isključivanja varijable
4.	*EDU4 – U mojoj organizaciji svi zaposlenici dobivaju dovoljnu i primjerenu edukaciju o informacijskoj sigurnosti** EDU5 - Zaposlenici su educirani oko svojih uloga i odgovornosti vezanih za informacijsku sigurnost i toga kako se ponašati na siguran način	Varijabla EDU4 visoko korelira s druge dvije varijable te njenim uklanjanjem rješava se pitanje dva visokokorelirajuća para varijabli
5.	*CMP2 – Moja organizacija provodi periodične provjere radi utvrđivanja usklađenosti sa politikom informacijske sigurnosti** CMP3 - U mojoj organizaciji provjerava se slijede li zaposlenici sigurnosne politike, procedure i smjernice	Slijeđenje odredbi politike informacijske sigurnosti podrazumijeva usklađenost s politikom
6.	CMP2 – Moja organizacija provodi periodične provjere radi utvrđivanja usklađenosti sa politikom informacijske sigurnosti *CMP4 - U mojoj organizaciji redovno se provjerava učinkovitost i potpunost politike informacijske sigurnosti**	Prosječni zaposlenik ne mora nužno znati provjerava li se potpunost sigurnosne politike, ali trebao bi znati provode li se provjere usklađenosti zaposlenika
7.	CMP3 – U mojoj organizaciji provjerava se slijede li zaposlenici sigurnosne politike, procedure i smjernice *CMP4 - U mojoj organizaciji redovno se provjerava učinkovitost i potpunost politike informacijske sigurnosti**	Prosječni zaposlenik ne mora nužno znati provjerava li se potpunost sigurnosne politike, ali trebao bi znati provode li se provjere slijeđenja politike od strane zaposlenika

* manifestne varijable koje se isključuju

Izvor: *vlastiti prikaz*

Kategorija *Organizacijske mjere* inicijalno se sastojala od 42 manifestne varijable raspoređene u 4 čimbenika kako je vidljivo iz Tablice 6.9., a zbog visoke korelacije isključeno je 5 manifestnih varijabli koje su u Tablici 6.9. naznačene crvenom bojom.

Tablica 6.9. Popis inicijalnih manifestnih varijabli po pojedinom čimbeniku kategorije *Organizacijske mjere*

Čimbenik	Varijable (čestice)	Broj varijabli
Politike i odgovornosti	POL1, POL2, POL3, POL4, POL5, POL6, POL7, POL8, POL9, POL10, POL11, POL12	12 (11)
Podrška rukovodstva	MNG1, MNG2, MNG3, MNG4, MNG5, MNG6, MNG7	7 (6)
Edukacija i osviještenost	EDU1, EDU2, EDU3, EDU4, EDU5, EDU6, EDU7, EDU8, EDU9, EDU10, EDU11, EDU12, EDU13, EDU14, EDU15, EDU16, EDU17, EDU18, EDU19	19 (18)
Usklađenost	CMP1, CMP2,CMP3, CMP4	4 (2)

Izvor: *vlastiti prikaz*

Kako bi se provjerilo jesu li podaci dobiveni empirijskim istraživanjem pogodni za faktorsku analizu, napravljena je Kaiser-Meyer-Olkin-ova (KMO) mjera adekvatnosti uzorka i Bartlettov test sfericiteta. Kao što je vidljivo iz Tablice 10. KMO iznosi 0,948 što se smatra izvrsnim

rezultatom, a Bartlettov test sfericiteta značajan je na razini $p < 0.001$ što znači da postoje adekvatne veze (korelacije) između manifestnih varijabli uključenih u analizu te se može nastaviti s provedbom faktorske analize jer se očekuje da promatrane manifestne varijable opisuju istu latentnu varijablu [307].

Tablica 6.10. Kaiser-Meyer-Olkin-ova (KMO) mjera adekvatnosti uzorka i Bartlettov test sfericiteta za kategoriju *Organizacijske mjere*

KMO i Bartlettov test

Kaiser-Meyer-Olkin-ova mjera adekvatnosti uzorka		0,948
Bartlettov test sfericiteta	Pribl. Hi-kvadrat	7056,758
	df	666
	Sig.	0,000

Izvor: *vlastiti prikaz*

Nakon što je isključeno 5 varijabli koje visoko koreliraju s drugima i napravljena provjera primjerenosti provođenja faktorske analize putem KMO mjere i Bartlettovog testa sfericiteta, napravljena je ekstrakcija faktora putem metode Principal axis factoring. Korištenjem Kaiserovog pravila o značajnosti varijabli koje imaju svojstvenu vrijednost (engl. *Eigenvalue*) veću od 1 predloženo je 6 faktora, kao što je vidljivo iz Tablice 6.11..

Tablica 6.11. Inicijalno određen broj faktora za kategoriju *Organizacijske mjere* putem vrijednosti svojstvenih faktora

Ukupna objašnjena varijanca

Faktor	Inicijalne svojstvene vrijednosti			Ekstrakcijske sume kvadriranih opterećenja			Rotacijske sume kvadriranih opterećenja		
	Ukupno	% varijance	Kumulativni %	Ukupno	% varijance	Kumulativni %	Ukupno	% varijance	Kumulativni %
1	17,693	47,820	47,820	17,364	46,929	46,929	6,225	16,825	16,825
2	2,244	6,064	53,884	1,862	5,033	51,963	5,812	15,707	32,532
3	1,718	4,642	58,526	1,387	3,750	55,713	4,003	10,818	43,350
4	1,262	3,412	61,939	0,888	2,400	58,113	3,973	10,737	54,087
5	1,177	3,181	65,120	0,652	1,761	59,874	1,562	4,221	58,308
6	1,055	2,852	67,972	0,567	1,533	61,407	1,147	3,099	61,407
7	0,965	2,609	70,581						
8	0,874	2,362	72,944						
9	0,843	2,279	75,223						
10	0,743	2,007	77,230						
11	0,687	1,856	79,086						
12	0,655	1,770	80,856						

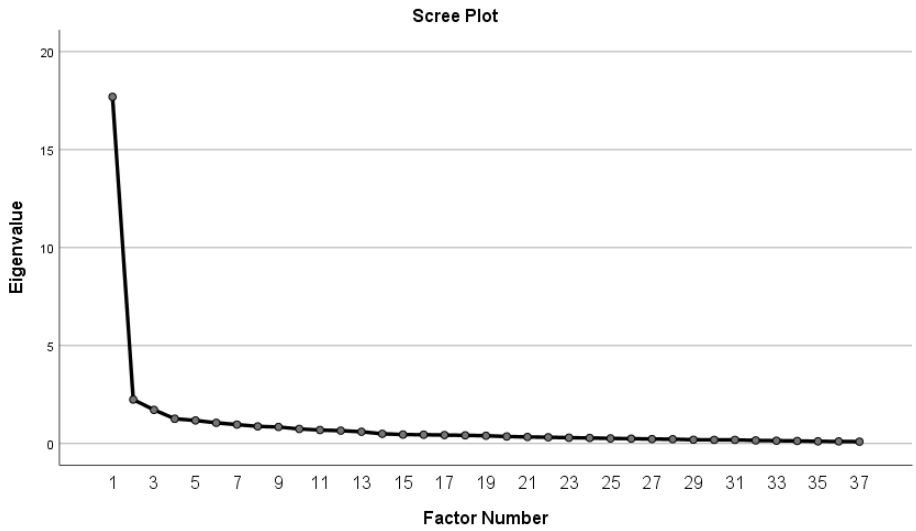
Tablica 6.11. Inicijalno određen broj faktora za kategoriju *Organizacijske mjere* putem vrijednosti svojstvenih faktora (nastavak)

Faktor	Inicijalne svojstvene vrijednosti			Ekstrakcijske sume kvadriranih opterećenja			Rotacijske sume kvadriranih opterećenja		
	Ukupno	% varijance	Kumulativni %	Ukupno	% varijance	Kumulativni %	Ukupno	% varijance	Kumulativni %
13	0,598	1,616	82,472						
14	0,495	1,339	83,811						
15	0,456	1,231	85,043						
16	0,449	1,215	86,257						
17	0,433	1,170	87,427						
18	0,415	1,122	88,549						
19	0,395	1,067	89,616						
20	0,357	0,965	90,582						
21	0,333	0,900	91,482						
22	0,318	0,859	92,341						
23	0,295	0,796	93,138						
24	0,282	0,761	93,899						
25	0,260	0,702	94,601						
26	0,248	0,670	95,271						
27	0,226	0,610	95,881						
28	0,220	0,596	96,477						
29	0,193	0,520	96,997						
30	0,187	0,506	97,504						
31	0,184	0,497	98,001						
32	0,157	0,425	98,425						
33	0,143	0,387	98,812						
34	0,127	0,344	99,156						
35	0,112	0,304	99,460						
36	0,106	0,285	99,745						
37	0,094	0,255	100,000						

Metoda ekstrakcije: Principal Axis Factoring.

Izvor: *vlastiti prikaz*

Scree test u ovoj situaciji ne pomaže previše zbog gusto raspoređenih varijabli na osi apscise, kao što je vidljivo na Grafikonu 6.2.



Grafikon 6.2. Određivanje mogućeg broja faktora za kategoriju *Organizacijske mjere* putem Scree testa

Izvor: *vlastiti prikaz*

Za određivanje broja faktora putem paralelne analize korištena je aplikacija MonteCarlo PCA for Parallel Analysis[12], a usporedni rezultati inicijalnih i nasumično simuliranih svojstvenih vrijednosti prikazani su u Tablici 6.12. iz koje je vidljivo kako su inicijalne svojstvene vrijednosti veće u prva tri para, nakon čega postaju veće nasumično simulirane svojstvene vrijednosti. Iz toga proizlazi da bi, prema kriteriju paralelne analize, broj ekstrahiranih faktora bio 3.

Tablica 6.12. Određivanje broja faktora za kategoriju *Organizacijske mjere* pomoću paralelne analize

Paralelna analiza

Faktor	Inicijalne svojstvene vrijednosti	Slučajne svojstvene vrijednosti
1	17,693	1,844
2	2,244	1,730
3	1,718	1,652
4	1,262	1,584
5	1,177	1,525
6	1,055	1,471

Izvor: *vlastiti prikaz*

Budući da se broj faktora koji najbolje opisuju odnos između manifestnih varijabli razlikuje na temelju rezultata Kaiserovog testa (6 faktora) i testa paralelne analize (3 faktora), a Scree test

[12] Dostupno na adresi: http://spss.allenandunwin.com.s3-website-ap-southeast-2.amazonaws.com/data-files.html#.Xnfh1nIo-Uk (pristupano: 17.05.2020.)

ne prikazuje jednostavno rješenje, potrebno je izvršiti daljnju analizu kako bi se u konačnici odredio optimalan broj faktora koji najbolje opisuju odnos između manifestnih varijabli u kategoriji *Organizacijske mjere*.

Sljedeći koraci obuhvaćali su izradu tablice komunaliteta i faktorske matrice. Iz tablice komunaliteta (Tablica 6.13.) vidljivo je da su svi inicijalni komunaliteti veći od 0,2 [324] te se sve manifestne varijable uzimaju u daljnju analizu.

Tablica 6.13. Tablica komunaliteta za kategoriju *Organizacijske mjere*

Komunaliteti

Varijabla	Početno stanje	Ekstrakcija	Varijabla	Početno stanje	Ekstrakcija
POL1	0,778	0,714	EDU3	0,664	0,683
POL3	0,799	0,773	EDU5	0,821	0,793
POL4	0,772	0,742	EDU6	0,738	0,713
POL5	0,742	0,631	EDU7	0,689	0,633
POL6	0,774	0,716	EDU8	0,667	0,577
POL7	0,728	0,570	EDU9	0,703	0,588
POL8	0,653	0,465	EDU10	0,419	0,348
POL9	0,606	0,510	EDU11	0,535	0,697
POL10	0,757	0,772	EDU12**	0,263	0,127
POL11	0,747	0,703	EDU13	0,404	0,268
POL12	0,579	0,557	EDU14	0,694	0,632
MNG1	0,714	0,701	EDU15	0,675	0,620
MNG2**	0,232	0,052	EDU16	0,799	0,776
MNG3	0,608	0,598	EDU17	0,820	0,763
MNG4	0,702	0,688	EDU18	0,741	0,738
MNG5	0,795	0,815	EDU19	0,757	0,713
MNG7	0,797	0,817	CMP1	0,540	0,492
EDU1	0,430	0,390	CMP3	0,659	0,654
EDU2	0,648	0,691			

Metoda ekstrakcije: Principal Axis Factoring.

Izvor: *vlastiti prikaz*

Sljedeći korak bio je dobivanje faktorske matrice. Budući da iz faktorske matrice nije bilo moguće jednostavno interpretirati rezultate, osim da dvije manifestne varijable (MNG2 i EDU12) nemaju značajno faktorsko opterećenje (>= 0,3), napravljena je i rotirana faktorska matrica (Tablica 6.14.).

Tablica 6.14. Početna i rotirana faktorska matrica za kategoriju *Organizacijske mjere*

	Faktorska matrica[a]							Rotirana faktorska matrica[a]					
	Faktor							Faktor					
	1	2	3	4	5	6		1	2	3	4	5	6
EDU16	0,852						POL10	0,706	0,425				
POL3	0,819						POL4	0,683	0,314		0,330		
POL10	0,805						POL3	0,680			0,347		
EDU17	0,804						POL6	0,663		0,316			
POL6	0,796						POL1	0,659					
EDU5	0,788						POL11	0,615		0,390			
POL4	0,786						POL5	0,594					
MNG7	0,785	-0,329					POL9	0,544					
POL1	0,779						POL7	0,537	0,442				
POL11	0,774						POL12	0,473				0,353	
CMP3	0,767						POL8	0,459	0,365				
MNG1	0,762						EDU9	0,449	0,406	0,333			
POL5	0,760						EDU5		0,764				
EDU9	0,755						EDU3		0,754				
MNG5	0,751			0,311			EDU6		0,656				
EDU15	0,750						EDU7		0,639		0,366		
EDU6	0,739		0,349				CMP3	0,390	0,583	0,325			
EDU14	0,729						EDU16	0,454	0,574	0,385			
EDU8	0,718						EDU15	0,313	0,545	0,301	0,359		
POL7	0,701						EDU8	0,382	0,536				
EDU7	0,699	-0,305					MNG2**						
MNG4	0,688	-0,350					EDU18			0,764			
EDU3	0,675		0,359				EDU19			0,724			
MNG3	0,670						EDU17	0,389	0,394	0,613			
EDU19	0,657	0,451					EDU14		0,420	0,547			
POL9	0,655						EDU13			0,473			
CMP1	0,648						CMP1		0,338	0,414			
POL8	0,635						EDU12**						
EDU18	0,633	0,414					MNG5	0,361			0,754		
EDU2	0,626						MNG7		0,449		0,704		
POL12	0,621						MNG4	0,313	0,333		0,678		
EDU10	0,456						MNG3				0,624		
EDU1	0,377						MNG1	0,469			0,582		
EDU12**							EDU11			0,314		0,739	
MNG2**							EDU10					0,431	
EDU11	0,435	0,494			0,323		EDU2		0,508		0,307		0,543
EDU13	0,312	0,313					EDU1						0,479

Metoda ekstrakcije: Principal Axis Factoring.

a. Izdvojeno 6 faktora. Potrebno 18 iteracija.

Izvor: *vlastiti prikaz*

Iz daljnje analize isključene su dvije manifestne varijable s nezadovoljavajućim faktorskim opterećenjem te je ponovno napravljena rotirana faktorska matrica. U toj matrici sve manifestne varijable imale su značajno faktorsko opterećenje te je napravljena analiza unakrsnog opterećenja. Iz rezultata prikazanih u Tablici 6.15. vidljivo je kako su varijable EDU16, CMP3, EDU8, MNG1, CMP1 i POL12, prema kriterijima koje su definirali Hair i suradnici [322], a opisano je u potpoglavlju 5.3.3., dobri kandidati za uklanjanje iz daljnje analize. Ujedno je potrebno uočiti kako je u ovoj iteraciji broj faktora predloženih na temelju svojstvenih vrijednosti (Kaiserovo pravilo) smanjen s početnih 6 na 5.

Tablica 6.15. Analiza unakrsnog opterećenja za kategoriju *Organizacijske mjere* – početno stanje

	Rotirana faktorska matrica[a]					**Kvadrat opterećenja**					
	Faktor					**Faktor**					**Omjer**
	1	2	3	4	5	1	2	3	4	5	
POL4	0,735		0,317			0,540		0,100			5,383
POL1	0,700										
POL3	0,688		0,346		0,305	0,473		0,120		0,093	3,951
POL10	0,675	0,380				0,456	0,144				3,164
POL6	0,633		0,308	0,317		0,401		0,095	0,100		4,003
POL7	0,599	0,379				0,359	0,144				2,496
POL5	0,572										
POL11	0,539			0,396		0,290			0,157		1,854
EDU16	0,529	0,499		0,394		0,280	0,249		0,155		1,125
POL8	0,527	0,321				0,278	0,103				2,706
EDU9	0,495	0,360		0,314		0,245	0,130		0,098		1,893
POL9	0,485										
EDU3		0,736									
EDU5	0,361	0,734				0,130	0,539				4,136
EDU6		0,675	0,313				0,455	0,098			4,635
EDU7		0,634	0,357				0,402	0,127			3,159
EDU2		0,569	0,337		0,354		0,324	0,114		0,125	2,584
CMP3	0,455	0,521		0,343		0,207	0,272		0,117		1,314
EDU8	0,454	0,499				0,206	0,249				1,205
EDU15	0,384	0,490	0,342	0,314		0,148	0,240	0,117	0,098		1,626
MNG5	0,386		0,735			0,149		0,540			3,616
MNG4	0,324	0,328	0,686			0,105	0,108	0,470			4,375
MNG7	0,336	0,433	0,679			0,113	0,187	0,461			2,460
MNG3			0,624								
MNG1	0,513		0,553			0,263		0,306			1,163
EDU18				0,771							
EDU19				0,710	0,331				0,504	0,110	4,593

Tablica 6.15. Analiza unakrsnog opterećenja za kategoriju *Organizacijske mjere* – početno stanje (nastavak)

	Rotirana faktorska matrica[a]					Kvadrat opterećenja					
	Faktor					Faktor					Omjer
	1	2	3	4	5	1	2	3	4	5	
EDU17	0,397	0,351		0,606		0,158	0,123		0,367		2,327
EDU14	0,338	0,359		0,533		0,114	0,129		0,284		2,204
EDU13				0,437							
CMP1		0,332		0,388	0,371		0,110		0,150	0,138	1,090
EDU11					0,611						
POL12	0,429				0,503	0,184				0,253	1,371
EDU10					0,494						
EDU1					0,456						

Metoda ekstrakcije: Principal Axis Factoring. Metoda rotacije: Varimax with Kaiser Normalization.

a. Rotacija se konvergirala u 9 iteracija.

Izvor: *vlastiti prikaz*

Uklanjanje manifestnih varijabli koje imaju izraženo unakrsno opterećenje obavljalo se na način da su takve varijable isključivane po koracima, jedna po jedna, na način da se prvo isključi manifestna varijabla čije je najveće opterećenje u pojedinom faktoru ujedno najmanje opterećenje od svih manifestnih varijabli s unakrsnim opterećenjem [324]. U prvom koraku je to bila manifestna varijabla CMP1, kako je vidljivo iz Tablice 6.15. Nakon svake isključene manifestne varijable ponovno bi se provela ista analiza. Nakon provedenih 7 koraka isključivanja pojedine manifestne varijable, u 8. koraku je dobivena matrica bez značajnog unakrsnog opterećenja te je dobiven konačni broj od 4 faktora na temelju Kaiserovog pravila te razmještaj manifestnih varijabli po faktorima (Tablica 6.16.).

Tablica 6.16. Analiza unakrsnog opterećenja za kategoriju *Organizacijske mjere* – završno stanje

	Rotirana faktorska matrica[a]				Kvadrat opterećenja				
	Faktor				Faktor				Omjer
	1	2	3	4	1	2	3	4	
POL4	**0,734**								
POL10	**0,719**	0,410			0,517	0,168			3,081
POL3	**0,698**		0,373	0,348	0,488		0,139	0,121	3,505
POL1	**0,677**		0,348		0,459		0,121		3,785
POL6	**0,654**		0,393		0,427		0,154		2,768
POL7	**0,623**	0,376			0,388	0,141			2,748
POL5	**0,611**		0,385		0,374		0,148		2,519
POL11	**0,569**		0,459		0,323		0,211		1,533

Tablica 6.16. Analiza unakrsnog opterećenja za kategoriju *Organizacijske mjere* – završno stanje (nastavak)

	Rotirana faktorska matrica[a]				**Kvadrat opterećenja**				
	Faktor				**Faktor**				**Omjer**
	1	2	3	4	1	2	3	4	
POL8	**0,554**	0,302			0,307	0,091			3,373
POL9	**0,496**								
EDU3		**0,738**							
EDU5	0,365	**0,714**			0,133	0,509			3,828
EDU6		**0,706**	0,336			0,498	0,113		4,423
EDU7		**0,636**		0,337		0,404		0,113	3,562
EDU2		**0,557**		0,316		0,310		0,100	3,107
EDU15	0,383	**0,523**			0,146	0,274			1,868
EDU19			**0,766**						
EDU18			**0,721**						
EDU17	0,387	0,375	**0,681**		0,150	0,141	0,463		3,087
EDU14	0,318	0,384	**0,550**		0,101	0,148	0,302		2,046
EDU11			**0,502**						
EDU13			**0,453**						
EDU1			**0,436**						
EDU10			**0,394**						
MNG5	0,400			**0,732**	0,160			0,536	3,344
MNG4	0,360	0,359		**0,655**	0,129	0,129		0,429	3,316
MNG7	0,351	0,471		**0,631**	0,124	0,222		0,398	1,796
MNG3	0,319	0,324		**0,602**	0,102	0,105		0,362	3,453

Metoda ekstrakcije: Principal Axis Factoring. Metoda rotacije: Varimax with Kaiser Normalization.
a. Rotacija se konvergirala u 8 iteracija.

Izvor: *vlastiti prikaz*

Na kraju je ponovno provedena paralelna analiza s promijenjenim parametrom za broj manifestnih varijabli (s početnih 37 na 28) s istim brojem sudionika (239) i brojem ponavljanja (100) koja je pokazala kako je i dalje ekstrahirani broj faktora pomoću ove metode 3 (Tablica 6.17.).

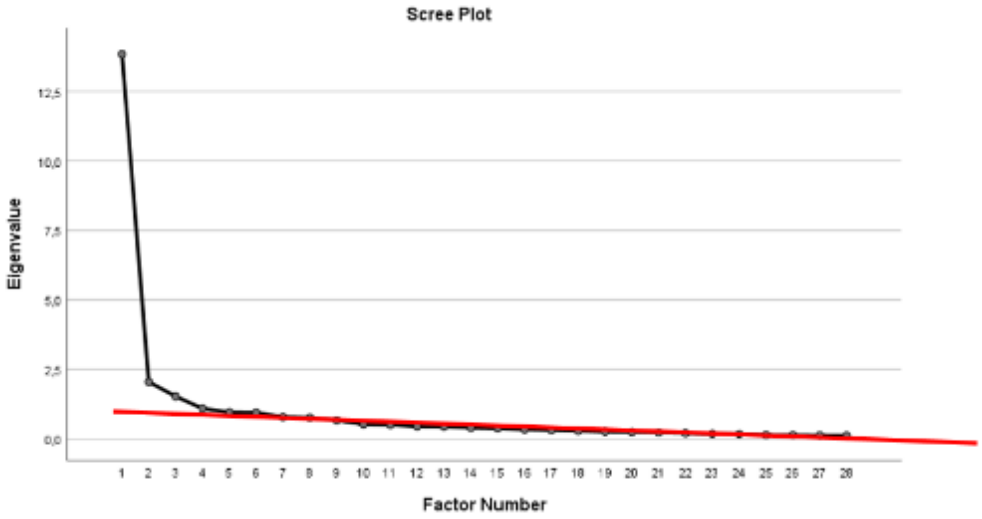
Tablica 6.17. Određivanje broja faktora za kategoriju *Organizacijske mjere* pomoću paralelne analize nakon smanjenja broja manifestnih varijabli

Paralelna analiza

Faktor	Inicijalne svojstvene vrijednosti	Slučajne svojstvene vrijednosti
1	13,841	1,691
2	2,049	1,592
3	1,526	1,512
4	1,089	1,446

Izvor: *vlastiti prikaz*

Novi Scree test (Grafikon 6.3.) pokazuje kako je moguće uzeti predloženi broj faktora 4 kao u slučaju Kaiserovog pravila.



Grafikon 6.3. Određivanje mogućeg broja faktora za kategoriju *Organizacijske mjere* putem Scree testa nakon smanjenja broja manifestnih varijabli

Izvor: *vlastiti prikaz*

Uzevši u obzir da je ukupno objašnjena varijanca putem ova 4 faktora 60,396%, kako je vidljivo u Tablici 6.18., može se zaključiti kako je zadovoljen i test kriterija postotka varijance koji pretpostavlja ukupni postotak objašnjene varijance u iznosu od barem 60% [307].

Tablica 6.18. Finalno određen broj faktora za kategoriju *Organizacijske mjere* putem vrijednosti svojstvenih faktora nakon smanjenja broja manifestnih varijabli

Faktor	Inicijalne svojstvene vrijednosti			Ekstrakcijske sume kvadriranih opterećenja			Rotacijske sume kvadriranih opterećenja		
	Ukupno	% varijance	Kumulativni %	Ukupno	% varijance	Kumulativni %	Ukupno	% varijance	Kumulativni %
1	13,841	49,431	49,431	13,494	48,193	48,193	5,582	19,935	19,935
2	2,049	7,317	56,748	1,621	5,789	53,982	4,290	15,322	35,256
3	1,526	5,449	62,197	1,163	4,152	58,134	4,141	14,789	50,045
4	1,089	3,888	66,085	0,633	2,261	60,396	2,898	10,350	60,396
5	0,954	3,406	69,490						
6	0,945	3,376	72,866						
7	0,782	2,792	75,658						
8	0,761	2,719	78,377						
9	0,664	2,370	80,746						
10	0,520	1,859	82,605						
11	0,500	1,786	84,392						
12	0,445	1,588	85,980						
13	0,439	1,566	87,546						
14	0,394	1,408	88,954						
15	0,374	1,336	90,290						
16	0,334	1,191	91,481						
17	0,311	1,112	92,593						
18	0,284	1,013	93,606						
19	0,258	0,922	94,527						
20	0,245	0,876	95,403						
21	0,224	0,799	96,202						
22	0,201	0,719	96,921						
23	0,179	0,639	97,561						
24	0,169	0,603	98,164						
25	0,140	0,501	98,665						
26	0,134	0,480	99,145						
27	0,123	0,440	99,585						
28	0,116	0,415	100,000						

Metoda ekstrakcije: Principal Axis Factoring.

Izvor: *vlastiti prikaz*

Na temelju svega navedenog, odlučeno je uzeti predložena 4 faktora za provedbu daljnje analize po pitanju unutarnje konzistentnosti.

Kao što je vidljivo iz Tablice 6.19., Cronbachov α koeficijent faktora 1 koji se sastoji od 10 manifestnih varijabli iznosi 0,941 što je znatno više od postavljenog praga u iznosu od 0,7 [306]. Isto tako, iako nije potrebno, isključivanje bilo koje od pripadnih manifestnih varijabli ne bi

doprinijelo povećanju koeficijenta, čime je potvrđena unutarnja konzistentnost prvog faktora. Cronbach-ov α koeficijent faktora 2 koji se sastoji od 6 manifestnih varijabli iznosi 0,907 što je također znatno više od postavljenog praga u iznosu od 0,7. Isto tako, iako nije potrebno, isključivanje bilo koje od pripadnih manifestnih varijabli ne bi doprinijelo povećanju koeficijenta, čime je potvrđena unutarnja konzistentnost drugog faktora. Faktor 3 sastoji se od 8 varijabli, a isključivanjem manifestne varijable EDU13 vrijednost α koeficijenta porasla bi na 0,852 no to nije potrebno iz razloga što je i trenutno njegov iznos (0,845) iznad postavljenog praga od 0,7. Time je potvrđena unutarnja konzistentnost trećeg faktora. Cronbachov α koeficijent faktora 4 koji se sastoji od 4 manifestne varijable iznosi 0,908 što je također znatno više od postavljenog praga u iznosu od 0,7. Isto tako, iako nije potrebno, isključivanje bilo koje od pripadnih manifestnih varijabli ne bi doprinijelo povećanju koeficijenta, čime je potvrđena unutarnja konzistentnost četvrtog faktora.

Tablica 6.19. Unutarnja konzistentnost faktora kategorije *Organizacijske mjere*

	Ukupna statistika ljestvice kada je čestica isključena				**Statistika pouzdanosti**
Faktor 1	**Srednja vrijednost ljestvice ako je čestica isključena**	**Varijanca ljestvice ako je čestica isključena**	**Ispravljena korelacija između čestice i rezultata ljestvice**	**Cronbachov alfa ako je čestica isključena**	**Broj čestica: 10**
					Cronbachov alfa
POL4	35,396	67,125	0,814	0,932	0,941
POL10	35,472	66,841	0,829	0,931	
POL3	35,175	67,900	0,830	0,932	
POL1	35,104	69,359	0,777	0,934	
POL6	35,552	66,339	0,809	0,932	
POL7	35,845	68,186	0,715	0,937	
POL5	35,562	68,627	0,774	0,934	
POL11	35,327	68,109	0,768	0,934	
POL8	35,734	69,940	0,635	0,941	
POL9	35,127	70,282	0,647	0,940	
Faktor 2	**Srednja vrijednost ljestvice ako je čestica isključena**	**Varijanca ljestvice ako je čestica isključena**	**Ispravljena korelacija između čestice i rezultata ljestvice**	**Cronbachov alfa ako je čestica isključena**	**Broj čestica: 6**
					Cronbachov alfa
EDU2	16,669	27,728	0,662	0,902	0,907
EDU3	17,275	24,813	0,764	0,888	
EDU5	17,085	25,119	0,810	0,881	
EDU6	16,950	25,220	0,809	0,881	
EDU7	17,221	25,694	0,742	0,891	
EDU15	16,975	25,405	0,689	0,900	

Tablica 6.19. Unutarnja konzistentnost faktora kategorije *Organizacijske mjere* (nastavak)

	Ukupna statistika ljestvice kada je čestica isključena				Statistika pouzdanosti
Faktor 3	**Srednja vrijednost ljestvice ako je čestica isključena**	**Varijanca ljestvice ako je čestica isključena**	**Ispravljena korelacija između čestice i rezultata ljestvice**	**Cronbachov alfa ako je čestica isključena**	**Broj čestica: 8**
					Cronbachov alfa
EDU19	28,768	29,132	0,737	0,810	0,845
EDU1	28,712	32,408	0,429	0,842	
EDU10	28,739	31,959	0,458	0,840	
EDU11	28,504	31,384	0,494	0,836	
EDU13	29,248	28,816	0,440	0,852	
EDU14	29,193	28,524	0,683	0,813	
EDU17	29,104	26,862	0,781	0,799	
EDU18	29,079	27,025	0,691	0,811	
Faktor 4	**Srednja vrijednost ljestvice ako je čestica isključena**	**Varijanca ljestvice ako je čestica isključena**	**Ispravljena korelacija između čestice i rezultata ljestvice**	**Cronbachov alfa ako je čestica isključena**	**Broj čestica: 4**
					Cronbachov alfa
MNG3	10,748	9,803	0,741	0,898	0,908
MNG4	10,810	9,545	0,789	0,881	
MNG5	10,534	9,558	0,816	0,872	
MNG7	10,692	9,156	0,820	0,870	

Izvor: *vlastiti prikaz*

U konačnici, izračunat je ukupni Cronbachov α koeficijent za sva četiri faktora odnosno 28 pripadajućih manifestnih varijabli koji iznosi 0,959 (Tablica 6.20.). Isključivanjem manifestne varijable EDU13 vrijednost α koeficijenta porasla bi na 0,962 što je minimalno povećanje koje bitno ne doprinosi poboljšanju budući da je i trenutno iznos α koeficijenta iznad postavljenog praga od 0,7. Time je potvrđena ukupna unutarnja konzistentnost sva 4 faktora i 28 manifestnih varijabli unutar kategorije *Organizacijske mjere*.

Tablica 6.20. Ukupna unutarnja konzistentnost kategorije *Organizacijske mjere*

Kategorija 1	Srednja vrijednost ljestvice ako je čestica isključena	Varijanca ljestvice ako je čestica isključena	Ispravljena korelacija između čestice i rezultata ljestvice	Cronbachov alfa ako je čestica isključena	Broj čestica: 28
					Cronbachov alfa
MNG3	103,599	456,901	0,655	0,958	0,959
MNG4	103,661	456,233	0,670	0,958	
MNG5	103,384	454,669	0,723	0,957	
MNG7	103,542	450,668	0,760	0,957	
POL1	102,850	456,408	0,745	0,957	
POL3	102,921	452,831	0,792	0,957	
POL4	103,142	451,871	0,759	0,957	
POL5	103,308	454,274	0,750	0,957	
POL6	103,298	449,066	0,774	0,957	
POL7	103,591	453,647	0,689	0,958	
POL8	103,480	457,783	0,620	0,958	
POL9	102,873	458,228	0,638	0,958	
POL10	103,218	450,568	0,785	0,957	
POL11	103,073	452,220	0,763	0,957	
EDU2	103,346	461,024	0,613	0,958	
EDU3	103,952	452,555	0,656	0,958	
EDU5	103,762	450,157	0,759	0,957	
EDU6	103,627	451,830	0,732	0,957	
EDU7	103,898	453,735	0,677	0,958	
EDU15	103,652	447,333	0,738	0,957	
EDU1	102,774	474,546	0,372	0,960	
EDU10	102,801	471,146	0,445	0,959	
EDU11	102,567	472,078	0,406	0,960	
EDU13	103,310	468,964	0,306	0,962	
EDU14	103,255	455,254	0,723	0,957	
EDU17	103,166	449,496	0,792	0,957	
EDU18	103,141	455,756	0,608	0,958	
EDU19	102,830	462,732	0,642	0,958	

Izvor: *vlastiti prikaz*

Nakon dobivanja konačnih faktora po pojedinoj kategoriji, potrebno ih je imenovati radi lakšeg korištenja u budućim istraživanjima te je, sukladno tome, prvi faktor iz Tablice 6.19. nazvan ***Politike i uloge***, drugi faktor ***Edukacija***, treći faktor ***Sigurnosna osviještenost***, a četvrti faktor ***Podrška rukovodstva***.

6.3.2.2. Kategorija Sociološki čimbenici

Kao i kod kategorije *Organizacijske mjere*, u prvom koraku napravljena je korelacijska matrica kako bi se identificirali parovi manifestnih varijabli koje visoko koreliraju (>0.8) te uklonila po jedna manifestna varijabla iz visokokorelirajućih parova radi smanjivanja multikolinearnosti (Tablica 6.21.).

Tablica 6.21. Korelacijska matrica za manifestne varijable iz kategorije *Sociološki čimbenici*

	BHV1	BHV2	BHV3	BHV4	BLF1	BLF2**	BLF3	BLF4**	BLF5	BLF6
BHV1	1,000	0,525	0,543	0,406	0,521	0,085	0,353	0,226	0,266	0,631
BHV2	0,525	1,000	0,526	0,706	0,421	-0,020	0,618	0,217	0,529	0,372
BHV3	0,543	0,526	1,000	0,486	0,484	0,093	0,421	0,342	0,291	0,491
BHV4	0,406	0,706	0,486	1,000	0,417	0,012	0,610	0,178	0,606	0,309
BLF1	0,521	0,421	0,484	0,417	1,000	-0,038	0,337	0,141	0,283	0,408
BLF2**	0,085	-0,020	0,093	0,012	-0,038	1,000	0,001	0,452	-0,018	0,095
BLF3	0,353	0,618	0,421	0,610	0,337	0,001	1,000	0,212	0,671	0,292
BLF4**	0,226	0,217	0,342	0,178	0,141	0,452	0,212	1,000	0,046	0,190
BLF5	0,266	0,529	0,291	0,606	0,283	-0,018	0,671	0,046	1,000	0,251
BLF6	0,631	0,372	0,491	0,309	0,408	0,095	0,292	0,190	0,251	1,000

a. Determinant = ,014

Izvor: *vlastiti prikaz*

Kao što je vidljivo iz Tablice 6.21. nije detektirana multikolinearnost putem visokokorelirajućih manifestnih varijabli kod kategorije *Sociološki čimbenici* te je svih inicijalno određenih 10 manifestnih varijabli raspoređenih u 2 čimbenika ušlo u daljnju analizu (Tablica 6.22.) odnosno provjeru jesu li dobiveni podaci pogodni za faktorsku analizu.

Tablica 6.22. Popis inicijalnih manifestnih varijabli po pojedinom čimbeniku kategorije *Sociološki čimbenici*

Čimbenik	**Varijable (čestice)**	**Broj varijabli**
Ponašanje	BHV1, BHV2, BHV3, BHV4	4
Uvjerenja	BLF1, BLF2, BLF3, BLF4, BLF5, BLF6	6

Izvor: *vlastiti prikaz*

Sukladno tome, napravljena je Kaiser-Meyer-Olkin-ova (KMO) mjera adekvatnosti uzorka i Bartlettov test sfericiteta, kao što je vidljivo u Tablici 6.23. KMO iznosi 0,835 što se smatra dobrim rezultatom, a Bartlettov test sfericiteta značajan je na razini $p < 0.001$ što znači da postoje adekvatne veze (korelacije) između varijabli uključenih u analizu te se može nastaviti s

provedbom faktorske analize jer se očekuje da promatrane manifestne varijable opisuju istu latentnu varijablu [307].

Tablica 6.23. Kaiser-Meyer-Olkin-ova (KMO) mjera adekvatnosti uzorka i Bartlettov test sfericiteta za kategoriju *Sociološki čimbenici*

KMO i Bartlettov test

Kaiser-Meyer-Olkin-ova mjera adekvatnosti uzorka		0,835
Bartlettov test sfericiteta	Pribl. Hi-kvadrat	999,998
	df	45
	Sig.	0,000

Izvor: *vlastiti prikaz*

Nakon što je napravljena provjera primjerenosti provođenja faktorske analize putem KMO mjere i Bartlettovog testa sfericiteta, napravljena je ekstrakcija faktora putem metode Principal axis factoring.

Korištenjem Kaiserovog pravila o značajnosti manifestnih varijabli koje imaju svojstvenu vrijednost (engl. *Eigenvalue*) veću od 1 predloženo je 3 faktora, kao što je vidljivo iz Tablice 6.24.

Tablica 6.24. Inicijalno određen broj faktora za kategoriju *Sociološki čimbenici* putem vrijednosti svojstvenih faktora

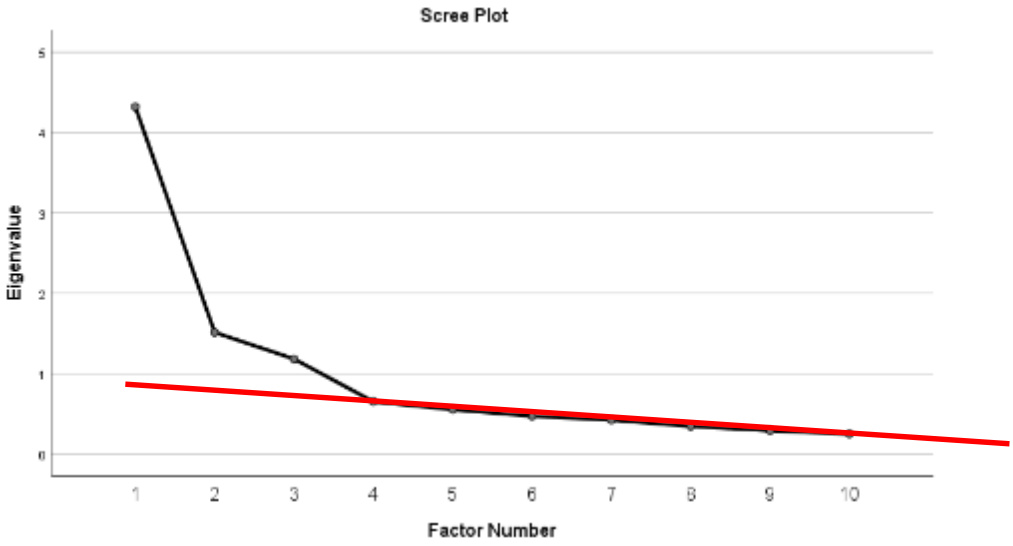
Ukupna objašnjena varijanca

Faktor	Inicijalne svojstvene vrijednosti			Ekstrakcijske sume kvadriranih opterećenja			Rotacijske sume kvadriranih opterećenja		
	Ukupno	% varijance	Kumulativni %	Ukupno	% varijance	Kumulativni %	Ukupno	% varijance	Kumulativni %
1	4,320	43,201	43,201	3,930	39,297	39,297	2,476	24,759	24,759
2	1,513	15,134	58,336	1,081	10,810	50,107	2,232	22,322	47,080
3	1,183	11,826	70,162	0,756	7,563	57,670	1,059	10,590	57,670
4	0,651	6,513	76,675						
5	0,553	5,530	82,206						
6	0,471	4,714	86,920						
7	0,423	4,232	91,152						
8	0,345	3,446	94,598						
9	0,291	2,906	97,503						
10	0,250	2,497	100,000						

Metoda ekstrakcije: Principal Axis Factoring.

Izvor: *vlastiti prikaz*

Scree test u ovoj situaciji također pokazuje, kao što je vidljivo na Grafikonu 6.4., kako bi odabir 3 faktora mogao biti ispravan.



Grafikon 6.4. Određivanje mogućeg broja faktora za kategoriju *Sociološki čimbenici* putem Scree testa

Izvor: *vlastiti prikaz*

Usporedni rezultati inicijalnih i nasumično simuliranih svojstvenih vrijednosti u svrhu određivanja broja faktora putem paralelne analize prikazani su u Tablici 6.25. iz koje je vidljivo kako su inicijalne svojstvene vrijednosti veće u prva tri para, nakon čega postaju veće nasumično simulirane svojstvene vrijednosti. Iz toga proizlazi da bi, prema kriteriju paralelne analize, broj ekstrahiranih faktora bio 3, iako je treća vrijednost granično blizu jedna drugoj.

Tablica 6.25. Određivanje broja faktora za kategoriju *Sociološki čimbenici* pomoću paralelne analize

Paralelna analiza

Faktor	Inicijalne svojstvene vrijednosti	Slučajne svojstvene vrijednosti
1	4,320	1,340
2	1,513	1,231
3	1,183	1,156
4	0,651	1,085
5	0,553	1,020
6	0,471	0,960
7	0,423	0,901
8	0,345	0,837
9	0,291	0,773
10	0,250	0,698

Izvor: *vlastiti prikaz*

Sljedeći koraci obuhvaćali su izradu tablice komunaliteta i faktorske matrice. Iz tablice komunaliteta (Tablica 6.26.) vidljivo je da su svi inicijalni komunaliteti veći od 0,2 te se sve varijable uzimaju u daljnju analizu.

Tablica 6.26. Tablica komunaliteta za kategoriju *Sociološki čimbenici*

Komunaliteti

Varijabla	Početno stanje	Ekstrakcija
POL1	0,778	0,714
POL3	0,799	0,773
POL4	0,772	0,742
POL5	0,742	0,631
POL6	0,774	0,716
POL7	0,728	0,570
POL8	0,653	0,465
POL9	0,606	0,510
POL10	0,757	0,772
POL11	0,747	0,703
POL12	0,579	0,557
MNG1	0,714	0,701
MNG2**	0,232	0,052
MNG3	0,608	0,598
MNG4	0,702	0,688
MNG5	0,795	0,815
MNG7	0,797	0,817
EDU1	0,430	0,390
EDU2	0,648	0,691

Izvor: *vlastiti prikaz*

Sljedeći korak bio je dobivanje faktorske matrice. Budući da iz faktorske matrice nije bilo moguće jednostavno interpretirati rezultate, osim da sve varijable imaju značajno faktorsko opterećenje (>= 3.0), kao što je vidljivo iz Tablice 6.27., napravljena je i rotirana faktorska matrica.

Tablica 6.27. Početna i rotirana faktorska matrica za kategoriju *Sociološki čimbenici*

	Faktorska matrica[a]				Rotirana faktorska matrica[a]		
	Faktor				Faktor		
	1	2	3		1	2	3
BHV2	0,793			BHV2	0,781		
BHV4	0,764			BHV4	0,759		
BLF3	0,723			BLF3	0,746	0,328	
BHV1	0,712		-0,393	BHV1	0,676	0,442	
BHV3	0,695			BHV3		0,820	
BLF5	0,626	-0,386		BLF5		0,679	
BLF1	0,586			BLF1	0,344	0,608	
BLF6	0,583		-0,319	BLF6		0,574	
BLF4**	0,349	0,647	0,434	BLF4**			0,828
BLF2**		0,459		BLF2**			0,542

Metoda ekstrakcije: Principal Axis Factoring.

a. Izdvojeno 6 faktora. Potrebno 18 iteracija.

Izvor: *vlastiti prikaz*

Kao što je vidljivo iz rotirane faktorske matrice sve manifestne varijable imale su značajno faktorsko opterećenje te je napravljena analiza unakrsnog opterećenja (Tablica 6.28.). Na temelju provedene analize unakrsnog opterećenja utvrđeno je kako ne postoji značajno unakrsno opterećenje čime je inicijalno postavljen broj faktora na temelju Kaiserovog pravila ujedno i konačan.

Tablica 6.28. Analiza unakrsnog opterećenja za kategoriju *Sociološki čimbenici*

	Rotirana faktorska matrica[a]			Kvadrat opterećenja			
	Faktor			Faktor			Omjer
	1	2	3	1	2	3	
BLF3	**0,781**						
BLF5	**0,759**						
BHV4	**0,746**	0,328		0,557	0,108		5,159
BHV2	**0,676**	0,442		0,457	0,195		2,340
BHV1		**0,820**					
BLF6		**0,679**					
BHV3	0,344	**0,608**		0,118	0,370		3,131
BLF1		**0,574**					
BLF4**			**0,828**			0,686	
BLF2**			**0,542**			0,294	

Metoda ekstrakcije: Principal Axis Factoring. Metoda rotacije: Varimax with Kaiser Normalization.

a. Rotacija se konvergirala u 4 iteracije. **obrnuto formulirane čestice

Izvor: *vlastiti prikaz*

Budući da nijedna manifestna varijabla nije isključena iz provedene analize, nije bilo potrebe ponovno provoditi analizu sa smanjenim brojem manifestnih varijabli već je moguće uzeti inicijalne vrijednosti kao konačne. Rezultati testa Kaiserovog pravila, Scree testa i paralelnog testa svi pokazali kako bi ekstrahirani broj faktora bio 3, a ukupno objašnjena varijanca putem ova 3 faktora iznosi 57,67%, što je dovoljno blizu predviđenoj granici od 60% objašnjene varijance za test postotka varijance. Međutim, uzimajući u obzir općeprihvaćeno pravilo da bi se pojedini faktor treba sastojati od minimalno tri manifestne varijable [319], [321], [323], [331], [332], odlučeno je kako će se isključiti faktor 3 koji se sastoji od samo dvije manifestne varijable, nakon čega je ponovljen postupak određivanja broja faktora putem svojstvenih vrijednosti (Tablica 6.29.), računanje komunaliteta, faktorske matrice i rotirane faktorske matrice te analiza unakrsnog opterećenja (Tablica 6.30.).

Tablica 6.29. Određivanje broja faktora nakon uklanjanja jednog faktora s dvije manifestne varijable

Ukupna objašnjena varijanca

Faktor	Inicijalne svojstvene vrijednosti			Ekstrakcijske sume kvadriranih opterećenja			Rotacijske sume kvadriranih opterećenja		
	Ukupno	% varijance	Kumulativni %	Ukupno	% varijance	Kumulativni %	Ukupno	% varijance	Kumulativni %
1	4,221	52,759	52,759	3,823	47,784	47,784	2,439	30,487	30,487
2	1,277	15,966	68,724	0,877	10,959	58,743	2,260	28,255	58,743
3	0,613	7,659	76,384						
4	0,535	6,693	83,076						
5	0,444	5,547	88,623						
6	0,359	4,491	93,114						
7	0,299	3,739	96,853						
8	0,252	3,147	100,000						

Metoda ekstrakcije: Principal Axis Factoring.

Izvor: *vlastiti prikaz*

Kao što je vidljivo iz Tablice 6.30., oba ekstrahirana faktora sastoje se od četiri manifestne varijable te je odlučeno uzeti predložena dva faktora za provedbu daljnje analize po pitanju unutarnje konzistentnosti.

Tablica 6.30. Analiza unakrsnog opterećenja za kategoriju *Sociološki čimbenici* – završno stanje

	Rotirana faktorska matrica[a]		Kvadrat opterećenja		
	Faktor		Faktor		Omjer
	1	2	1	2	
BLF3	**0,776**				
BLF5	**0,760**				
BHV4	**0,746**	0,336	0,557	0,113	4,944
BHV2	**0,672**	0,450	0,451	0,203	2,227
BHV1		**0,825**			
BLF6		**0,690**			
BHV3	0,339	**0,628**	0,115	0,395	3,446
BLF1		**0,566**			

Metoda ekstrakcije: Principal Axis Factoring. Metoda rotacije: Varimax with Kaiser Normalization.
a. Rotacija se konvergirala u 3 iteracije.

Izvor: *vlastiti prikaz*

Kao što je vidljivo iz Tablice 6.31., Cronbach-ov α koeficijent faktora 1 koji se sastoji od 4 manifestne varijable iznosi 0,869 što je iznad postavljenog praga u iznosu od 0,7 [306]. Isto tako, isključivanje bilo koje od pripadnih manifestnih varijabli ne bi doprinijelo povećanju koeficijenta, čime je potvrđena unutarnja konzistentnost prvog faktora. Nadalje, Cronbachov α koeficijent faktora 2 koji se također sastoji od 4 manifestne varijable iznosi 0,799 što je više od postavljenog praga u iznosu od 0,7, a isključivanje bilo koje od pripadnih manifestnih varijabli ne bi doprinijelo povećanju koeficijenta, čime je potvrđena unutarnja konzistentnost drugog faktora.

Tablica 6.31. Unutarnja konzistentnost faktora kategorije *Sociološki čimbenici*

	Ukupna statistika ljestvice kada je čestica isključena			Statistika pouzdanosti	
Faktor 1	Srednja vrijednost ljestvice ako je čestica isključena	Varijanca ljestvice ako je čestica isključena	Ispravljena korelacija između čestice i rezultata ljestvice	Cronbachov alfa ako je čestica isključena	Broj čestica: 4 Cronbachov alfa
BHV2	10,594	8,917	0,712	0,555	0,869
BHV4	10,899	8,589	0,745	0,583	
BLF3	11,001	8,543	0,735	0,556	
BLF5	11,249	8,921	0,690	0,512	

Tablica 6.31. Unutarnja konzistentnost faktora kategorije *Sociološki čimbenici* (nastavak)

	Ukupna statistika ljestvice kada je čestica isključena				Statistika pouzdanosti	
Faktor 2	**Srednja vrijednost ljestvice ako je čestica isključena**	**Varijanca ljestvice ako je čestica isključena**	**Ispravljena korelacija između čestice i rezultata ljestvice**	**Cronbachov alfa ako je čestica isključena**	**Broj čestica: 4**	**Cronbachov alfa**
BHV1	12,478	5,786	0,698	0,513	0,799	
BLF6	12,505	6,081	0,609	0,432		
BHV3	13,001	5,146	0,613	0,377		
BLF1	13,157	5,422	0,564	0,331		

Izvor: *vlastiti prikaz*

U konačnici, izračunat je ukupni Cronbachov α koeficijent za sva tri faktora odnosno 8 pripadajućih manifestnih varijabli te iznosi 0,870 (Tablica 6.32.). Isključivanjem bilo koje manifestne varijable vrijednost α koeficijenta ne bi porasla. Ovime je potvrđena ukupna interna konzistentnost oba faktora i 8 manifestnih varijabli unutar kategorije *Sociološki čimbenici*.

Tablica 6.32. Ukupna unutarnja konzistentnost kategorije *Sociološki čimbenici*

Kategorija 2	**Srednja vrijednost ljestvice ako je čestica isključena**	**Varijanca ljestvice ako je čestica isključena**	**Ispravljena korelacija između čestice i rezultata ljestvice**	**Cronbachov alfa ako je čestica isključena**	**Broj čestica: 8**	**Cronbachov alfa**
BHV1	27,059	30,822	0,620	0,549	0,870	
BHV2	27,641	27,430	0,746	0,615		
BHV3	27,582	28,908	0,623	0,454		
BHV4	27,946	27,457	0,718	0,602		
BLF1	27,739	29,913	0,543	0,355		
BLF3	28,049	27,849	0,665	0,564		
BLF5	28,296	28,999	0,579	0,522		
BLF6	27,086	31,739	0,514	0,437		

Izvor: *vlastiti prikaz*

Nakon dobivanja konačnih faktora po pojedinoj kategoriji, radi lakšeg korištenja u budućim istraživanjima, prvi faktor iz Tablice 6.31. nazvan je ***Uvjerenja***, a drugi faktor ***Ponašanje***.

6.3.2.3. Kategorija Tehničke mjere

Kao i kod preostale dvije kategorije, u prvom koraku napravljena je korelacijska matrica (Tablica 6.33.) kako bi se identificirali parovi manifestnih varijabli koje visoko koreliraju (>0.8) te uklonila po jedna manifestna varijabla iz visokokorelirajućih parova radi smanjivanja multikolinearnosti.

Tablica 6.33. Korelacijska matrica za manifestnih varijabli iz kategorije *Tehničke mjere*

	AV1	AV2	AV3	AV4	AV5	BCK1	BCK2	BCK3
AV1	1,000	0,747	0,527	0,346	0,325	0,461	0,383	0,358
AV2	0,747	1,000	0,640	0,460	0,405	0,534	0,403	0,387
AV3	0,527	0,640	1,000	0,641	0,601	0,516	0,539	0,587
AV4	0,346	0,460	0,641	1,000	0,893	0,367	0,404	0,536
AV5	0,325	0,405	0,601	0,893	1,000	0,355	0,461	0,536
BCK1	0,461	0,534	0,516	0,367	0,355	1,000	0,587	0,590
BCK2	0,383	0,403	0,539	0,404	0,461	0,587	1,000	0,713
BCK3	0,358	0,387	0,587	0,536	0,536	0,590	0,713	1,000
BCK4	0,383	0,491	0,322	0,187	0,175	0,559	0,330	0,379
AA1	0,195	0,309	0,528	0,604	0,494	0,265	0,359	0,454
AA2	0,305	0,327	0,296	0,475	0,465	0,283	0,286	0,337
AA3	0,306	0,383	0,271	0,193	0,162	0,360	0,182	0,156
AA4	0,253	0,321	0,477	0,499	0,487	0,299	0,376	0,461
AA5	0,360	0,476	0,436	0,434	0,419	0,489	0,354	0,484
AA6	0,316	0,432	0,573	0,560	0,515	0,421	0,487	0,603

	BCK4	AA1	AA2	AA3	AA4	AA5	AA6
AV1	0,383	0,195	0,305	0,306	0,253	0,360	0,316
AV2	0,491	0,309	0,327	0,383	0,321	0,476	0,432
AV3	0,322	0,528	0,296	0,271	0,477	0,436	0,573
AV4	0,187	0,604	0,475	0,193	0,499	0,434	0,560
AV5	0,175	0,494	0,465	0,162	0,487	0,419	0,515
BCK1	0,559	0,265	0,283	0,360	0,299	0,489	0,421
BCK2	0,330	0,359	0,286	0,182	0,376	0,354	0,487
BCK3	0,379	0,454	0,337	0,156	0,461	0,484	0,603
BCK4	1,000	0,178	0,250	0,290	0,227	0,420	0,299
AA1	0,178	1,000	0,397	0,149	0,502	0,338	0,557
AA2	0,250	0,397	1,000	0,293	0,570	0,460	0,438
AA3	0,290	0,149	0,293	1,000	0,349	0,387	0,313
AA4	0,227	0,502	0,570	0,349	1,000	0,595	0,658
AA5	0,420	0,338	0,460	0,387	0,595	1,000	0,583
AA6	0,299	0,557	0,438	0,313	0,658	0,583	1,000

a. Determinant = 6,475E-5

Izvor: *vlastiti prikaz*

Kategorija *Tehničke mjere* inicijalno se sastojala od 15 manifestnih varijabli raspoređenih u 3 čimbenika kako je vidljivo iz Tablice 6.34., a zbog visoke korelacije između manifestnih varijabli AV4 - *Antivirusni sustav neophodan je za moju organizaciju* i AV5 - *Implementacija antivirusne zaštite neophodna je za svaku organizaciju koja u svom poslovanju koristi informacijske sustave*, isključena je manifestna varijabla AV4 koja je u Tablici 6.34. naznačena crvenom bojom. Obrazloženje isključivanja manifestne varijable AV4 leži u činjenici da, ako stoji tvrdnja da je antivirusna zaštita neophodna za sve organizacije koje koriste informacijske sustave, onda je neophodna i za promatranu organizaciju.

Tablica 6.34. Popis inicijalnih manifestnih varijabli po pojedinom čimbeniku kategorije *Tehničke mjere*

Čimbenik	**Varijable (čestice)**	**Broj varijabli**
Antivirusna zaštita	AV1, AV2, AV3, AV4, AV5	5 (4)
Sigurnosna kopija	BCK1, BCK2, BCK3, BCK4	4
Autentikacija i autorizacija	AA1, AA2, AA3, AA4, AA5, AA6	6

Izvor: *vlastiti prikaz*

Kako bi se provjerilo jesu li dobiveni podaci pogodni za faktorsku analizu, napravljena je Kaiser-Meyer-Olkin-ova (KMO) mjera adekvatnosti uzorka i Bartlettov test sfericiteta i za kategoriju *Tehničke mjere*. Kao što je vidljivo u Tablici 6.35., KMO iznosi 0,892 što se smatra dobrim rezultatom, a Bartlettov test sfericiteta značajan je na razini $p < 0.001$ što znači da postoje adekvatne veze (korelacije) između manifestnih varijabli uključenih u analizu te se može nastaviti s provedbom faktorske analize jer se očekuje da promatrane manifestne varijable opisuju istu latentnu varijablu [307].

Tablica 6.35. Kaiser-Meyer-Olkin-ova (KMO) mjera adekvatnosti uzorka i Bartlettov test sfericiteta za kategoriju *Tehničke mjere*

KMO i Bartlettov test

Kaiser-Meyer-Olkin-ova mjera adekvatnosti uzorka		0,892
Bartlettov test sfericiteta	Pribl. Hi-kvadrat	1799,555
	df	91
	Sig.	0,000

Izvor: *vlastiti prikaz*

Nakon što je isključena jedna manifestna varijabla koja visoko korelira s drugom i provedena provjera primjerenosti provođenja faktorske analize putem KMO mjere i Bartlettovog testa sfericiteta, napravljena je ekstrakcija faktora putem metode Principal axis factoring. Korištenjem Kaiserovog pravila o značajnosti manifestnih varijabli koje imaju svojstvenu vrijednost (engl. *Eigenvalue*) veću od 1 predloženo je 3 faktora, kao što je vidljivo iz Tablice 6.36.

Tablica 6.36. Inicijalno određen broj faktora za kategoriju *Tehničke mjere* putem vrijednosti svojstvenih faktora

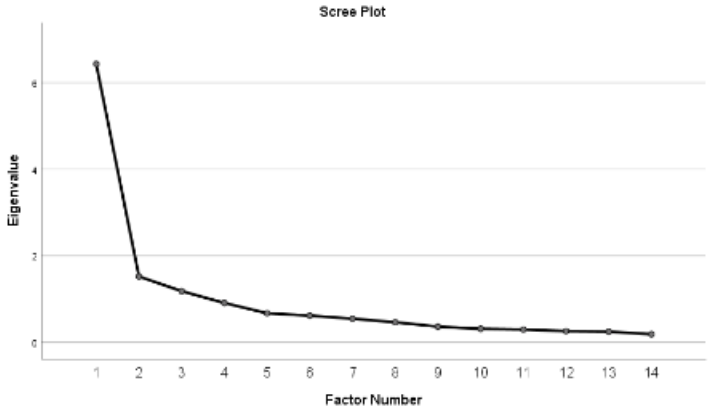
Ukupna objašnjena varijanca

Faktor	Inicijalne svojstvene vrijednosti			Ekstrakcijske sume kvadriranih opterećenja			Rotacijske sume kvadriranih opterećenja		
	Ukupno	% varijance	Kumulativni %	Ukupno	% varijance	Kumulativni %	Ukupno	% varijance	Kumulativni %
1	6,431	45,938	45,938	6,025	43,033	43,033	2,774	19,813	19,813
2	1,521	10,866	56,804	1,094	7,815	50,848	2,620	18,713	38,526
3	1,182	8,445	65,249	0,743	5,308	56,155	2,468	17,629	56,155
4	0,909	6,492	71,741						
5	0,672	4,798	76,539						
6	0,616	4,400	80,939						
7	0,545	3,896	84,835						
8	0,463	3,308	88,143						
9	0,361	2,582	90,725						
10	0,312	2,226	92,950						
11	0,295	2,109	95,059						
12	0,259	1,848	96,907						
13	0,246	1,755	98,662						
14	0,187	1,338	100,000						

Metoda ekstrakcije: Principal Axis Factoring.

Izvor: *vlastiti prikaz*

Scree test je prikazan na Grafikonu 6.5. iz kojeg je vidljivo kako na temelju ovog testa možemo razmatrati o ekstrakciji 2, 3 ili 4 faktora.



Grafikon 6.5. Određivanje mogućeg broja faktora za kategoriju *Tehničke mjere* Scree testom

Izvor: *vlastiti prikaz*

Usporedni rezultati inicijalnih i nasumično simuliranih svojstvenih vrijednosti u svrhu određivanja broja faktora putem paralelne analize prikazani su u Tablici 6.37. iz koje je vidljivo kako su inicijalne svojstvene vrijednosti veće u prva dva para, nakon čega postaju veće nasumično simulirane svojstvene vrijednosti. Iz toga proizlazi da bi, prema kriteriju paralelne analize, broj ekstrahiranih faktora bio 2.

Tablica 6.37. Određivanje broja faktora za kategoriju *Tehničke mjere* pomoću paralelne analize

Paralelna analiza

Faktor	Inicijalne svojstvene vrijednosti	Slučajne svojstvene vrijednosti
1	6,977	1,429
2	1,652	1,324
3	1,198	1,245
4	0,992	1,178
5	0,677	1,119

Izvor: *vlastiti prikaz*

Budući da se broj faktora koji najbolje opisuju odnos između manifestnih varijabli razlikuje na temelju rezultata Kaiser-ovog testa (3 faktora) i testa paralelne analize (2 faktora), a Scree test ne prikazuje jednoznačno rješenje, potrebno je izvršiti daljnju analizu kako bi se u konačnici odredio optimalan broj faktora koji najbolje opisuju odnos između manifestnih varijabli u kategoriji *Tehničke mjere*.

Sljedeći koraci obuhvaćali su izradu tablice komunaliteta i faktorske matrice. Iz tablice komunaliteta (Tablica 6.38.) vidljivo je da su svi inicijalni komunaliteti veći od 0,2 te se sve manifestne varijable uzimaju u daljnju analizu.

Tablica 6.38. Tablica komunaliteta za kategoriju *Tehničke mjere*

Komunaliteti

Varijabla	Početno stanje	Ekstrakcija
AV1	0,584	0,552
AV2	0,702	0,755
AV3	0,662	0,604
AV5	0,509	0,489
BCK1	0,587	0,594
BCK2	0,574	0,625
BCK3	0,666	0,773
BCK4	0,402	0,366
AA1	0,443	0,439
AA2	0,439	0,427
AA3	0,284	0,301
AA4	0,608	0,753
AA5	0,544	0,535
AA6	0,615	0,650

Izvor: *vlastiti prikaz*

Sljedeći korak bio je dobivanje faktorske matrice. Budući da iz faktorske matrice nije bilo moguće jednostavno interpretirati rezultate, osim da sve manifestne varijable imaju značajno faktorsko opterećenje (>= 3.0), kao što je vidljivo iz Tablice 6.39., napravljena je i rotirana faktorska matrica.

Kao što je vidljivo iz rotirane faktorske matrice sve manifestne varijable imale su značajno faktorsko opterećenje te je napravljena analiza unakrsnog opterećenja. Iz rezultata prikazanih u Tablici 6.40. vidljivo je kako su varijable AV5 i BCK1, prema kriterijima koje su definirali Hair i suradnici [322], dobri kandidati za uklanjanje iz daljnje analize.

Tablica 6.39. Početna i rotirana faktorska matrica za kategoriju *Tehničke mjere*

	Faktorska matrica[a]				Rotirana faktorska matrica[b]		
	Faktor				Faktor		
	1	2	3		1	2	3
AV3	0,766			AA4	0,831		
BCK3	0,763		-0,429	AA6	0,646		0,426
AA6	0,757			AA2	0,598		
AV2	0,719	0,453		AA5	0,556	0,427	
AA4	0,694	-0,441		AA1	0,531		0,391
AA5	0,692			AV5	0,493		0,466
BCK1	0,690	0,313		AV2		0,807	
BCK2	0,679		-0,402	AV1		0,696	
AV5	0,656			BCK1		0,579	0,488
AV1	0,598	0,426		BCK4		0,549	
AA1	0,576	-0,323		AA3	0,318	0,446	
AA2	0,557			BCK3	0,312		0,792
BCK4	0,509	0,322		BCK2			0,715

Metoda ekstrakcije: Principal Axis Factoring.
a. Izdvojeno 3 faktora. Potrebno 10 iteracija.

Metoda rotacije: Varimax with Kaiser Normalization.
Metoda ektrakcije: Principal Axis Factoring.
b. Rotacija se konvergirala u 8 iteracija.

Izvor: *vlastiti prikaz*

Tablica 6.40. Analiza unakrsnog opterećenja za kategoriju *Tehničke mjere* – početno stanje

	Rotirana faktorska matrica[a]			Kvadrat opterećenja			
	Faktor			Faktor			Omjer
	1	2	3	1	2	3	
AA4	0,831						
AA6	0,646		0,426	0,417		0,181	2,304
AA2	0,598						
AA5	0,556	0,427		0,310	0,182		1,698
AA1	0,531		0,391	0,282		0,153	1,848
AV5	0,493		0,466	0,243		0,217	1,117
AV2		0,807					
AV1		0,696					
BCK1		0,579	0,488		0,335	0,238	1,408
BCK4		0,549					
AA3	0,318	0,446		0,101	0,199		1,961
BCK3	0,312		0,792	0,097		0,627	6,438
BCK2			0,715				
AV3	0,371	0,424	0,535	0,138	0,180	0,286	1,591

Metoda ekstrakcije: Principal Axis Factoring. Rotation Method: Varimax with Kaiser Normalization.
a. Rotacija se konvergirala u 8 iteracija.

Izvor: *vlastiti prikaz*

Uklanjanje manifestnih varijabli koje imaju izraženo unakrsno opterećenje obavljalo se na način da su takve manifestne varijable isključivane po koracima, jedna po jedna, na način da se prvo isključi manifestna varijabla čije je najveće opterećenje u pojedinom faktoru ujedno najmanje opterećenje od svih manifestnih varijabli s unakrsnim opterećenjem [324]. U prvom koraku je to bila manifestna varijabla AV5, kako je vidljivo iz Tablice 6.40. Nakon svake isključene manifestne varijable ponovno bi se provela ista analiza. Nakon provedena 4 koraka isključivanja pojedine manifestne varijable, u 5. koraku je dobivena matrica bez značajnog unakrsnog opterećenja te je dobiven konačni broj od 2 faktora (za razliku od početna 3) na temelju Kaiserovog pravila te razmještaj manifestnih varijabli po faktorima (Tablica 6.41.).

Tablica 6.41. Analiza unakrsnog opterećenja za kategoriju *Tehničke mjere* – završno stanje

	Rotirana faktorska matrica[a]			**Kvadrat opterećenja**			
	Faktor			**Faktor**			**Omjer**
	1	2	3	1	2	3	
AA4	**0,793**				AA4	0,793	
AA6	**0,792**				AA6	0,792	
BCK3	**0,633**	0,357	0,401	0,128	BCK3	0,633	3,140
AA1	**0,616**				AA1	0,616	
AA5	**0,601**	0,369	0,362	0,136	AA5	0,601	2,653
AA2	**0,551**				AA2	0,551	
BCK2	**0,501**	0,383	0,251	0,146	BCK2	0,501	1,713
AV2		**0,861**			AV2		
AV1		**0,783**			AV1		
BCK4		**0,496**			BCK4		

Metoda ekstrakcije: Principal Axis Factoring. Rotation Method: Varimax with Kaiser Normalization.

a. Rotacija se konvergirala u 3 iteracije.

Izvor: *vlastiti prikaz*

Na kraju je ponovno provedena paralelna analiza s promijenjenim parametrom za broj manifestnih varijabli (s početnih 14 na 10) s istim brojem sudionika (239) i brojem ponavljanja (100) koja je pokazala kako je i dalje ekstrahirani broj faktora pomoću ove metode 2 (Tablica 6.42.).

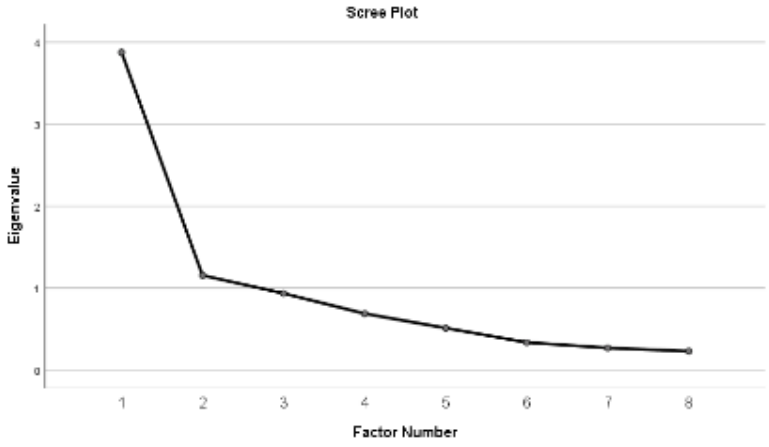
Tablica 6.42. Određivanje broja faktora za kategoriju *Tehničke mjere* pomoću paralelne analize nakon smanjenja broja manifestnih varijabli

Paralelna analiza

Faktor	Inicijalne svojstvene vrijednosti	Slučajne svojstvene vrijednosti
1	4,755	1,337
2	1,335	1,232
3	0,942	1,153
4	0,716	1,082
5	0,586	1,017

Izvor: *vlastiti prikaz*

Novi Scree test (Grafikon 6.6.) pokazuje kako je moguće uzeti 2 ili 3 faktora za konačni odabir.



Grafikon 6.6. Određivanje mogućeg broja faktora za kategoriju *Tehničke mjere* putem Scree testa nakon smanjenja broja manifestnih varijabli

Izvor: *vlastiti prikaz*

Ukupno objašnjena varijanca za 2 faktora iznosi 52,595%, kako je vidljivo u Tablici 6.43., što je niže od ciljanih 60%, no Hair [322] napominje kako je za društvene znanosti prihvatljiv čak i postotak manji od 60% ukupne varijance.

Tablica 6.43. Finalno određen broj faktora za kategoriju *Tehničke mjere* putem vrijednosti svojstvenih faktora nakon smanjenja broja manifestnih varijabli

Ukupna objašnjena varijanca

Faktor	Inicijalne svojstvene vrijednosti			Ekstrakcijske sume kvadriranih opterećenja			Rotacijske sume kvadriranih opterećenja		
	Ukupno	% varijance	Kumulativni %	Ukupno	% varijance	Kumulativni %	Ukupno	% varijance	Kumulativni %
1	4,755	47,555	47,555	4,305	43,051	43,051	3,104	31,037	31,037
2	1,335	13,353	60,907	0,954	9,545	52,595	2,156	21,559	52,595
3	0,942	9,418	70,326						
4	0,716	7,159	77,484						
5	0,586	5,862	83,347						
6	0,555	5,548	88,894						
7	0,340	3,396	92,290						
8	0,299	2,993	95,283						
9	0,265	2,646	97,930						
10	0,207	2,070	100,000						

Metoda ekstrakcije: Principal Axis Factoring.

Izvor: *vlastiti prikaz*

Uzevši u obzir da je određivanje mogućeg broja faktora putem svojstvenih vrijednosti, Scree testa i paralelnog testa, odlučeno je uzeti 2 faktora za provedbu daljnje analize po pitanju unutarnje konzistentnosti.

Kao što je vidljivo iz Tablice 6.44., Cronbachov α koeficijent faktora 1 koji se sastoji od 10 manifestnih varijabli iznosi 0,941 što je znatno više od postavljenog praga u iznosu od 0,7 [306]. Isto tako, iako nije potrebno, isključivanje bilo koje od pripadnih manifestnih varijabli ne bi doprinijelo povećanju koeficijenta, čime je potvrđena unutarnja konzistentnost prvog faktora.

Cronbachov α koeficijent faktora 2 koji se sastoji od 6 manifestnih varijabli iznosi 0,907 što je također znatno više od postavljenog praga u iznosu od 0,7. Isto tako, iako nije potrebno, isključivanje bilo koje od pripadnih manifestnih varijabli ne bi doprinijelo povećanju koeficijenta, čime je potvrđena unutarnja konzistentnost drugog faktora.

Faktor 3 sastoji se od 8 manifestnih varijabli, a isključivanjem manifestne varijable EDU13 vrijednost α koeficijenta porasla bi na 0,852 no to nije potrebno iz razloga što je i trenutno njegov iznos (0,845) iznad postavljenog praga od 0,7. Time je potvrđena unutarnja konzistentnost trećeg faktora.

Cronbachov α koeficijent faktora 4 koji se sastoji od 4 manifestne varijable iznosi 0,908 što je također znatno više od postavljenog praga u iznosu od 0,7. Isto tako, iako nije potrebno, isključivanje bilo koje od pripadnih manifestnih varijabli ne bi doprinijelo povećanju koeficijenta, čime je potvrđena unutarnja konzistentnost četvrtog faktora.

Tablica 6.44. Unutarnja konzistentnost faktora kategorije *Tehničke mjere*

	Ukupna statistika ljestvice kada je čestica isključena				**Statistika pouzdanosti**
Faktor 1	**Srednja vrijednost ljestvice ako je čestica isključena**	**Varijanca ljestvice ako je čestica isključena**	**Ispravljena korelacija između čestice i rezultata ljestvice**	**Cronbachov alfa ako je čestica isključena**	**Broj čestica: 7** **Cronbachov alfa**
BCK2	27,831	13,585	0,559	0,516	0,861
BCK3	27,641	13,770	0,693	0,615	
AA1	27,534	14,846	0,566	0,377	
AA2	27,601	14,366	0,541	0,363	
AA4	27,576	13,494	0,710	0,576	
AA5	27,741	13,224	0,623	0,459	
AA6	27,699	13,284	0,753	0,602	
Faktor 2	**Srednja vrijednost ljestvice ako je čestica isključena**	**Varijanca ljestvice ako je čestica isključena**	**Ispravljena korelacija između čestice i rezultata ljestvice**	**Cronbachov alfa ako je čestica isključena**	**Broj čestica: 3** **Cronbachov alfa**
AV1	8,289	3,607	0,728	0,607	0,758
AV2	8,565	3,381	0,465	0,241	
BCK4	8,523	3,588	0,622	0,558	

Izvor: *vlastiti prikaz*

U konačnici, izračunat je ukupni Cronbachov α koeficijent za oba faktora odnosno 10 pripadajućih manifestnih varijabli koji iznosi 0,866 (Tablica 6.45.). Isključivanjem bilo koje od preostalih manifestnih varijabli vrijednost α koeficijenta ne bi rasla u odnosu na trenutno stanje. Time je potvrđena ukupna unutarnja konzistentnost oba faktora i 10 manifestnih varijabli unutar kategorije *Tehničke mjere*.

Tablica 6.45. Ukupna unutarnja konzistentnost kategorije *Tehničke mjere*

Kategorija 3	Srednja vrijednost ljestvice ako je čestica isključena	Varijanca ljestvice ako je čestica isključena	Ispravljena korelacija između čestice i rezultata ljestvice	Cronbachov alfa ako je čestica isključena	Broj čestica: 10
					Cronbachov alfa
AV1	40,793	30,458	0,543	0,578	0,866
AV2	40,560	30,073	0,655	0,651	
BCK2	40,520	30,689	0,586	0,537	
BCK3	40,329	31,239	0,676	0,624	
BCK4	40,836	29,624	0,478	0,317	
AA1	40,223	33,193	0,503	0,388	
AA2	40,290	32,189	0,526	0,379	
AA4	40,265	31,467	0,616	0,584	
AA5	40,430	30,043	0,658	0,522	
AA6	40,388	30,842	0,693	0,609	

Izvor: *vlastiti prikaz*

Nakon dobivanja konačnih faktora, radi lakšeg korištenja u budućim istraživanjima, prvi faktor iz Tablice 6.44. nazvan je ***Očuvanje povjerljivosti i dostupnosti***, a drugi faktor ***Očuvanje integriteta***.

6.4. Okvir i rezultati analize prikupljenih podataka

Nakon prikupljanja podataka putem empirijskog istraživanja i provedbe faktorske analize nad dobivenim podacima kojom se provjerila valjanost i pouzdanost mjernog instrumenta koji čini temelj za okvir za procjenu i unapređenje kulture informacijske sigurnosti, u ovoj završnoj fazi napravljena je deskriptivna statistička analiza prikupljenih podataka te provedba analize povezanosti kulture informacijske sigurnosti s primjenom implementiranih mjera informacijske sigurnosti u organizaciji u svrhu konačne validacije predloženog konceptualnog okvira.

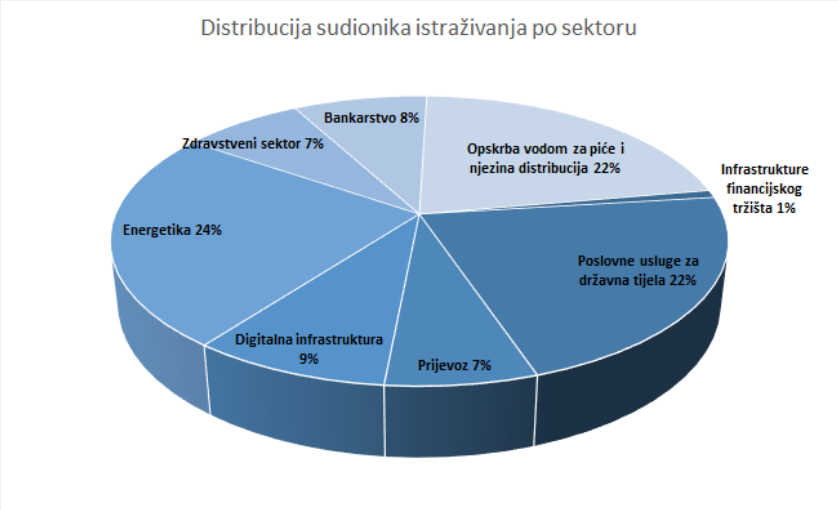
6.4.1. Deskriptivna statistička analiza

Analiza prikupljenih podataka vezanih uz obilježja sudionika provedena je mjerama deskriptivne statistike uključujući frekvenciju obilježja i proporciju, dok su sumarni opisi distribucija kvantitativnih varijabli vezani uz čimbenike kulture informacijske sigurnosti i stvarno stanje implementiranih mjera dobre sigurnosne prakse analizirani putem frekvencije obilježja, proporcije, aritmetičke sredine i standardne devijacije.

6.4.1.1. Sudionici istraživanja

Kao što je već ranije rečeno, u prikupljanju podataka putem online upitnika koje je trajalo u periodu od 01.11.2019. do 31.01.2020. godine sudjelovalo je ukupno 506 sudionika, od čega je 240 sudionika u potpunosti ispunilo upitnik, a 266 djelomično. Naknadnim uvidom u upitnike koji su bili u potpunosti ispunjeni utvrđeno je kako je kod jednog sudionika u svim odgovorima bila odabrana opcija „nije primjenjivo" te je taj upitnik isključen iz daljnje analize za koju se koristio preostali set od 239 ispunjenih upitnika.

Od ukupnog broja sudionika, 123 (51%) ih je bilo ženskog spola dok ih je 116 (49%) bilo muškog spola. Kao što je vidljivo iz Grafikona 6.7. najviše sudionika bilo je iz sektora energetike (24%), sektora opskrbe vodom za piće njezine distribucije (22%) te sektora poslovnih usluga za državna tijela (22%), a najmanje (svega 1%) iz sektora infrastrukture financijskog tržišta.



Grafikon 6.7. Distribucija sudionika empirijskog istraživanja po sektoru
(Izvor: *vlastiti prikaz*)

Što se tiče dobi sudionika, velika većina sudionika (154 odnosno 64,4%) nalazi se u rasponu od 30 do 49 godina, dok je svega 1 sudionik (0,4%) mlađi od 25 godina. Prema stupnju obrazovanja, najviše sudionika ima završen diplomski studij (diplomski sveučilišni studij ili specijalistički diplomski stručni studij), njih 157 (67,7%), dok je najmanje sudionika (5 odnosno 2,1%) imalo završenu gimnaziju. Nijedan sudionik nije imao završenu samo osnovnu školu ili trogodišnju srednju strukovnu školu za industrijska, obrtnička i zanatska zanimanja dok je 13,4% sudionika steklo neki oblik poslijediplomskog obrazovanja. Po pitanju ukupnog radnog iskustva, najveći broj ispitanika (80 odnosno 33,5%) imao je 10 do 20 godina radnog

staža, dok su svega 3 sudionika (1,2%) imala manje od dvije godine radnog staža. Što se tiče radnog iskustva u trenutnoj organizaciji, također je najveći broj sudionika (67 odnosno 28%) proveo između 10 i 20 godina u trenutnoj organizaciji, dok je njih 13 (5,4%) tamo kraće od godine dana. Tablica 6.46. prikazuje demografske karakteristike sudionika empirijskog istraživanja.

Tablica 6.46. Demografske karakteristike sudionika empirijskog istraživanja

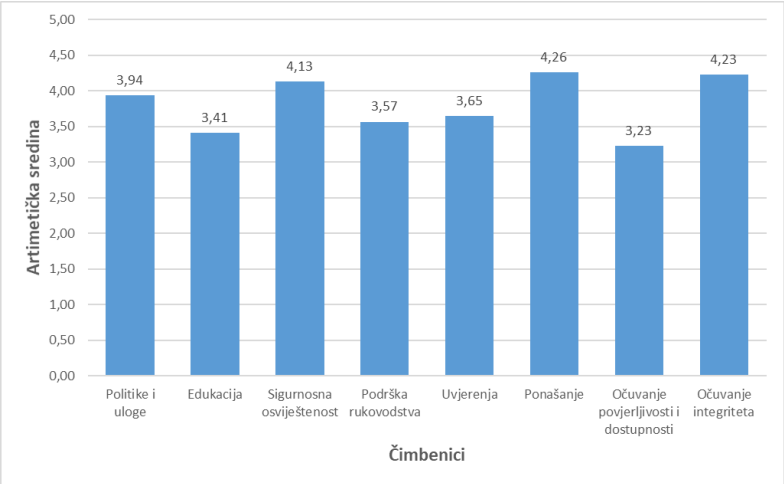
Dob	**N**	**%**	**Stupanj obrazovanja**	**N**	**%**
15-19	0	0,0%	Osnovna škola	0	0,0%
20-24	1	0,4%	Trogodišnja srednja strukovna škola (za industrijska, obrtnička, zanatska zanimanja) (SSS)	0	0,0%
25-29	17	7,1%	Četverogodišnja srednja strukovna škola (npr. tehnička, ekonomska, medicinska) (SSS)	17	7,1%
30-39	81	33,9%	Gimnazija (SSS)	5	2,1%
40-49	73	30,5%	Viša škola, preddiplomski sveučilišni studij, stručni studij (sveučilišni prvostupnik/stručni prvostupnik/VŠS)	28	11,7%
50-59	52	21,8%	Diplomski sveučilišni studij, specijalistički diplomski stručni studij (magistar struke/stručni specijalist/VSS)	157	65,7%
60+	15	6,3%	Poslijediplomski specijalistički studij (univ. spec.)	14	5,9%
			Znanstveni magisterij (mr. sc.) ili doktorat (dr. sc.)	18	7,5%
Ukupno radno iskustvo	**N**	**%**	**Radno iskustvo u trenutnoj organizaciji**	**N**	**%**
<1	1	0,4%	<1	13	5,4%
1-2	2	0,8%	1-2	18	7,5%
2-3	12	5,0%	2-3	18	7,5%
3-5	14	5,9%	3-5	24	10,0%
5-10	35	14,6%	5-10	42	17,6%
10-20	80	33,5%	10-20	67	28,0%
20-30	53	22,2%	20-30	31	13,0%
30+	42	17,6%	30+	26	10,9%

Izvor: *vlastiti prikaz*

6.4.1.2. Podaci dobiveni empirijskim istraživanjem

Za sve čestice mjernog instrumenta, podaci dobiveni empirijskim istraživanjem analizirani su putem proporcije, aritmetičke sredine i standardne devijacije, a izrađena deskriptivna statistička analiza nalazi se u Prilogu 6.

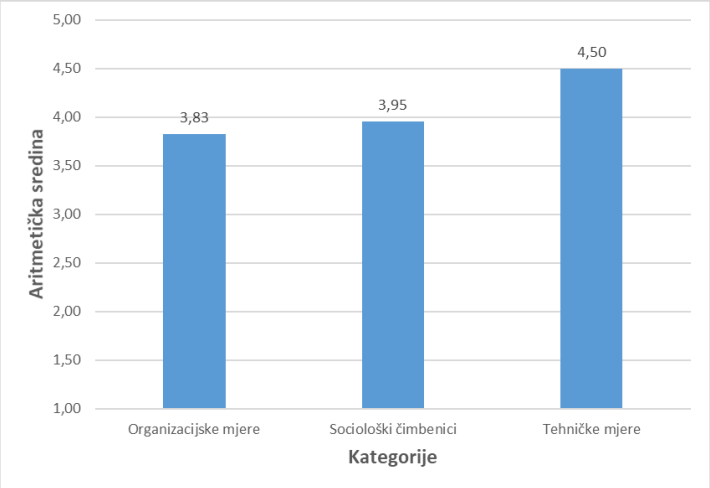
Standardna devijacija predstavlja mjeru koliko aritmetička sredina predstavlja promatrane podatke, gdje veliko standardno odstupanje ukazuje na to da aritmetička sredina nije dobra reprezentacija podataka jer se rezultati skupljaju široko oko prosjeka, dok s druge strane, malo standardno odstupanje ukazuje na manje raštrkanih podataka od srednje vrijednosti što pokazuje da aritmetička sredina adekvatno predstavlja podatke [307]. Vrijednosti standardne devijacije u ovom istraživanju bile su relativno male u usporedbi sa aritmetičkom sredinom te se stoga može razumno zaključiti da se srednja vrijednost može koristiti kao reprezentativna ocjena za svaku varijablu u skupu podataka. Grafikon 6.8. prikazuje aritmetičku sredinu čimbenika kulture informacijske sigurnosti.



Grafikon 6.8. Aritmetička sredina čimbenika kulture informacijske sigurnosti

Izvor: *vlastiti prikaz*

Grafikon 6.9. prikazuje aritmetičku sredinu tri kategorije kulture informacijske sigurnosti na temelju podataka dobivenih empirijskim istraživanjem iz kojeg je vidljivo kako se sve tri kategorije mogu smatrati ključnima budući da su iznosi aritmetičke sredine veći od sredine mjerne ljestvice koja se sastojala od 5 stupnjeva.



Grafikon 6.9. Aritmetička sredina kategorija kulture informacijske sigurnosti

Izvor: *vlastiti prikaz*

Od ukupno 46 manifestnih varijabli vezanih za čimbenike kulture informacijske sigurnosti, a koje su ostale u mjernom instrumentu nakon provjere sadržajne i konstruktne valjanosti i pouzdanosti putem validacije eksperata i faktorske analize, u ovom dijelu izdvojene su samo neke, koje mogu predstavljati značajnu informaciju, kako za istraživače, tako i za rukovodstvo, ne samo u promatranim organizacijama, već u svim organizacijama kojima bi to moglo biti od interesa.

Jedno od ugodnih iznenađenja u ovom istraživanju bili su odgovori na tvrdnju „*Ako poštujem pravila vezana uz informacijsku sigurnost, mogu pomoći u zaštiti informacijske imovine svoje organizacije*" gdje je čak 90,38% sudionika odgovorilo da se uglavnom ili u potpunosti slaže s tvrdnjom što može biti pokazatelj visoke razine svijesti o informacijskoj sigurnosti i upoznatosti sa stalno prisutnim prijetnjama i ranjivostima vezanima uz informacijsku imovinu organizacije.

Dodatno iznenađenje bili su rezultati tri tvrdnje vezane uz tehničke čimbenike, koje su imale apsolutno najbolju vrijednost. Tako je za tvrdnju „*Informacije trebaju biti zaštićene od neovlaštene upotrebe (čitanja, izmjene, brisanja)*" čak 82,85% sudionika izjavilo da se u potpunosti slaže s tom tvrdnjom, što, ako se uzmu u obzir i odgovori gdje se sudionici uglavnom slažu, dovodi do skoro 95% slaganja s navedenom tvrdnjom, uz napomenu da nijedan sudionik na ovom pitanju nije odabrao opciju „nije primjenjivo". Za tvrdnju „*Prilikom promjene lozinke, ona mora biti određene duljine i kombinacija malih i velikih slova te brojeva*", 80,33% sudionika izjavilo je kako se u potpunosti slaže, dok je 82,01% to isto izjavilo za tvrdnju „*Svim povjerljivim informacijama treba se moći pristupiti samo s odgovarajućim korisničkim imenom i lozinkom*". Ovi nalazi ukazuju na važnost tehničkih mjera informacijske sigurnosti koje se,

unatoč tome što je posljednjih nekoliko desetljeća naglasak na upravljačkom dijelu informacijske sigurnosti, ne smiju zanemariti, što ističu i Dlamini i suradnici [1].

S druge strane, na tvrdnju „*U mojoj organizaciji podržava se periodičko održavanje radionica za zaposlenike na temu informacijske sigurnosti*" čak trećina sudionika (30,96 %) odgovorilo je da se uglavnom ili u potpunosti ne slaže, što pokazuje kako je i dalje prisutan problem podrške rukovodstva za inicijative informacijske sigurnosti, o čemu se već duže vrijeme raspravlja u relevantnoj literaturi. S tim u vezi može se promatrati i tvrdnja „*Neću otkriti svoju lozinku za pristup računalu nikome pa čak ni svom nadređenom*" na koju je 21,34% sudionika odgovorilo kako se uglavnom ili u potpunosti ne slaže. Razlog za takve odgovore može biti u činjenici da su se ti sudionici već nalazili u situaciji gdje bi ih njihov nadređeni tražio lozinku za pristup sustavu dok je zaposlenik odsutan s radnog mjesta, a „posao se treba obaviti jučer", u kom slučaju je onda to povezano s manjkom podrške rukovodstva za sigurnosno ponašanje unutar organizacije i informacijsku sigurnost općenito. Drugi mogući razlog, mogao bi proizlaziti iz manjka edukacije o dobrim sigurnosnim praksama i pravilima ponašanja propisanim u sigurnosnim politikama, ako postoje.

Dodatne dvije tvrdnje čiji bi odgovori mogli biti korisni rukovoditeljima i općenito osobama koje donose odluke u organizacijama su „*Zaposlenici su educirani oko svojih uloga i odgovornosti vezanih za informacijsku sigurnost i toga kako se ponašati na siguran način*" te „*Smatram da je znanje o informacijskoj sigurnosti mojih kolega u organizaciji na zadovoljavajućoj razini*" gdje je 25,52% sudionika odgovorilo da se uglavnom ili u potpunosti ne slaže s prvom tvrdnjom odnosno 28,03% da se uglavnom ili u potpunosti ne slaže s drugom tvrdnjom, budući da odgovori na te tvrdnje ukazuju kako je potrebno konstantno ulagati u edukaciju zaposlenika po pitanju informacijske sigurnosti kako bi oni postali rješenje, a ne dio problema.

6.4.1. Analiza povezanosti kulture informacijske sigurnosti s primjenom implementiranih mjera dobre prakse informacijske sigurnosti

Konačni cilj ovog istraživanja bio je dobiti validiranu strukturu okvira za procjenu i unapređenje kulture informacijske sigurnosti koji će omogućiti interpretaciju identificiranih čimbenika koji prema kategorijama čine kulturu informacijske sigurnosti. Konceptualni okvir temeljio se na izrađenom mjernom instrumentu i dijelio njegovu strukturu, odnosno sastojao se od 95 manifestnih varijabli (čestice) kojima se opisuje 13 latentnih varijabli prve razine (čimbenici) te 3 latentne varijable druge razine (kategorije) koje su opisane tim čimbenicima.

Upravo spomenuti čimbenici i kategorije iz mjernog instrumenta sastavni su dijelovi okvira za procjenu i unapređenje kulture informacijske sigurnosti te se validacijom mjernog instrumenta formira konačna konstrukcija okvira sa svim pripadajućim kategorijama i čimbenicima, čime je djelomično validiran i sam okvir. Validacija konceptualnog okvira započela je validacijom mjernog instrumenta provjerom sadržajne i konstruktne valjanosti mjernog instrumenta putem mišljenja eksperata, a zatim provođenjem faktorske analize kojom se, uz valjanost, provjeravala i pouzdanost mjernog instrumenta putem mjere unutarnje konzistentnosti.

Nakon provjere sadržajne i konstruktne valjanosti, mjerni instrument, a time i konceptualni okvir, sadržavao je ukupno 67 manifestnih varijabli te 11 latentnih varijabli prvog reda koje su činile 3 latentne varijable drugog reda na temelju kojeg je provedeno empirijsko istraživanje. Na temelju rezultata empirijskog istraživanja provedena je eksploratorna faktorska analiza kojom se dobilo ukupno 8 faktora odnosno latentnih varijabli prvog stupnja, koje su opisane od strane 46 manifestnih varijabli te raspoređene u prvotno oformljene 3 latentne varijable drugog reda (kategorije). Formiranjem konačne strukture mjernog instrumenta, mjernom instrumentu je potvrđena valjanost i pouzdanost čime je provedena validacija mjernog instrumenta i time ostvaren **drugi postavljeni cilj istraživanja**.

Validacijom mjernog instrumenta validiran je i konceptualni okvir u dijelu teoretske strukture samog okvira odnosno koncepata koji čine okvir, čime je potvrđena **hipoteza H1**. Da bi se konceptualni okvir validirao i u praktičnom dijelu, odnosno da bi se pokazalo kako je njegova struktura koja je nastala na temelju teorije, primjenjiva u praksi, bilo je potrebno analizirati povezanost kulture informacijske sigurnosti s primjenom implementiranih mjera dobre prakse informacijske sigurnosti na temelju 12 pitanja o objektivnim pokazateljima primjene implementiranih mjera informacijske sigurnosti u sklopu mjernog instrumenta.

Kako bi se testirala značajnost povezanosti kulture informacijske sigurnosti i stvarnog stanja po pitanju implementiranosti mjera dobre prakse, napravljena je korelacijska analiza koristeći parametrijsku metodu izračuna Pearsonovog koeficijenta korelacije i neparametrijsku metodu izračuna Spearmanovog rho koeficijenta [343]. Bitno je naglasiti kako koeficijent korelacije ukazuje na snagu međusobnog odnosa dvije varijable, ali povezanost te dvije varijable ne daje objašnjenje uzročnosti, što se ovim istraživanjem nije ni ispitivalo.

Jedna od varijabli između koje je računata korelacija bila je varijabla *SS_final* koja je označavala stvarno stanje u organizaciji po pitanju praksi vezanih uz informacijsku sigurnost

(primjerice, zaključavanje računala nakon napuštanja radnog mjesta, sudjelovanje na edukacijama i radionicama podizanja svijesti vezano za informacijsku sigurnost, obveza korištenja složenih lozinki prilikom prijave na informacijski sustav i sl.).

Varijabla *SS_final* sastojala se od 12 čestica (pitanja) na koje su sudionici odgovarali zajedno s pitanjima vezanim uz stavove o kulturi informacijske sigurnosti. Za razliku od pitanja iz kategorija *Organizacijske mjere, Sociološki čimbenici* i *Tehničke mjere* gdje su odgovori bili bazirani na ordinalnoj semantičkoj skali s pet stupnjeva, od „*1 - u potpunosti se ne slažem*", do „*5 – u potpunosti se slažem*", kod ovog tipa pitanja bilo je nekoliko vrsta ponuđenih odgovora. Tako su neka pitanja imala ponuđene odgovore tipa a) „*1 – u potpunosti se slažem*" do „*5 – u potpunosti se ne slažem*"; b) „*1 - uopće ne*" do „*5 - vrlo često*" ili c) „*1 - 0 puta*" do „*5 - 4 i više puta*", kao što je vidljivo u Prilogu 1.

Druga varijabla između koje je računata korelacija bila je nova varijabla *KULTURA_final* koju je trebalo izračunati, a koja je obuhvaćala čestice (pitanja) iz kategorija *Organizacijske mjere, Sociološki čimbenici* i *Tehničke mjere* za koje je faktorskom analizom potvrđeno da čine mjerni instrument, a samim time i okvir za procjenu i unapređenje kulture informacijske sigurnosti.

U svrhu testiranja druge hipoteze (H2) korištena je parametrijska kao i neparametrijska korelacijska analiza, odnosno Pearsonov koeficijent korelacije (Tablica 6.47.) i Spearmanov rho koeficijent (Tablica 6.48.). Kao što je vidljivo na temelju prikazanih rezultata, obje metode dale su slične rezultate. Iz rezultata dobivenih analiza, na razini značajnosti $\alpha = 0.01$, može se zaključiti kako postoji **pozitivna korelacija relativno slabe jačine** između varijabli koje predstavljaju stvarno stanje i kulturu informacijske sigurnosti (Pearsonov koeficijent korelacije $r = 0{,}395$, $n = 239$, $p = 0.000$; Spearmanov rho koeficijent $r_s = 0{,}373$, $n = 239$, $p = 0.000$).

Tablica 6.47. Izračun Pearsonovog koeficijenta korelacije (r) između varijabli stvarno stanje i kultura

Korelacije

		KULTURA_final	SS_final
KULTURA_final	Pearsonova korelacija	1	,395**
	Sig. (dvosmjerna)		0,000
	N	239	239
SS_final	Pearsonova korelacija	,395**	1
	Sig. (dvosmjerna)	0,000	
	N	239	239

****. Korelacija je signifikantna na razini 0,01 (dvosmjerna).**

Izvor: *vlastiti prikaz*

Tablica 6.48. Izračun Spearmanovog koeficijenta rho (r_s) između varijabli stvarno stanje i kultura

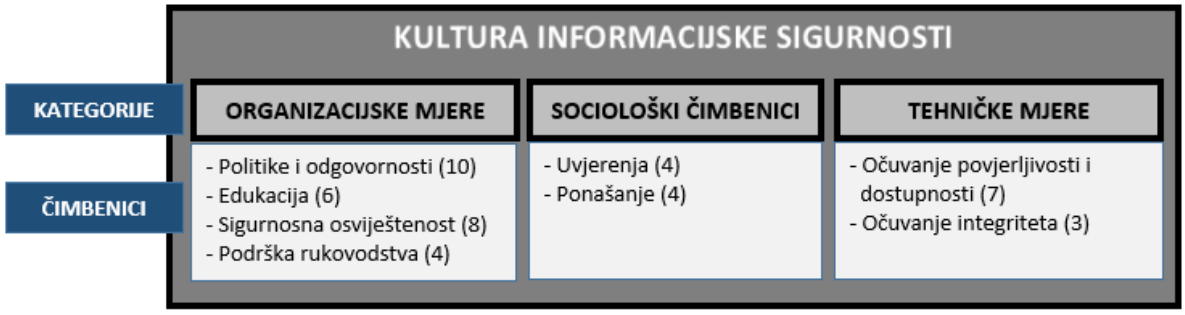
Korelacije

			KULTURA_final	SS_final
Spearmanov rho	**KULTURA_final**	**Koeficijent korelacije**	**1**	**,373****
		Sig. (dvosmjerna)		**0,000**
		N	**239**	**239**
	SS_final	**Koeficijent korelacije**	**,373****	**1**
		Sig. (2-tailed)	**0,000**	
		N	**239**	**239**

****. Korelacija je signifikantna na razini 0,01 (dvosmjerna).**

Izvor: *vlastiti prikaz*

Interpretirajući ove rezultate možemo zaključiti kako će, u slučaju postojanja razvijene kulture informacijske sigurnosti u organizaciji, vjerojatno biti prisutna i primjena odgovarajućih implementiranih mjera informacijske sigurnosti, čime je potvrđena **hipoteza H2**.



Slika 6.2. Okvir za procjenu i unapređenje kulture informacijske sigurnosti

Izvor: *vlastiti prikaz*

Validirani okvir za procjenu i unapređenje kulture informacijske sigurnosti prikazan je na Slici 6.2. Potvrdom hipoteze H2 te na temelju validiranog mjernog instrumenta i rezultata provedenog empirijskog istraživanja nakon čega je utvrđena konačna struktura predloženog okvira za procjenu i unapređenje kulture informacijske sigurnosti, predloženi okvir je validiran, čime je postignut **treći postavljeni cilj istraživanja**.

7. ZAKLJUČAK

Posljednje poglavlje ovog rada nastavlja se na prethodno na način da sažima dobivene rezultate istraživanja te navodi proizašle znanstvene i društvene doprinose, ali istovremeno navodi prepoznata ograničenja ovog istraživanja te na kraju pruža smjernice za buduća istraživanja.

Istraživanje opisano u ovoj disertaciji sastojalo se od četiri faze u kojima su se koristile kvalitativne i kvantitativne znanstvene metode kako bi se ostvarili postavljeni ciljevi istraživanja te testirale postavljene hipoteze.

Prvi cilj istraživanja, *identificirati čimbenike koji čine kulturu informacijske sigurnosti,* **ostvaren** je u prvoj fazi istraživanja putem pregleda i analize relevantne literature što je rezultiralo prikazom identificiranih čimbenika kulture, sumiranih u Tablici 9. u potpoglavlju 6.1.

Drugi cilj istraživanja, *razviti mjerni instrument za procjenu kulture informacijske sigurnosti koji sadrži ključne čimbenike koji su vezani uz kulturu informacijske sigurnosti unutar organizacije* postignut je aktivnostima iz više različitih faza istraživanja. Tako su se prvo kreirale čestice mjernog instrumenta na temelju pregleda i analize relevantne literature čime je definirano 95 manifestnih varijabli (čestice) kojima se opisuje 13 latentnih varijabli prve razine (čimbenici) te 3 latentne varijable druge razine (kategorije), nakon čega se pristupilo validaciji mjernog instrumenta provjerom njegove sadržajne i konstruktne valjanosti te pouzdanosti. Sadržajna i konstruktna valjanost prvo je ispitana putem mišljenja eksperata (potpoglavlje 6.3.), a zatim provođenjem eksploratorne faktorske analize kojom se, uz valjanost, provjeravala i pouzdanost mjernog instrumenta putem mjere unutarnje konzistentnosti (potpoglavlje 6.3.2).

Nakon provjere sadržajne i konstruktne valjanosti putem mišljenja eksperata upotrebom metode zatvorenog sortiranja karata te izračunom pokazatelja kao što su omjer sadržajne valjanosti, prosječna vrijednost relativne važnosti, omjer pogodaka i Fleiss Kappa koeficijent, mjerni instrument je sadržavao ukupno 67 manifestnih varijabli te 11 latentnih varijabli prvog reda koje su činile 3 latentne varijable drugog reda, nakon čega je provedeno empirijsko istraživanje. Na temelju rezultata empirijskog istraživanja provedena je eksploratorna faktorska analiza metodom Principal axis factoring i ortogonalnom Varimax rotacijom koja je rezultirala s ukupno 8 faktora odnosno čimbenika koji čine tri glavne kategorije radnog okvira za procjenu i unapređenje kulture informacijske sigurnosti. Tako kategoriju *Organizacijske mjere* opisuju 4 čimbenika koji objašnjavaju 60,40% zajedničke varijance skupa varijabli, dok kategorije

Sociološki čimbenici i *Tehničke mjere* svaku opisuje po dva čimbenika koji objašnjavaju 58,74% zajedničke varijance za kategoriju *Sociološki čimbenici* odnosno 52,60% zajedničke varijance za kategoriju *Tehničke mjere*. Ujedno, faktorskom analizom smanjen je broj manifestnih varijabli na 28 s početnih 42 za kategoriju *Organizacijske mjere*, odnosno na 8 s početnih 10 za kategoriju *Sociološki čimbenici* i na 10 s početnih 15 za kategoriju *Tehničke mjere*. Formiranjem konačne strukture mjernog instrumenta, mjernom instrumentu je potvrđena valjanost i pouzdanost čime je provedena validacija mjernog instrumenta i time **ostvaren drugi postavljeni cilj istraživanja**.

Treći istraživački cilj, *razviti i validirati okvir za procjenu i unapređenje kulture informacijske sigurnosti*, usko je vezan uz drugi cilj istraživanja iz razloga što se predloženi okvir temeljio na izrađenom mjernom instrumentu i dijelio njegovu strukturu, odnosno sastojao se od prvotno definiranih 95 manifestnih varijabli kojima se opisuje 13 čimbenika te 3 kategorije koje su opisane tim čimbenicima (potpoglavlja 6.2. i 6.3.). Provjerom valjanosti mjernog instrumenta, a time i radnog okvira za procjenu i unapređenje kulture informacijske sigurnosti od strane eksperata, djelomično je potvrđena hipoteza *H1: Organizacijske mjere i sociološki čimbenici zajedno s tehničkim mjerama ključne su kategorije u procjeni i unapređenju kulture informacijske sigurnosti u organizaciji,* dok je validacijom mjernog instrumenta nakon provođenja faktorske analize validiran i konceptualni okvir u dijelu teoretske strukture samog okvira odnosno koncepata koji čine okvir (potpoglavlje 6.4.2.). Time je **postignut treći istraživački cilj** te cjelovito **potvrđena hipoteza H1**.

Za testiranje hipoteze *H2: Razina kulture informacijske sigurnosti pozitivno je povezana s primjenom implementiranih mjera informacijske sigurnosti u organizaciji na način da veća razina kulture informacijske sigurnosti predstavlja veću primjenu implementiranih mjera informacijske sigurnosti* provedena je korelacijska analiza. Korelacijskom analizom koja je provedena koristeći kako parametrijsku metodu Pearsonovog koeficijenta korelacije tako i neparametrijsku metodu Spearmanovog rho koeficijenta utvrđena je *relativno slaba, pozitivna povezanost* između varijabli koje predstavljaju stvarno stanje i kulturu informacijske sigurnosti. Interpretirajući ove rezultate možemo zaključiti kako će, u slučaju postojanja razvijene kulture informacijske sigurnosti u organizaciji, vjerojatno biti prisutna i primjena odgovarajućih implementiranih mjera informacijske sigurnosti, čime je **potvrđena hipoteza H2**.

7.1. Doprinos provedenog istraživanja

Istraživanje opisano ovom disertacijom, uz ilustraciju kako je za istraživanje u području informacijske sigurnosti moguće koristiti kombinaciju kvalitativnih i kvantitativnih znanstvenih metoda, rezultiralo je s nekoliko značajnih znanstvenih doprinosa u području kulture informacijske sigurnosti.

Najznačajniji prepoznati **znanstveni doprinosi** su: (1) sistematizacija znanja iz područja kulture informacijske sigurnosti na temelju opsežnog pregleda relevantne znanstvene literature o kulturi informacijske sigurnosti i upravljanju informacijskom sigurnošću; (2) identifikacija ključnih čimbenika koje čine kulturu informacijske sigurnosti; (3) razvijen i validiran mjerni instrument za procjenu kulture informacijske sigurnosti temeljen na dosadašnjim istraživanjima i preporukama za poboljšanje postojećih anketnih upitnika te provedenom empirijskom istraživanju; (4) razvijen i validiran okvir za procjenu i unapređenje kulture informacijske sigurnosti koji kulturu informacijske sigurnosti ne promatra u samo jednom aspektu (primjerice ponašanja zaposlenika) već u obzir uzima njenu organizacijsku, sociološku i tehničku komponentu.

Uz navedeni znanstveni doprinos, prepoznat je i određeni **društveni doprinos** na način da rukovodstvo organizacije može upotrijebiti rezultate ovog istraživanja fokusirajući ograničene resurse na one elemente koji doprinose unapređenju kulture informacijske sigurnosti čime bi se uštedjelo vrijeme i novac te ujedno stvorila dodana vrijednost i preveniralo nastajanje rizika vezanih uz informacijsku sigurnost koji mogu negativno utjecati na samu organizaciju kao i njezine zaposlenike. Naime, razvijeni radni okvir za procjenu i unapređenje kulture informacijske sigurnosti promatra 3 ključne kategorije (organizacijske mjere, sociološke čimbenike i tehničke mjere) kulture informacijske sigurnosti čime predstavlja uravnoteženi alat kojim je moguće identificirati i utjecati na onu komponentu koja ne doprinosi dovoljno postojećoj kulturi informacijske sigurnosti, odnosno u suprotnom, na onu koja uvelike utječe na postojeću kulturu informacijske sigurnosti i omogućava stvaranje dodane vrijednosti za organizaciju u cjelini.

7.2. Ograničenja provedenog istraživanja

Sva istraživanja, neovisno o vrsti, opsegu, veličini i trajanju neizbježno sa sobom povlače i određena ograničenja pa tako ni istraživanje provedeno u sklopu izrade ove doktorske disertacije nije iznimka.

Jedno od glavnih prepoznatih ograničenja ovog istraživanja bila je nemogućnost kreiranja statistički reprezentativnog uzorka organizacija koje čine operatore ključnih usluga kao i zaposlenika odnosno samih sudionika istraživanja, uslijed nemogućnosti određivanja veličine cjelokupne populacije. To ograničenje ujedno je vezano uz ograničenu mogućnost generalizacije rezultata zbog korištenja neprobabilističke metode uzorkovanja.

Sljedeće ograničenje predstavlja relativno malen, iako dovoljan, broj eksperata koji su sudjelovali u provjeri sadržajne i konstruktne valjanosti mjernog instrumenta. Jedno od značajnih ograničenja koje se općenito javlja u društvenim istraživanjima je i razina (ne)motiviranosti sudionika za sudjelovanje u istraživanju što rezultira slabim odazivom sudionika. To se pokazalo i u ovom slučaju gdje je gotovo polovica sudionika odustala od ispunjavanja upitnika čije je trajanje bilo procijenjeno na 15 minuta. U ovom istraživanju postojala je velika diversifikacija ispitivanih organizacija unutar sektora, kao i samih sektora pa je tako posebno slab odaziv bio u sektoru infrastruktura financijskog tržišta zbog čega nije moguće izvući neke statistički značajne zaključke o konkretno tom sektoru.

Također, iako je pregled relevantne literature obavljen na sistematičan način, postoje neka moguća ograničenja prilikom tog procesa. Budući da je pregled, odabir i procjenu relevantnosti pojedine literature radio autor ove disertacije radio samostalno, taj proces temeljio se na subjektivnoj procjeni koja je mogla utjecati na ishod pregleda literature u smislu isključivanja nekih radova koji bi bili predmetom interesa za ovo istraživanje, kao i uključivanjem nekih koji možda ne doprinose značajno samoj temi istraživanja. Dodatno, prilikom pregleda literature, u obzir su uzimani samo radovi na engleskom jeziku dok su ostali jezici zanemareni.

7.3. Smjernice za buduća istraživanja

Rezultati istraživanja opisanog u ovoj disertaciji otvorili su mogućnosti za nova istraživanja. Primjerice, potrebno je provesti dodatna empirijska istraživanja kojima bi se mogla poboljšati kvaliteta razvijenog okvira za procjenu i unapređenje kulture informacijske sigurnosti, zajedno s pripadajućim mjernim instrumentom. Budući da je validacija okvira provedena na relativno malom, ali prihvatljivom uzorku, istraživanje koje bi uključilo više sudionika, pogotovo ako bi se odabir sudionika temeljio na probabilističkom uzorkovanju, moglo bi značajno obogatiti postojeći okvir i pripadajući mjerni instrument, kao i povećati mogućnost generalizacije dobivenih zaključaka.

Također, moguće je provesti ovakvo istraživanje u drugim sektorima, koji ne predstavljaju operatore ključnih usluga kako bi se mogli usporediti rezultati i vidjeti postoje li značajne razlike između tih skupina organizacija. Rezultati ovog istraživanja mogu se testirati i u različitim okruženjima izvan Republike Hrvatske budući da kontekst nacionalne kulture i možebitnih specifičnih obilježja koje nacionalna kultura sa sobom nosi, nije uključen u razvijeni okvir. Dodatno, bilo bi zanimljivo istražiti u kolikoj mjeri je ovaj radni okvir primjenjiv na mala i srednja poduzeća, budući da je ovaj okvir, iako nije specifično rađen samo za operatore ključnih usluga, testiran uglavnom na većim organizacijama budući da su u pravilu operatori ključnih usluga organizacije s većim brojem zaposlenika.

Kao dodatna mogućnost nameće se i potreba istraživanja kojim bi se ispitalo postoje li neki čimbenici koji nisu uključeni u dosadašnje radne okvire i modele, uključujući radni okvir nastao ovim istraživanjem, a koji bi mogli značajno utjecati na razinu kulture informacijske sigurnosti u organizaciji. Ukoliko bi se takav čimbenik pronašao, kako bi se on uklopio u postojeću strukturu izrađenog ranog okvira? Jedna od mogućnosti je i dodatno proširiti izrađeni okvir s nekim od postojećih i već prepoznatih čimbenika koji su iz ovog ili onog razloga izostavljeni iz konceptualizacije izrađenog okvira. Iako, povećanjem broja elemenata koji čine okvir, povećava se i potreban broj sudionika čime se potencijalno može doći u slijepu ulicu s istraživanjem, ukoliko istraživač neće biti u mogućnosti skupiti reprezentativan uzorak sudionika. Buduća istraživanja mogla bi uključivati i ispitivanje veza između identificiranih kategorija i čimbenika okvira te kreiranje i validiranje modela uz pomoć strukturalnog modeliranja.

U konačnici, budući da područje kulture informacijske sigurnosti još uvijek nije u potpunosti shvaćeno, istraživanja o tome kako uspostaviti i održavati dobru kulturu informacijske sigurnosti i dalje su dobrodošla.

LITERATURA

[1] M. Dlamini, J. Eloff, and M. Eloff, “Information security: The moving target,” *Comput. Secur.*, vol. 28, no. 3–4, pp. 189–198, 2009.

[2] Z. A. Soomro, M. H. Shah, and J. Ahmed, “Information security management needs more holistic approach: A literature review,” *Int. J. Inf. Manage.*, vol. 36, no. 2, pp. 215–225, 2016.

[3] T. Kayworth and D. Whitten, “Effective Information Security Requires a Balance of Social and Technology Factors,” *Mis Q. Exec.*, vol. 9, no. 3, pp. 163–175, 2010.

[4] E. Yildirim, “The importance of information security awareness for the success of business enterprises,” in *Advances in Intelligent Systems and Computing*, 2016, pp. 211–222.

[5] H. W. Glaspie and W. Karwowski, “Human Factors in Information Security Culture: A Literature Review,” in *Advances in Human Factors in Cybersecurity*, D. Nicholson, Ed. Springer, 2018, pp. 269–280.

[6] A. Alhogail, “Design and validation of information security culture framework,” *Comput. Human Behav.*, vol. 49, pp. 567–575, 2015.

[7] E. Sherif, S. Furnell, and N. Clarke, “An Identification of Variables Influencing the Establishment of Information Security Culture,” in *Proceedings of the Third International Conference on Human Aspects of Information Security, Privacy, and Trust*, 2015, vol. 9190, no. 2010, pp. 436–448.

[8] M. Tang, M. Li, and T. Zhang, “The impacts of organizational culture on information security culture: a case study,” *Inf. Technol. Manag.*, vol. 17, no. 2, pp. 179–186, 2016.

[9] C. Colwill, “Human factors in information security: The insider threat - Who can you trust these days?,” *Inf. Secur. Tech. Rep.*, vol. 14, no. 4, pp. 186–196, 2009.

[10] S. Panguluri, T. D. Nelson, and R. P. Wyman, “Creating a Cyber Security Culture for Your Water/Waste Water Utility,” in *Cyber-Physical Security*, R. M. C. and S. Hakim, Ed. Springer, 2017, pp. 133–160.

[11] A. Alhogail and A. Mirza, “Information security culture: A definition and a literature review,” in *2014 World Congress on Computer Applications and Information Systems, WCCAIS 2014*, 2014, pp. 1-7.

[12] L. Connolly, M. Lang, and D. Tygar, “Managing Employee Security Behaviour in Organisations: The Role of Cultural Factors and Individual Values,” in *SEC 2014, IFIP AICT 428*, 2014, pp. 417–430.

[13] A. Mahfuth, S. Yussof, A. A. Baker, and N. Ali, “A systematic literature review: Information security culture,” in *International Conference on Research and Innovation in Information Systems, ICRIIS,* 2017, pp. 1–6.

[14] H. Stewart and J. Jürjens, “Information security management and the human aspect in organizations,” *Inf. Comput. Secur.*, vol. 25, no. 5, pp. 494–534, 2017.

[15] M. A. Alnatheer, “A Conceptual Model to Understand Information Security Culture,” *Int. J. Soc. Sci. Humanit.*, vol. 4, no. 2, pp. 104–107, 2014.

[16] A. Da Veiga, “An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture,” *Inf. Comput. Secur.*, vol. 26, no. 5, pp. 584–612, 2018.

[17] A. Da Veiga and N. Martins, “Improving the information security culture through monitoring and implementation actions illustrated through a case study,” *Comput. Secur.*, vol. 49, pp. 162–176, 2015.

[18] N. H. Hassan, Z. Ismail, and N. Maarop, “Understanding Relationship Between Security Culture and Knowledge Management,” in *KMO 2014, LNBIP 185*, 2014, pp. 397–402.

[19] EY, “Cybersecurity regained: preparing to face cyber attacks - 20th Global Information Security Survey 2017-18.” p. 32, 2017.

[20] M. Al-Awadi and K. Renaud, “Success factors in information security: implementation in organizations,” in *IADIS International Conference e-Society*, 2007, no. December, pp. 169–176.

[21] S. M. Furnell, M. Gennatou, and P. S. Dowland, “A prototype tool for information security awareness and training,” *Logist. Inf. Manag.*, vol. 15, no. 5/6, pp. 352–357, 2002.

[22] W. AI-Salihy, J. R. Ann Sures, and R. Sures, “Effectivess of Information Systems Security in IT Organizations in Malaysia,” in *9th Asia-Pacific Conference on Communications*, 2003, pp. 716–720.

[23] J. R. Vacca, Ed., *Computer and Information Security Handbook*, Third Edit. Morgan Kaufmann, 2017.

[24] W. Jin and Z. Yu, “The Analysis of Information System Security Issue Based on Economics,” in *International Conference on Information Engineering and Communications Technology (IECT 2016)*, 2016.

[25] T. Campbell, *Practical Information Security Management*. Apress, 2016.

[26] Leksikografski zavod Miroslav Krleža, “Hrvatska enciklopedija, mrežno izdanje,” 2020. [Online]. Available: http://www.enciklopedija.hr. [Accessed: 04-May-2020].

[27] Russell Ackoff, “From Data to Wisdom,” *J. Appl. Syst. Anal.*, no. 16, pp. 3–9, 1989.

[28] M. E. Whitman and H. J. Mattord, *Principles of Information Security*, Sixth Edit. Cengage Learning, 2018.

[29] A. Chopra and M. Chaudhary, *Implementing an Information Security Management System*. Apress, 2020.

[30] Mehdi Kazemi, “Evaluation of information security management system success factors: Case study of Municipal organization,” *African J. Bus. Manag.*, vol. 6, no. 14, pp. 4982–4989, 2012.

[31] S. Flowerday and R. Von Solms, “What constitutes information integrity?,” *SA J. Inf. Manag.*, vol. 9, no. 4, 2007.

[32] ISO/IEC, “ISO/IEC 27000 - Information technology - Security techniques - Information security management systems - Overview and vocabulary.” 2018.

[33] M. Nieles, K. Dempsey, and V. Y. Pillitteri, “NIST Special Publication 800-12 Revision 1 - An introduction to information security,” 2017.

[34] T. Helokunnas and R. Kuusisto, “Information Security Culture in a Value Net,” in *IEEE International Engineering Management Conference*, 2003, pp. 190–194.

[35] U. H. Rao and U. Nayak, *The InfoSec Handbook*. Apress, 2014.

[36] S. Posthumus and R. Von Solms, “A framework for the governance of information security,” *Comput. Secur.*, vol. 23, no. 8, pp. 638–646, 2004.

[37] A. Alkalbani, H. Deng, and B. Kam, “A Conceptual Framework for Information Security in Public Organizations for E-Government Development,” in *25th Australasian Conference on Information Systems*, 2014.

[38] J. More, A. Stieber, and C. Liu, *Breaking Into Information Security: Crafting a Custom Career Path to Get the Job You Really Want*. Syngress, 2016.

[39] D. Kim and M. G. Solomon, *Fundamentals of Information Systems Security*, Third Edit. Jones & Bartlett Learning, 2018.

[40] P. Salus, “Net Insecurity: Then and Now (1969–1998),” *Sane ’98 Online*, 1998. [Online]. Available: http://www.sane.nl/events/sane98/aftermath/salus.html. [Accessed: 25-Apr-2020].

[41] S. E. Choi, J. T. Martins, and I. Bernik, “Information security: Listening to the perspective of organisational insiders,” *J. Inf. Sci.*, vol. 44, no. 6, pp. 752–767, 2018.

[42] Z. Krakar, S. T. Rotim, M. Žgela, K. Arbanas, and T. Kišasondi, *Korporativna informacijska sigurnost*. Fakultet organizacije i informatike Sveučilišta u Zagrebu & Zavod za informatičku djelatnost Hrvatske d.o.o., 2014.

[43] S. H. (Basie) von Solms, “The 5 Waves of Information Security – From Kristian Beckman to the Present,” in *IFIP Advances in Information and Communication Technology*, K. Rannenberg, V. Varadharajan, and C. Weber, Eds. 2010, pp. 1–8.

[44] B. Von Solms, “Information security - The third wave?,” *Comput. Secur.*, vol. 19, no. 7, pp. 615–620, 2000.

[45] B. von Solms, “Information Security - The Fourth Wave,” *Comput. Secur.*, vol. 25, no. 3, pp. 165–168, 2006.

[46] ISO/IEC, “ISO/IEC 27032 - Information technology - Security techniques — Guidelines for cybersecurity.” 2012.

[47] R. Von Solms and J. Van Niekerk, “From information security to cyber security,” *Comput. Secur.*, vol. 38, pp. 97–102, 2013.

[48] R. Reid and J. Van Niekerk, “From Information Security to Cyber Security Cultures,” in *Information Security South Africa (ISSA)*, 2014, pp. 1–7.

[49] A. Da Veiga, “A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument,” in *Proceedings of 2016 SAI Computing Conference, SAI 2016*, 2016, pp. 1006–1015.

[50] N. Gcaza and R. von Solms, “Cybersecurity culture: An ill-defined problem,” in *IFIP Advances in Information and Communication Technology*, 2017, vol. 503, pp. 98–109.

[51] M. Spremić, *Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije*. Zagreb: Ekonomski fakultet, Sveučilišna tiskara d.o.o., 2017.

[52] B. von Solms and R. von Solms, “Cyber Security and Information Security – What goes where?,” *Inf. Comput. Secur.*, vol. 26, no. 1, pp. 2–9, 2018.

[53] R. De Bruin and S. H. Von Solms, “Cybersecurity Governance: How can we measure it?,” in *2016 IST-Africa Conference, IST-Africa 2016*, 2016, pp. 1–9.

[54] I. Lopes and P. Oliveira, “Understanding Information Security Culture: A Survey in Small and Medium Sized Enterprises,” in *New Perspectives in Information Systems and Technologies, Volume 1, Advances in Intelligent Systems and Computing 275*, 2014, pp. 277–286.

[55] K. Arbanas and N. Žajdela Hrustek, “Key success factors of information systems security,” *J. Inf. Organ. Sci.*, vol. 43, no. 2, pp. 131–144, 2019.

[56] H. Haqaf and M. Koyuncu, “Understanding key skills for information security managers,” *Int. J. Inf. Manage.*, vol. 43, pp. 165–172, 2018.

[57] A. Volchkov, *Information Security Governance: Framework and Toolset for CISOs and Decision Makers*. CRC Press, Taylor & Francis Group, 2019.

[58] A. B. Ruighaver, S. B. Maynard, and S. Chang, “Organisational security culture: Extending the end-user perspective,” *Comput. Secur.*, vol. 26, no. 1, pp. 56–62, 2007.

[59] N. H. Hassan and Z. Ismail, “A Conceptual Model for Investigating Factors Influencing Information Security Culture in Healthcare Environment,” in *International Congress on Interdisciplinary Business and Social Science 2012*, 2012, vol. 65, pp. 1007–1012.

[60] S. E. Chang and C.-S. Lin, “Exploring organizational culture for information security management,” *Ind. Manag. Data Syst.*, vol. 107, no. 3, pp. 438–458, 2007.

[61] B. Von Solms and R. Von Solms, “The 10 deadly sins of information security management,” *Comput. Secur.*, vol. 23, no. 5, pp. 371–376, 2004.

[62] J. Kwon, J. R. Ulmer, and T. Wang, “The Association between Top Management Involvement and Compensation and Information Security Breaches,” *J. Inf. Syst.*, vol. 27, no. 1, pp. 219–236, 2013.

[63] M. Zammani and R. Razali, “An Empirical Study of Information Security Management Success Factors,” *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 6, no. 6, pp. 904–913, 2016.

[64] M. Spremić, *Digitalna transformacija poslovanja*. Zagreb: Ekonomski fakultet, Sveučilišna tiskara d.o.o., 2017.

[65] M. Spremić, “Holistic approach for governing information system security,” in *Proceedings of the World Congress on Engineering 2013 Vol II, WCE 2013*, 2013, pp. 1242–1247.

[66] T. Herath and H. R. Rao, “Protection motivation and deterrence: A framework for security policy compliance in organisations,” *Eur. J. Inf. Syst.*, vol. 18, no. 2, pp. 106–125, 2009.

[67] Y. Chen, K. Ramamurthy, and K. W. Wen, “Organizations’ information security policy compliance: Stick or carrot approach?,” *J. Manag. Inf. Syst.*, vol. 29, no. 3, pp. 157–188, 2012.

[68] J. S. Lim, S. Chang, S. Maynard, and A. Ahmad, “Exploring the Relationship between Organizational Culture and Information Security Culture,” in *Proceedings of the 7th Australian Information Security Management Conference*, 2009, no. December, pp. 88–97.

[69] A. N. Singh, M. P. Gupta, and A. Ojha, “Identifying factors of ‘organizational information security management,’” *J. Enterp. Inf. Manag.*, vol. 27, no. 5, pp. 644–667, 2014.

[70] L. Connolly and M. Lang, “Information Systems Security: The Role of Cultural Aspects in Organizational Settings,” in *Proceedings of the Eighth Pre-ICIS Workshop on*

Information Security and Privacy, 2013, pp. 1–16.

[71] A. McIlwraith, *Information Security and Employee Behaviour*. Gower Publishing Limited, 2006.

[72] B. Von Solms, "Information security - A multidimensional discipline," *Comput. Secur.*, vol. 20, no. 6, pp. 504–508, 2001.

[73] W. D. Kearney and H. A. Kruger, "Can perceptual differences account for enigmatic information security behaviour in an organisation?," *Comput. Secur.*, vol. 61, pp. 46–58, 2016.

[74] T. Schlienger and S. Teufel, "Information Security Culture - The Socio-Cultural Dimension in Information Security Management," in *Security in the information society: visions and perspectives. IFIP TC11 International Conference on Information Security (Sec2002)*, 2002, pp. 191–201.

[75] Q. Hu, T. Dinev, P. Hart, and D. Cooke, "Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture," *Decis. Sci.*, vol. 43, no. 4, pp. 615–660, 2012.

[76] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," *Comput. Secur.*, vol. 25, no. 4, pp. 289–296, 2006.

[77] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Q.*, vol. 34, no. 3, pp. 523–548, 2010.

[78] A. A. Norman and N. M. Yasin, "Information systems security management (ISSM) success factor: Retrospection from the scholars," *African J. Bus. Manag.*, vol. 7, no. 27, pp. 2646–2656, 2013.

[79] R. Reid, J. Van Niekerk, and K. Renaud, "Information security culture: A general living systems theory perspective," in *2014 Information Security for South Africa - Proceedings of the ISSA 2014 Conference*, 2014, pp. 1–8.

[80] A. Da Veiga and N. Martins, "Information security culture: A comparative analysis of four assessments," in *Proceedings of the 8th European Conference on Information Management and Evaluation, ECIME 2014*, 2014, pp. 49–57.

[81] A. Almubark, N. Hatanaka, O. Uchida, and Y. Ikeda, "Identifying the Organizational Factors of Information Security Incidents," in *Second International Conference on Computing Technology and Information Management (ICCTIM)*, 2015, pp. 7–12.

[82] E. D. Frauenstein and R. Von Solms, "Combatting phishing: A holistic human approach," in *2014 Information Security for South Africa - Proceedings of the ISSA 2014*

Conference, 2014, pp. 1–10.

[83] I. Alsmadi, R. Burdwell, A. Aleroud, A. Wahbeh, M. Al-Qudah, and A. Al-Omari, *Practical Information Security*. Springer International Publishing AG, 2018.

[84] M. Ciampa, *Security Awareness: Applying Practical Security in Your World*, Third Edit. Course Technology, Cengage Learning, 2010.

[85] M.-D. Mclaughlin and J. Gogan, "Challenges and Best Practices in Information Security Management," *Mis Q. Exec.*, vol. 17, no. 3, pp. 237–262, 2018.

[86] K. Parsons, A. Mccormac, M. Butavicius, and L. Ferguson, "Human Factors and Information Security : Individual , Culture and Security Environment," *Sci. Technol.*, no. DSTO-TR-2484, p. 45, 2010.

[87] Z. Tu and Y. Yuan, "Critical Success Factors Analysis on Effective Information Security Management: A Literature Review," in *Twentieth Americas Conference on Information Systems*, 2014, pp. 1–13.

[88] J. Van Niekerk and R. Von Solms, "A theory based approach to information security culture change," *Inf.*, vol. 16, no. 6 B, pp. 3907–3930, 2013.

[89] D. Ashenden, "Information Security Management: A Human Challenge?," *Inf. Secur. Tech. Rep.*, vol. 13, no. 4, pp. 195–201, 2008.

[90] R. Oppliger and B. Wildhaber, "Common Misconceptions in Computer and Information Security," *Computer (Long. Beach. Calif).*, vol. 45, no. 6, pp. 102–104, 2012.

[91] R. Ye and L. Feng, "Technical and Economic Models of Information Security," in *2015 International Conference on Computer Science and Applications (Csa)*, 2015, pp. 329–332.

[92] H. S. Rhee, Y. U. Ryu, and C. T. Kim, "Unrealistic optimism on information security management," *Comput. Secur.*, vol. 31, no. 2, pp. 221–232, 2012.

[93] V. Bolek, A. Látecková, A. Romanová, and F. Korcek, "Factors affecting information security focused on SME and agricultural enterprises," *Agris On-line Pap. Econ. Informatics*, vol. 8, no. 4, pp. 37–50, 2016.

[94] K. A. Barton, G. Tejay, M. Lane, and S. Terrell, "Information system security commitment: A study of external influences on senior management," *Comput. Secur.*, vol. 59, pp. 9–25, 2016.

[95] J. F. Van Niekerk and R. Von Solms, "Information security culture: A management perspective," *Comput. Secur.*, vol. 29, no. 4, pp. 476–486, 2010.

[96] C. E. Tu, C. Z., Yuan, Y., Archer, N., & Connelly, "Strategic Value Alignment for Information Security Management: A Critical Success Factor Analysis," *Inf. Comput.*

Secur., vol. 26, no. 2, pp. 150–170, 2018.

[97] R. Herold, *Managing an Information Security and Privacy Awareness and Training Program*, Second Edi. CRC Press, Taylor & Francis Group, 2011.

[98] J. Abbas, H. K. Mahmood, and F. Hussain, "Information Security Management for Small and Medium Size Enterprises," *Sci.Int.(Lahore)*, vol. 27, no. 3, pp. 2393–2398, 2015.

[99] E. Metalidou, C. Marinagi, P. Trivellas, N. Eberhagen, C. Skourlas, and G. Giannakopoulos, "The Human Factor of Information Security: Unintentional Damage Perspective," *Procedia - Soc. Behav. Sci.*, vol. 147, pp. 424–428, 2014.

[100] K. Knapp and C. Ferrante, "Policy Awareness, Enforcement and Maintenance: Critical to Information Security Effectiveness in Organizations," *J. Manag. Policy Pract.*, vol. 13, no. 5, pp. 66–80, 2012.

[101] M. Karlsson, T. Denk, and J. Åström, "Perceptions of organizational culture and value conflicts in information security management," *Inf. Comput. Secur.*, vol. 26, no. 2, pp. 213–229, 2018.

[102] A. Aminnezhad, R. Mahmod, and M. T. Abdullah, "Survey on Economics of Information Security," *Int. J. Comput. Sci. Netw. Secur.*, vol. 16, no. 7, pp. 99–116, 2016.

[103] J. J. C. H. Ryan and D. J. Ryan, "Expected benefits of information security investments," *Comput. Secur.*, vol. 25, pp. 579–288, 2006.

[104] R. B. X. (Robert) Luo, "Investigating security investment impact on firm performance," *Int. J. Account. Inf. Manag.*, vol. 22, no. 3, pp. 194–208, 2014.

[105] P. Ifinedo, "Critical Times for Organizations: What Should Be Done to Curb Workers' Noncompliance With IS Security Policy Guidelines?," *Inf. Syst. Manag.*, vol. 33, no. 1, pp. 30–41, 2016.

[106] L. A. Gordon and M. P. Loeb, "The Economics of Information Security Investment," *ACM Trans. Inf. Syst. Secur.*, vol. 5, no. 4, pp. 438–457, 2002.

[107] K. Haufe, R. Colomo-palacios, and V. Stantchev, "A process framework for information security management," *Inf. J. Inf. Syst. Proj. Manag.*, vol. 4, no. 4, pp. 27–47, 2016.

[108] A. Stewart, "Can spending on information security be justified? Evaluating the security spending decision from the perspective of a rational actor," *Inf. Manag. Comput. Secur.*, vol. 20, no. 4, pp. 312–326, 2012.

[109] C. (Qian) Feng and T. Wang, "Does CIO risk appetite matter? Evidence from information security breach incidents," *Int. J. Account. Inf. Syst.*, vol. 32, no. November, pp. 59–75, 2019.

[110] K. Dunkerley and G. Tejay, "Developing an Information Systems Security Success

Model for eGovernment Context," in *Proceedings of the Fifteenth Americas Conference on Information Systems*, 2009, pp. 1–8.

[111] D. Swinhoe, "The 15 biggest data breaches of the 21st century," *CSO Online*, 2020. [Online]. Available: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html. [Accessed: 11-May-2020].

[112] Deloitte, "The future of cyber survey 2019," 2019.

[113] B. Gardner and V. Thomas, *Building an Information Security Awareness Program*. Syngress, 2014.

[114] L. A. Maglaras *et al.*, "Cyber security of critical infrastructures," *ICT Express*, vol. 4, no. 1, pp. 42–45, 2018.

[115] J. Järveläinen, "IT incidents and business impacts: Validating a framework for continuity management in information systems," *Int. J. Inf. Manage.*, vol. 33, no. 3, pp. 583–590, 2013.

[116] S. C. Hsiao and D. Y. Kao, "The static analysis of WannaCry ransomware," in *International Conference on Advanced Communication Technology, ICACT*, 2018, pp. 153–158.

[117] IBM Security and Ponemon Institute, "Cost of a Data Breach Report 2019," 2019.

[118] J. Davis, "2.9M Patients Impacted by 9-Year Dominion National Hack," *HealthITSecurity*, 2019. [Online]. Available: https://healthitsecurity.com/news/insurer-dominion-national-reports-server-hack-that-began-august-2010. [Accessed: 11-May-2020].

[119] R. J. Robles, M. K. Choi, E. S. Cho, S. S. Kim, G. C. Park, and J. H. Lee, "Common threats and vulnerabilities of critical infrastructures," *Int. J. Control Autom.*, vol. 1, no. 1, pp. 17–22, 2008.

[120] D. Ki-Aries and S. Faily, "Persona-centred information security awareness," *Comput. Secur.*, vol. 70, pp. 663–674, 2017.

[121] EY, "Is cybersecurity about more than protection?," 2019.

[122] Verizon, "Insider Threat Report," 2019.

[123] ENISA, "ENISA Threat Landscape Report 2018," 2019.

[124] M. Chan, I. Woon, and A. Kankanhalli, "Perceptions of Information Security at the Workplace : Linking Information Security Climate to Compliant Behavior Mark Chan National University of Singapore Irene Woon School of Computing , National University of Singapore Atreyi Kankanhalli School of Com," *J. Inf. Priv. Secur.*, vol. 1, no. 3, pp. 18–41, 2005.

[125] E. Humphreys, “Information security management standards: Compliance, governance and risk management,” *Inf. Secur. Tech. Rep.*, vol. 13, no. 4, pp. 247–255, 2008.

[126] C. Pace, “Why HR and IT departments should talk talk,” *Strateg. HR Rev.*, vol. 15, no. 3, pp. 118–122, 2016.

[127] J. D’Arcy and G. Greene, “The Multifaceted Nature of Security Culture and Its Influence on End User Behavior,” in *IFIP TC 8 International Workshop on Information Systems Security Research*, 2009, pp. 145–157.

[128] K. D. Mitnick and W. L. Simon, *The Art of Deception*. Wiley Publishing, Inc., 2002.

[129] J. E. Thomas and G. C. Galligher, “Improving Backup System Evaluations in Information Security Risk Assessments to Combat Ransomware,” *Comput. Inf. Sci.*, vol. 11, no. 1, pp. 14–25, 2018.

[130] K. D. Dunkerley and G. Tejay, “A Confirmatory Analysis of Information Systems Security Success Factors,” in *Proceedings of the 44th Hawaii International Conference on System Sciences*, 2011, pp. 1–10.

[131] U. Hugl and H. Valkanover, “Managing Information Security: The ‘Human Factor’ from the Point of View of IT Professionals, Decision Makers and Scientists,” in *15th Americas Conference on Information Systems, AMCIS*, 2009.

[132] P. Choejey, D. Murray, and C. C. Fung, “Exploring Critical Success Factors for Cybersecurity in Bhutan’S Government Organizations,” in *Eighth International Conference on Networks & Communications*, 2016, no. December, pp. 49–61.

[133] C. G. Reddick, “Management support and information security: an empirical study of Texas state agencies in the USA,” *Electron. Gov. an Int. J.*, vol. 6, no. 4, pp. 361–377, 2009.

[134] A. Kankanhalli, H. H. Teo, B. C. Y. Tan, and K. K. Wei, “An integrative study of information systems security effectiveness,” *Int. J. Inf. Manage.*, vol. 23, no. 2, pp. 139–154, 2003.

[135] R. Von Solms and B. Von Solms, “From policies to culture,” *Comput. Secur.*, vol. 23, no. 4, pp. 275–279, 2004.

[136] H. Yoo, J. H. Lee, and J. Chung, “An analysis of the survey results on nuclear security culture for personnel at nuclear facilities,” *Prog. Nucl. Energy*, vol. 112, no. July 2018, pp. 75–79, 2019.

[137] S. R. Boss, L. J. Kirsch, I. Angermeier, R. A. Shingler, and R. W. Boss, “If someone is watching, I’ll do what I’m asked: Mandatoriness, control, and information security,” *Eur. J. Inf. Syst.*, vol. 18, no. 2, pp. 151–164, 2009.

[138] A. AlHogail and A. Mirza, “A proposal of an organizational information security culture framework,” in *Proceedings of International Conference on Information, Communication Technology and System (ICTS) 2014*, 2014, pp. 243–249.

[139] S. Dojkovski, S. Lichtenstein, and M. J. Warren, “Fostering Information Security Culture in Small and Medium Size Enterprises: An Interpretive Study in Australia,” in *ECIS 2007 Proceedings*, 2007, pp. 1560–1571.

[140] A. Martins and J. Elofe, “Assessing Information Security Culture,” in *Proceedings of the ISSA 2002 Information for Security for South-Africa 2nd Annual Conference*, 2002, pp. 203–214.

[141] F. Al-Izki and G. R. S. Weir, “Management Attitudes Toward Information Security in Omani Public Sector Organisations,” in *Proceedings - 2016 Cybersecurity and Cyberforensics Conference*, 2016, pp. 107–112.

[142] E. Karanja, “The role of the chief information security officer in the management of IT security,” *Inf. Comput. Secur.*, vol. 25, no. 3, pp. 300–329, 2017.

[143] EY, “EY Global Information Security Survey 2020: How does security evolve from bolted on to built-in?,” 2020.

[144] Z. Ahmad, M. Norhashim, O. T. Song, and L. T. Hui, “A typology of employees’ information security behaviour,” in *4th International Conference on Information and Communication Technology, ICoICT 2016*, 2016, pp. 1–4.

[145] ENISA, “Cyber Security Culture in organisations,” 2017.

[146] R. K. Rainer, T. E. Marshall, K. J. Knapp, and G. H. Montgomery, “Do information security professionals and business managers view information security issues differently?,” *Inf. Syst. Secur.*, vol. 16, no. 2, pp. 100–108, 2007.

[147] K. Arbanas and D. Alagić, “Requirements of practice in relation to the existing information technology and security management competencies,” in *Proceedings of the 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2014, pp. 1411–1416.

[148] K. Pažur Aničić, B. Divjak, and K. Arbanas, “Preparing ICT Graduates for Real-World Challenges: Results of a Meta-Analysis,” *IEEE Trans. Educ.*, vol. 60, no. 3, pp. 191–197, 2017.

[149] A. Da Veiga, “The Influence of Information Security Policies on Information Security Culture: Illustrated through a Case Study,” in *Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015) The*, 2015, pp. 22–33.

[150] N. F. Doherty and H. Fulford, “Aligning the Information Security Policy with the Strategic Information Systems Plan,” *Comput. Secur.*, vol. 25, no. 1, pp. 55–63, 2006.

[151] J. Goo, M.-S. Yim, and D. J. Kim, “A Path to Successful Management of Employee Security Compliance: An Empirical Study of Information Security Climate,” *IEEE Trans. Prof. Commun.*, vol. 57, no. 4, pp. 286–308, 2014.

[152] H. M. Al-Mukahal and K. Alshare, “An examination of factors that influence the number of information security policy violations in Qatari organizations,” *Inf. Comput. Secur.*, vol. 23, no. 1, pp. 102–118, 2015.

[153] J. Y. Son, “Out of fear or desire? Toward a better understanding of employees’ motivation to follow IS security policies,” *Inf. Manag.*, vol. 48, no. 7, pp. 296–302, 2011.

[154] T. R. Peltier, “Implementing an information security awareness program,” *Inf. Syst. Secur.*, vol. 14, no. 2, pp. 37–49, 2005.

[155] I. Okere, J. Van Niekerk, and M. Carroll, “Assessing information security culture: A critical analysis of current approaches,” in *2012 Information Security for South Africa - Proceedings of the ISSA 2012 Conference*, 2012, pp. 1–8.

[156] H. Paananen, M. Lapke, and M. Siponen, “State of the art in information security policy development,” *Comput. Secur.*, vol. 88, pp. 1–14, 2020.

[157] S. V. Flowerday and T. Tuyikeze, “Information security policy development and implementation: The what, how and who,” *Comput. Secur.*, vol. 61, pp. 169–183, 2016.

[158] M. P. Buthelezi, J. A. Van Der Poll, and E. O. Ochola, “Ambiguity as a Barrier to Information Security Policy Compliance: A Content Analysis,” in *2016 International Conference on Computational Science and Computational Intelligence Ambiguity*, 2016, pp. 1360–1367.

[159] A. C. Johnston, M. Warkentin, A. R. Dennis, and M. Siponen, “Speak their Language: Designing Effective Messages to Improve Employees’ Information Security Decision Making,” *Decis. Sci.*, vol. 50, no. 2, pp. 245–284, 2019.

[160] A. Martins and J. Elofe, “Information Security Culture,” in *IFIP Advances in Information and Communication Technology*, 2002, pp. 203–214.

[161] A. Da Veiga, “Comparing the information security culture of employees who had read the information security policy and those who had not,” *Inf. Comput. Secur.*, vol. 24, no. 2, pp. 139–151, 2016.

[162] J. Van Niekerk and R. Von Solms, “A holistic framework for the fostering of an information security sub-culture in organizations,” in *Proceedings of the ISSA 2005 New Knowledge Today Conference*, 2005, no. January, pp. 1–13.

[163] J. Van Niekerk and R. von Solms, “Understanding Information Security Culture: A Conceptual Framework,” in *Proceedings of the ISSA 2006 from Insight to Foresight Conference*, 2006, pp. 1–11.

[164] Y. Chen, K. Ramamurthy, and K. W. Wen, “Impacts of comprehensive information security programs on information security culture,” *J. Comput. Inf. Syst.*, vol. 55, no. 3, pp. 11–19, 2015.

[165] A. Koohang, A. Nowak, J. Paliszkiewicz, and J. H. Nord, “Information Security Policy Compliance: Leadership, Trust, Role Values, and Awareness,” *J. Comput. Inf. Syst.*, vol. 60, no. 1, pp. 1–8, 2020.

[166] P. Ifinedo, “Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory,” *Comput. Secur.*, vol. 31, no. 1, pp. 83–95, 2012.

[167] M. Eminağaoğlu, E. Uçar, and Ş. Eren, “The positive outcomes of information security awareness training in companies - A case study,” *Inf. Secur. Tech. Rep.*, vol. 14, no. 4, pp. 223–229, 2009.

[168] X. Chen, D. Wu, L. Chen, and J. K. L. Teng, “Sanction severity and employees’ information security policy compliance: Investigating mediating, moderating, and control variables,” *Inf. Manag.*, vol. 55, no. 8, pp. 1049–1060, 2018.

[169] E. Amankwa, M. Loock, and E. Kritzinger, “A conceptual analysis of information security education, information security training and information security awareness definitions,” in *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)*, 2014, pp. 248–252.

[170] C. Roper, L. Fischer, and J. Grau, *Security Education, Awareness and Training: From Theory to Practice*. Burlington, USA: Elsevier Butterworth-Heinemann, 2006.

[171] D. Tse, Z. Xie, and Z. Song, “Awareness of information security and its implications to legal and ethical issues in our daily life,” in *IEEE International Conference on Industrial Engineering and Engineering Management*, 2017, pp. 1236–1240.

[172] R. S. Shaw, C. C. Chen, A. L. Harris, and H. J. Huang, “The impact of information richness on information security awareness training effectiveness,” *Comput. Educ.*, vol. 52, no. 1, pp. 92–100, 2009.

[173] J. D’Arcy and A. Hovav, “Does one size fit all? Examining the differential effects of IS security countermeasures,” *J. Bus. Ethics*, vol. 89, no. 1, pp. 59–71, 2009.

[174] T. Gundu and S. V Flowerday, “The Enemy Within: A Behavioural Intention Model and an Information Security Awareness Process,” in *2012 Information Security for South*

Africa, 2012, pp. 1–8.

[175] S. Al Awawdeh and A. Tubaishat, "An information security awareness program to address common security concerns in IT unit," in *ITNG 2014 - Proceedings of the 11th International Conference on Information Technology: New Generations*, 2014, pp. 273–278.

[176] B. D. Cone, C. E. Irvine, M. F. Thompson, and T. D. Nguyen, "A video game for cyber security training and awareness," *Comput. Secur.*, vol. 26, no. 1, pp. 63–72, 2007.

[177] G. Stewart and D. Lacey, "Death by a thousand facts: Criticising the technocratic approach to information security awareness," in *Proceedings of the Fifth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2011)*, 2011, pp. 11–21.

[178] W. D. Kearney and H. A. Kruger, "Phishing and organisational learning," *IFIP Adv. Inf. Commun. Technol.*, vol. 405, pp. 379–390, 2013.

[179] T. Schlienger and S. Teufel, "Information security culture – from analysis to change," *South African Comput. J.*, vol. 31, pp. 46–52, 2003.

[180] D. P. Snyman, H. Kruger, and W. D. Kearney, "I shall, we shall, and all others will: paradoxical information security behaviour," *Inf. Comput. Secur.*, vol. 26, no. 3, pp. 290–305, 2018.

[181] S. L. Pfleeger, M. A. Sasse, and A. Furnham, "From weakest link to security hero: Transforming staff security behavior," *J. Homel. Secur. Emerg. Manag.*, vol. 11, no. 4, pp. 489–510, 2014.

[182] J. Anttila and K. Jussila, "Challenges for the Comprehensive and Integrated Information Security Management," in *Proceedings - 13th International Conference on Computational Intelligence and Security, CIS 2017*, 2017, pp. 586–589.

[183] C. Vroom and R. Von Solms, "Towards information security behavioural compliance," *Comput. Secur.*, vol. 23, no. 3, pp. 191–198, 2004.

[184] M. A. Alnatheer, "Information Security Culture Critical Success Factors," in *2015 12th International Conference on Information Technology - New Generations*, 2015, pp. 731–735.

[185] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies," *Comput. Secur.*, vol. 66, pp. 40–51, 2017.

[186] A. Wiley, A. McCormac, and D. Calic, "More than the individual: Examining the relationship between culture and Information Security Awareness," *Comput. Secur.*, vol.

88, p. 101640, 2020.

[187] K. Šolić, K. Nenadić, and D. Galić, “Empirical Study on the Correlation between User Awareness and Information Security,” *Int. J. Electr. Comput. Eng. Syst.*, vol. 3, no. 2, pp. 47–51, 2012.

[188] I. Al-Mayahi and S. P. Mansoor, “Information security culture assessment: Case study,” in *2013 IEEE 3rd International Conference on Information Science and Technology, ICIST 2013*, 2013, pp. 789–792.

[189] B. Lebek, J. Uffen, M. H. Breitner, M. Neumann, and B. Hohler, “Employees’ information security awareness and behavior: A literature review,” in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2013, pp. 2978–2987.

[190] W. Rocha Flores and M. Ekstedt, “Shaping intention to resist social engineering through transformational leadership, information security culture and awareness,” *Comput. Secur.*, vol. 59, pp. 26–44, 2016.

[191] K. Koh, A. B. Ruighaver, S. B. Maynard, and A. Ahmad, “Security governance: Its impact on security culture,” in *Proceedings of 3rd Australian Information Security Management Conference*, 2005, no. January, pp. 47–58.

[192] M. N. Masrek, Q. N. Harun, and M. K. Zaini, “Information Security Culture for Malaysian Public Organization: a Conceptual Framework,” in *4Th International Conference on Education and Social Sciences (Intcess 2017)*, 2017, pp. 156–166.

[193] S. Aurigemma and R. Panko, “A composite framework for behavioral compliance with information security policies,” in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2012, pp. 3248–3257.

[194] I. Hwang, D. Kim, T. Kim, and S. Kim, “Why not comply with information security? An empirical approach for the causes of non-compliance,” *Manag. Environ. Qual. An Int. J.*, vol. 41, no. 1, pp. 2–18, 2017.

[195] M. A. Noureddine, A. Marturano, K. Keefe, M. Bashiry, and W. H. Sanders, “Accounting for the human user in predictive security models,” in *Proceedings of IEEE Pacific Rim International Symposium on Dependable Computing, PRDC*, 2017, pp. 329–338.

[196] L. Li, W. He, L. Xu, A. Ivan, M. Anwar, and X. Yuan, “Does explicit information security policy affect employees’ cyber security behavior? A pilot study,” in *Proceedings - 2nd International Conference on Enterprise Systems, ES 2014*, 2014, pp. 169–173.

[197] E. Sherif and S. Furnell, “A Conceptual Model for Cultivating an Information Security

Culture," *Int. J. Inf. Secur. Res.*, vol. 5, no. 2, pp. 565–573, 2015.

[198] P. A. Chia, S. B. Maynard, and A. B. Ruighaver, "Exploring Organisational Security Culture: Developing a comprehensive research model," in *IS ONE World Conference*, 2002, no. April, pp. 1–13.

[199] T. Herath and H. R. Rao, "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness," *Decis. Support Syst.*, vol. 47, no. 2, pp. 154–165, 2009.

[200] S. Pahnila, M. Siponen, and A. Mahmood, "Employees' Behavior towards IS Security Policy Compliance," in *40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, 2007.

[201] N. S. Safa *et al.*, "Deterrence and prevention-based model to mitigate information security insider threats in organisations," *Futur. Gener. Comput. Syst.*, vol. 97, pp. 587–597, 2019.

[202] Y. Xue, H. Liang, and L. Wu, "Punishment, justice, and compliance in mandatory IT settings," *Inf. Syst. Res.*, vol. 22, no. 2, pp. 400–414, 2011.

[203] A. Greig, K. Renaud, and S. Flowerday, "An ethnographic study to assess the enactment of information security culture in a retail store," in *2015 World Congress on Internet Security, WorldCIS 2015*, 2015, pp. 61–66.

[204] Angraini, R. A. Alias, and Okfalisa, "Information security policy compliance: Systematic literature review," *Procedia Comput. Sci.*, vol. 161, pp. 1216–1224, 2019.

[205] E. Albrechtsen, "A qualitative study of users' view on information security," *Comput. Secur.*, vol. 26, no. 4, pp. 276–289, 2007.

[206] M. Siponen, S. Pahnila, and M. A. Mahmood, "Compliance with Information Security Policies: An Empirical Investigation," *Computer (Long. Beach. Calif).*, vol. 43, no. 2, pp. 64–71, 2010.

[207] E. Amankwa, M. Loock, and E. Kritzinger, "Establishing information security policy compliance culture in organizations," *Inf. Comput. Secur.*, vol. 26, no. 4, pp. 420–436, 2018.

[208] H. Thompson, "The Human Element of Information Security," *IEEE Secur. Priv. Mag.*, vol. 11, no. 1, pp. 32–35, 2013.

[209] R. M. Åhlfeldt, P. Spagnoletti, and G. Sindre, "Improving the information security model by using TFI," in *IFIP International Federation for Information Processing*, vol. 232, Springer, 2007, pp. 73–84.

[210] H. F. Cervone, "Information doesn't always want to be free: An overview of regulations

affecting information security," *Digit. Libr. Perspect.*, vol. 32, no. 2, pp. 68–72, 2016.

[211] Europski parlament i Vijeće Europske Unije, "Direktiva (EU) 2016/1148 - Direktiva o sigurnosti mrežnih i informacijskih sustava," *Službeni List Eur. unije*, vol. 194, pp. 1–30, 2016.

[212] The Parliamentary Office of Science and Technology, "Cyber Security of UK Infrastructure," *Postnote*, no. 554. pp. 1–6, 2017.

[213] Europski parlament i Vijeće Europske Unije, "Uredba (EU) 2016/679 - Opća uredba o zaštiti podataka," *Službeni List Eur. unije*, vol. 119, pp. 1–88, 2016.

[214] Europski parlament i Vijeće europske unije, "Uredba (EU) 2019/881 Akt o kibersigurnosti," *Službeni List Eur. unije*, vol. 151, pp. 15–69, 2019.

[215] Hrvatski sabor, "Zakon o informacijskoj sigurnosti," *Nar. novine 79/07*, 2007.

[216] Hrvatski sabor, "Zakon o tajnosti podataka," *Nar. novine 79/07, 86/12*, 2007.

[217] Hrvatski sabor, "Zakon o zaštiti tajnosti podataka," *Nar. novine 108/96*, 1996.

[218] Hrvatski sabor, "Zakon o provedbi Opće uredbe o zaštiti podataka," *Nar. novine 42/18*, 2018.

[219] Hrvatski sabor, "Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga," *Nar. novine 64/18*, 2018.

[220] Payment Card Industry (PCI) Data Security Standard, "Payment Card Industry Data Security Standard (PCI DSS) - Requirements and Security Assessment Procedures," *PCI Security Standards Council*. 2018.

[221] K. Harisaiprasad, "COBIT 2019 and COBIT 5 Comparison," *COBIT focus newsletters*, 2020. [Online]. Available: https://www.isaca.org/resources/news-and-trends/newsletters/cobit-focus/2020/cobit-2019-and-cobit-5-comparison.

[222] ISACA, "COBIT 2019 Framework: Governance and Management Objectives," 2018.

[223] S. Thacker, S. Barr, R. Pant, J. W. Hall, and D. Alderson, "Geographic Hotspots of Critical National Infrastructure," *Risk Anal.*, vol. 37, no. 12, pp. 2490–2505, 2017.

[224] A. Jones, "Critical infrastructure protection," *Comput. Fraud Secur.*, no. April, pp. 11–15, 2007.

[225] ISO/IEC, "ISO/IEC 27019 -Information technology - Security techniques - Information security controls for the energy utility industry." 2017.

[226] Vijeće Europske Unije, "Direktiva Vijeća 2008/114/EZ o utvrđivanju i označivanju europske kritične infrastrukture i procjeni potrebe poboljšanja njezine zaštite," *Službeni List Eur. unije*, vol. 18, no. 3, pp. 172–179, 2008.

[227] Hrvatski sabor, "Zakon o kritičnim infrastrukturama," *Nar. novine 56/13*, 2013.

[228] Centre for the Protection of National Infrastructure, “Critical National Infrastructure,” 2020. [Online]. Available: https://www.cpni.gov.uk/critical-national-infrastructure-0. [Accessed: 26-May-2020].

[229] Federal Republic of Germany, “National Strategy for Critical Infrastructure Protection (CIP Strategy).” 2009.

[230] The White House, “Presidential Policy Directive (PPD/21) Critical Infrastructure Security and Resilience,” 2013. [Online]. Available: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil. [Accessed: 26-May-2020].

[231] Her Majesty the Queen in Right of Canada, “National Strategy for Critical Infrastructure.” 2009.

[232] Vlada Republike Hrvatske, “Odluka o određivanju sektora iz kojih središnja tijela državne uprave identificiraju nacionalne kritične infrastrukture te liste redoslijeda sektora kritičnih infrastruktura,” *Nar. novine 108/2013*, 2013.

[233] Ured Vijeća za nacionalnu sigurnost, “Izvješće o provedbi akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti u 2017. godini,” 2018.

[234] Vlada Republike Hrvatske, “Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga,” *Nar. novine 68/18*, 2018.

[235] Ured Vijeća za nacionalnu sigurnost, “Izvješće o provedbi akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti u 2018. godini,” 2019.

[236] World Economic Forum, “The Global Risks Report 2020,” 2020.

[237] S. Mansfield-Devine, “Critical infrastructure: understanding the threat,” *Comput. Fraud Secur.*, no. July, pp. 16–20, 2018.

[238] Robert M. Lee, Michael J. Assante, and Tim Conway, “Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case,” *Electricity Information Sharing and Analysis Center (E-ISAC)*. 2016.

[239] ENISA, “ENISA Threat Landscape Report 2017,” 2018.

[240] T. Seals, “NotPetya Linked to Industroyer Attack on Ukraine Energy Grid,” *Threatpost.com*, 2018. [Online]. Available: https://threatpost.com/notpetya-linked-to-industroyer-attack-on-ukraine-energy-grid/138287/. [Accessed: 26-May-2020].

[241] A. Greenberg, “The Untold Story of NotPetya, the Most Devastating Cyberattack in History,” *Wired.com*, 2018. [Online]. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/. [Accessed: 26-May-2020].

[242] B. Ivezić, “Love ih policija i stručnjaci iz SAD-a: Kibernetički kriminalci ucijenili Inu

za 100 milijuna kuna?," *Poslovni.hr*, 2020. [Online]. Available: https://www.poslovni.hr/kolumne/velike-kompanije-u-strahu-zbog-ucjena-kibernetickih-kriminalaca-4215239. [Accessed: 26-May-2020].

[243] Poslovni.hr, "Iz grada Đakova prevarantu uplatili 50.000 eura, nije im palo na pamet da provjere vrlo sumnjivo ime," 2018. [Online]. Available: https://www.poslovni.hr/hrvatska/iz-grada-akova-prevarantu-uplatili-50000-eura-nije-im-palo-na-pamet-da-provjere-vrlo-sumnjivo-ime-344950. [Accessed: 14-Apr-2020].

[244] A. Nasir, R. Abdullah Arshah, and M. R. Ab Hamid, "A dimension-based information security culture model and its relationship with employees' security behavior: A case study in Malaysian higher educational institutions," *Inf. Secur. J.*, vol. 28, no. 3, pp. 55–80, 2019.

[245] A. Da Veiga and J. H. P. Eloff, "A framework and assessment instrument for information security culture," *Comput. Secur.*, vol. 29, no. 2, pp. 196–207, 2010.

[246] T. Gebrasilase and L. F. Lessa, "Information Security Culture in Public Hospitals: The Case of Hawassa Referral Hospital," *African J. Inf. Syst.*, vol. 3, no. 3, p. 1, 2011.

[247] D. D. Warrick, "What leaders need to know about organizational culture," *Bus. Horiz.*, vol. 60, no. 3, pp. 395–404, 2017.

[248] K. J. Knapp, T. E. Marshall, R. K. Rainer, and F. N. Ford, "Information security: Management's effect on culture and policy," *Inf. Manag. Comput. Secur.*, vol. 14, no. 1, pp. 24–36, 2006.

[249] F. Nel and L. Drevin, "Key elements of an information security culture in organisations," *Inf. Comput. Secur.*, vol. 27, no. 2, pp. 146–164, 2019.

[250] M. N. Masrek, "Assessing information security culture: The case of Malaysia public organization," in *4th International Conference on Information Technology, Computer, and Electrical Engineering*, 2017, pp. 1–1.

[251] M. Mokwetli and T. Zuva, "Adoption of the ICT Security Culture in SMME's in the Gauteng Province, South Africa," in *2018 International Conference on Advances in Big Data, Computing and Data Communication Systems, icABCD 2018*, 2018, pp. 1–7.

[252] A. Mahfuth, S. Yussof, A. A. Bakar, B. Ali, and W. Abdallah, "A Conceptual Model for Exploring the Factors Influencing Information Security Culture," *Int. J. Secur. Its Appl.*, vol. 11, no. 5, pp. 15–26, 2017.

[253] A. Al Hogail, "Cultivating and Assessing an Organizational Information Security Culture; an Empirical Study," *Int. J. Secur. Its Appl.*, vol. 9, no. 7, pp. 163–178, 2015.

[254] M. Alnatheer and K. Nelson, "A proposed framework for understanding Information

Security culture and practices in the Saudi context," in *Proceedings of the 7th Australian Information Security Management Conference*, 2009, no. December, pp. 6–17.

[255] F. Karlsson, J. Åström, and M. Karlsson, *Information security culture state-of-the-art review between 2000 and 2013*, vol. 23, no. 3. 2015.

[256] N. H. Hassan, Z. Ismail, and N. Maarop, "Information Security Culture: A Systematic Literature Review," in *Proceedings of the 5th International Conference on Computing and Informatics*, 2015, pp. 456–463.

[257] A. da Veiga, L. V. Astakhova, A. Botha, and M. Herselman, "Defining organisational information security culture—Perspectives from academia and industry," *Comput. Secur.*, vol. 92, p. 101713, 2020.

[258] A. AlHogail and A. Mirza, "Organizational Information Security Culture Assessment," in *The 2015 International Conference on Security and Management*, 2015, pp. 286–292.

[259] T. Schlienger and S. Teufel, "Analyzing information security culture: Increased trust by an appropriate information security culture," in *Proceedings - International Workshop on Database and Expert Systems Applications, DEXA*, 2003, pp. 405–409.

[260] S. Ramachandran and S. V. Rao, "Security cultures in organizations: A theoretical model," in *Proceedings of the Twelfth Americas Conference on Information Systems*, 2006, vol. 6, pp. 3460–3464.

[261] S. Alfawaz, K. Nelson, and K. Mohannak, "Information security culture: A behaviour compliance conceptual framework," in *Australasian Information Security Conference (AISC)*, 2010, pp. 51–60.

[262] J. A. Chatman and S. E. Cha, "Leading by leveraging culture," *Calif. Manage. Rev.*, vol. 45, no. 4, 2003.

[263] J. Malcolmson, "What is Security Culture? Does it differ in content from general Organisational Culture?," in *Proceedings - International Carnahan Conference on Security Technology*, 2009, pp. 361–366.

[264] A. Tolah, S. M. Furnell, and M. Papadaki, "A Comprehensive Framework for Cultivating and Assessing Information Security Culture," *Elev. Int. Symp. Hum. Asp. Inf. Secur. Assur.*, no. HAISA 2017, pp. 52–64, 2017.

[265] N. H. Hassan and Z. Ismail, "Information security culture in healthcare informatics: A preliminary investigation," *J. Theor. Appl. Inf. Technol.*, vol. 88, no. 2, pp. 202–209, 2016.

[266] A. AlKalbani, H. Deng, and B. Kam, "Organisational security culture and information security compliance for e-government development: The moderating effect of social

pressure," in *Pacific Asia Conference on Information Systems, PACIS 2015 - Proceedings*, 2015.

[267] A. Da Veiga and N. Martins, "Information security culture and information protection culture: A validated assessment instrument," *Comput. Law Secur. Rev.*, vol. 31, no. 2, pp. 243–256, 2015.

[268] G. Dhillon, R. Syed, and C. Pedron, "Interpreting information security culture: An organizational transformation case study," *Comput. Secur.*, vol. 56, pp. 63–69, 2016.

[269] S. Govender;, E. Kritzinger;, and M. Loock, "The Influence of National Culture on Information Security Culture," in *IST-Africa Week Conference*, 2016, pp. 1–9.

[270] N. Martins and A. Da Veiga, "An Information security culture model validated with structural equation modelling," in *Proceedings of the 9th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2015*, 2015, no. July, pp. 11–21.

[271] A. Ahmad, K. C. Desouza, S. B. Maynard, H. Naseer, and R. L. Baskerville, "How integration of cyber security management and incident response enables organizational learning," *J. Assoc. Inf. Sci. Technol.*, pp. 1–15, 2019.

[272] O. S. Ibidunni and A. G. Mayowa, "Predicting Performance through the Elements of Organizational Culture," *Arch. Bus. Res.*, vol. 2, no. 6, pp. 62–82, 2014.

[273] S. Ramachandran, S. V. Rao, and T. Goles, "Information security cultures of four professions: A comparative study," in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2008, pp. 1–10.

[274] S. Ramachandran, C. Rao, T. Goles, and G. Dhillon, "Variations in information security cultures across professions: A qualitative study," *Commun. Assoc. Inf. Syst.*, vol. 33, no. 1, pp. 163–204, 2013.

[275] E. Kummerow and N. Kirby, *Organisational Culture: Concept, Context and Measurement (Two Volumes)*. World Scientific Publishing Co. Pte. Ltd., 2014.

[276] E. H. Schein, *Organizational Culture and Leadership*. San Francisco, CA, USA: Jossey-Bass, 1985.

[277] E. H. Schein, *Organizational Culture and Leadership*, Fourth Edi. Jossey-Bass, 2010.

[278] E. H. Schein and P. Schein, *Organizational Culture and Leadership*, Fifth Edit. John Wiley & Sons, Inc., 2017.

[279] E. H. Schein, *Corporate Culture Survival Guide*, Second Edi. Jossey-Bass, 2009.

[280] J. R. Detert, R. G. Schroeder, and J. J. Mauriel, "A Framework for Linking Culture and Improvement Initiatives in Organizations," *Acad. Manag. Rev.*, vol. 25, no. 4, pp. 850–

863, 2000.

[281] P. Chia, S. B. Maynard, and A. B. Ruighaver, “Understanding Organisational Security Culture,” in *Information Systems: The Challenges of Theory and Practice*, 2003, pp. 335–365.

[282] B. Lebek, J. Uffen, M. Neumann, B. Hohler, and M. H. Breitner, “Information security awareness and behavior: a theory-based literature review,” *Manag. Res. Rev.*, vol. 37, no. 12, pp. 1049–1092, 2014.

[283] J. D’Arcy and T. Herath, “A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings,” *Eur. J. Inf. Syst.*, vol. 20, pp. 643–658, 2011.

[284] J. D’Arcy, A. Hovav, and D. Galletta, “User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach,” *Inf. Syst. Res.*, vol. 20, no. 1, pp. 79–98, 2009.

[285] A. C. Johnston and M. Warkentin, “Fear Appeals and Information Security Behaviors: An Empirical Study,” *MIS Q.*, vol. 34, no. 3, pp. 549–566, 2010.

[286] J. Lee and Y. Lee, “A holistic model of computer abuse within organizations,” *Inf. Manag. Comput. Secur.*, vol. 10, no. 2, pp. 57–63, 2002.

[287] A. Nasir, R. A. Arshah, M. R. A. Hamid, and S. Fahmy, “An analysis on the dimensions of information security culture concept: A review,” *J. Inf. Secur. Appl.*, vol. 44, pp. 12–22, 2019.

[288] M. Alnatheer, T. Chan, and K. Nelson, “Understanding and measuring information security culture,” in *Proceedings - Pacific Asia Conference on Information Systems, PACIS 2012*, 2012.

[289] S. Kraemer and P. Carayon, “Computer and information security culture: Findings from two studies,” in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 2005, pp. 1483–1487.

[290] S. Dojkovski, S. Lichtenstein, and M. Warren, “Challenges in fostering an information security culture in Australian small and medium sized enterprises,” in *Proceedings of the 5th European conference on Information Warfare and Security*, 2006, pp. 31–40.

[291] S. Dojkovski, S. Lichtenstein, and M. Warren, “Developing information security culture in small and medium size enterprises: Australian case studies,” in *6th European Conference on Information Warfare and Security 2007, ECIW 2007*, 2007, pp. 55–65.

[292] S. Dojkovski, S. Lichtenstein, and M. J. Warren, “Enabling information security culture: Influences and challenges for Australian SMEs,” in *ACIS 2010 Proceedings - 21st*

Australasian Conference on Information Systems, 2010.

[293] J. S. Lim, A. Ahmad, S. Chang, and S. Maynard, "Embedding Information Security Culture Emerging Concerns and Challenges," in *PACIS 2010 Proceedings*, 2010, no. January, pp. 463–474.

[294] N. Martins and A. Da Veiga, "The Value of Using a Validated Information Security Culture Assessment Instrument," in *8th European Conference on IS Management and Evaluation*, 2014, no. 8, pp. 146–154.

[295] A. Tkalac Verčić, D. Sinčić Ćorić, and N. Pološki Vokić, *Priručnik za metodologiju istraživačkog rada*. Zagreb: M.E.P. d.o.o., 2010.

[296] J. W. Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, 4th Editio. SAGE Publications, 2014.

[297] J. W. Creswell, *Educational Research*, Fourth Edi. 2012.

[298] A. Dickson, J. A. Agyem, and E. K. Hussein, "Theoretical and Conceptual Framework: Mandatory Ingredients of a Quality Research," *Int. J. Sci. Res.*, vol. 7, no. 1, pp. 93–98, 2018.

[299] G. L. Polites, N. Roberts, and J. Thatcher, "Conceptualizing models using multidimensional constructs: A review and guidelines for their use," *Eur. J. Inf. Syst.*, vol. 21, no. 1, pp. 22–48, 2012.

[300] M. Mejovšek, *Metode znanstvenog istraživanja u društvenim i humanističkim znanostima*. Naklada Slap200, 2008.

[301] M. Žugaj, *Znanstvena istraživanja u društvenim znanostima i nastanak znanstvenog djela*. Tonimir, 2007.

[302] G. C. Moore and I. Benbasat, "Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation Stable," *Inf. Syst. Res.*, vol. 2, no. 3, pp. 192–222, 1991.

[303] D. Sedera, G. Gable, and T. Chan, "Measuring enterprise systems success: A preliminary model," in *Proceedings of the 9th Americas Conference on Information Systems (AMCIS 2003)*, 2003, pp. 476–485.

[304] J. F. Hair, W. C. Black, B. J. Babin, R. E. Anderson, J. Liang, and F. Chen, *Multivariate Data Analysis*, Seventh ed. Pearson Prentice Hall, 2010.

[305] P. C. Cozby and S. C. Bates, *Methods in Behavioral Research*, Eleventh E. McGraw Hill, 2012.

[306] D. Straub, M.-C. Boudreau, and D. Gefen, "Validation Guidelines for IS Positivist Research," *Commun. Assoc. Inf. Syst.*, vol. 13, no. 1, Mar. 2004.

[307] A. Field, *Discovering Statistics Using IBM SPSS Statistics*, 4th Editio. SAGE Publications, 2013.

[308] C. H. Lawshe, "A Quantitative Approach To Content Validity," *Pers. Psychol.*, vol. 28, no. 4, pp. 563–575, 1975.

[309] B. R. Lewis, C. A. Snyder, and R. K. Rainer, "An empirical assessment of the information resource management construct," *J. Manag. Inf. Syst.*, vol. 12, no. 1, pp. 199–223, 1995.

[310] N. J. Salkind, Ed., *Encyclopedia of Research Design - Volume 1*. SAGE Publications, 2010.

[311] A. Y. Nahm, S. S. Rao, L. E. Solis-Galvan, and T. S. Ragu-Nathan, "The Q-Sort Method: Assessing Reliability And Construct Validity Of Questionnaire Items At A Pre-Testing Stage," *J. Mod. Appl. Stat. Methods*, vol. 1, no. 1, pp. 114–125, 2002.

[312] Stacie Petter, D. Straub, and A. Rai, "Specifying Formative Constructs in Information Systems Research," *MIS Q.*, vol. 31, no. 4, pp. 623–656, 2007.

[313] J. F. Hair, G. T. M. Hult, C. M. Ringle, and M. Sarstedt, *A Primer on Partial Least Squares Structural Equation Modeling*. SAGE Publications, 2014.

[314] J. L. Fleiss, "Measuring Nominal Scale Agreement Among Many Raters," *Psychol. Bull.*, vol. 76, no. 5, pp. 378–382, 1971.

[315] J. R. Landis and G. G. Koch, "The Measurement of Observer Agreement for Categorical Data," *Biometrics*, vol. 33, no. 1, pp. 159–174, 1977.

[316] D. G. Altman, *Practical statistics for medical research*. 1991.

[317] L. J. Cronbach, "Coefficient alpha and the internal structure of tests," *Psychometrika*, vol. 16, no. 3, pp. 297–334, 1951.

[318] A. E. Hurley *et al.*, "Exploratory and confirmatory factor analysis: Guidelines, issues, and alternatives," *J. Organ. Behav.*, vol. 18, pp. 667–683, 1997.

[319] P. Brewerton and L. Millward, *Organizational Research Methods*. SAGE Publications, 2001.

[320] D. Gefen and D. Straub, "A Practical Guide To Factorial Validity Using PLS-Graph: Tutorial And Annotated Example," *Commun. Assoc. Inf. Syst.*, vol. 16, no. July, 2005.

[321] R. C. MacCallum, K. F. Widaman, S. Zhang, and S. Hong, "Sample size in factor analysis," *Psychol. Methods*, vol. 4, no. 1, pp. 84–99, 1999.

[322] J. F. Hair, W. C. Black, B. J. Babin, and R. E. Anderson, *Multivariate Data Analysis*. Cengage Learning EMEA, 2019.

[323] R. B. Cattel, *The Scientific Use if Factor Analysis in Behavioral and Life Sciences*.

Plenum Press, 1978.

[324] P. Samuels, “Advice on Exploratory Factor Analysis.” Centre for Academic Success, Birmingham City University, 2017.

[325] J. Pallant, *SPSS Survival Manual: A step by step guide to data analysis using SPSS for Windows (Version 12)*. 2005.

[326] B. G. Tabachnick and L. S. Fidell, *Using Multivariate Statistics*, Sixth Edit. Pearson Education, 2013.

[327] J. W. Osborne and A. B. Costello, “Best Practices in Exploratory Factor Analysis: Four Recommendations for Getting the Most From Your Analysis,” *Pract. assesment, Res. Eval.*, vol. 10, no. 7, pp. 1–9, 2005.

[328] K. A. Yeomans and P. A. Golder, “The Guttman-Kaiser Criterion as a Predictor of the Number of Common Factors,” *J. R. Stat. Soc.*, vol. 31, no. 3, p. 221, 1982.

[329] R. B. Cattell, “Multivariate Behavioral Translator disclaimer The Scree Test For The Number Of Factors,” *Multivariate Behav. Res.*, vol. 1, no. 2, pp. 245–276, 1966.

[330] A. L. Comrey, *A First Course in Factor Analysis*, Second Edi. Psychology Press, 1992.

[331] M. W. Watkins, “Exploratory Factor Analysis: A Guide to Best Practice,” *J. Black Psychol.*, vol. 44, no. 3, pp. 219–246, 2018.

[332] L. R. Fabrigar and D. T. Wegener, *Exploratory Factor Analysis*. Oxford University Press, 2012.

[333] N. H. Hassan, N. Maarop, Z. Ismail, and W. Z. Abidin, “Information security culture in health informatics environment: A qualitative approach,” in *International Conference on Research and Innovation in Information Systems, ICRIIS*, 2017, pp. 1–6.

[334] A. Nasir, R. A. Arshah, and M. R. Ab Hamid, “Information Security Policy Compliance Behavior Based on Comprehensive Dimensions of Information Security Culture,” in *Proceedings of the 2017 International Conference on Information System and Data Mining*, 2017, pp. 56–60.

[335] A. da Veiga, N. Martins, and J. H. P. Eloff, “Information security culture – validation of an assessment instrument,” *South African Bus. Rev.*, vol. 11, no. 1, pp. 147–166, 2007.

[336] A. da Veiga and N. Martins, “Defining and identifying dominant information security cultures and subcultures,” *Comput. Secur.*, vol. 70, pp. 72–94, 2017.

[337] Z. Ruhwanya and J. Ophoff, “Information Security Culture Assessment of Small and Medium-Sized Enterprises in Tanzania,” in *International Conference on Social Implications of Computers in Developing Countries*, 2019, vol. 551, pp. 776–788.

[338] J. D’Arcy and G. Greene, “Security culture and the employment relationship as drivers

of employees' security compliance," *Inf. Comput. Secur.*, vol. 22, no. 5, pp. 474–489, 2014.

[339] A. Alhogail and A. Mirza, "Information security culture: A definition and a literature review," in *2014 World Congress on Computer Applications and Information Systems, WCCAIS 2014*, 2014.

[340] S. Labovitz, "The Assignment of Numbers to Rank Order Categories," *Am. Sociol. Rev.*, vol. 35, no. 3, pp. 515–524, 1970.

[341] Hrvatski sabor, "Zakon o pravu na pristup informacijama," *Nar. novine 25/13, 85/15*, 2013.

[342] E. Babbie, *The Practice of Social Research*, 14th editi. Cengage Learning, 2014.

[343] L. Cohen, L. Manion, and K. Morrison, *Research Methods in Education*, Sixth Edit. 2007.

[344] E. Yeniman Yildirim, G. Akalp, S. Aytac, and N. Bayram, "Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey," *Int. J. Inf. Manage.*, vol. 31, no. 4, pp. 360–365, 2011.

[345] M. Qingxiong, A. C. Johnston, and J. M. Pearson, "Information security management objectives and practices: A parsimonious framework," *Inf. Manag. Comput. Secur.*, vol. 16, no. 3, pp. 251–270, 2008.

[346] K. D. Dunkerley, "Developing an Information Systems Security Success Model for Organizational Context," Graduate School of Computer and Information Sciences Nova Southeastern University, 2011.

[347] N. Humaidi and V. Balakrishnan, "Indirect effect of management support on users' compliance behaviour towards information security policies," *Heal. Inf. Manag. J.*, vol. 47, no. 1, pp. 1–11, 2018.

[348] K. J. Knapp, F. N. Ford, T. E. Marshall, and R. K. Rainer, "Information security Effectiveness: conceptualization and Validation of a theory," 2007.

[349] J. Y. Han, Y. J. Kim, and H. Kim, "An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective," *Comput. Secur.*, vol. 66, no. 2017, pp. 52–65, 2017.

[350] R. E. Pierce, "Key factors in the success of an organization's information security culture: A quantitative study and analysis," Capella University, 2012.

[351] N. S. Safa and R. Von Solms, "An information security knowledge sharing model in organizations," *Comput. Human Behav.*, vol. 57, pp. 442–451, 2016.

PRILOZI

Prilog 1. Čestice mjernog instrumenta

Tablica 9.1. Čestice mjernog instrumenta prije i nakon validacije od strane eksperata

Rbr.	Oznaka	Čestica[13]	Izvor	Napomena
1	EDU1	Ako imam priliku, sudjelovat ću na edukacijama i radionicama vezanim uz informacijsku sigurnost	Prilagođeno prema: [152]	
2	EDU10	Ako ja ne pridajem dovoljno pažnje odredbama politike informacijske sigurnosti, informacijska imovina moje organizacije je podložna riziku	Prilagođeno prema: [77]	
3	BHV1	Ako poštujem pravila vezana uz informacijsku sigurnost, mogu pomoći u zaštiti informacijske imovine svoje organizacije	Prilagođeno prema: [199]	
4	POL8	Ako se otkrije da sam kršio/la organizacijske politike informacijske sigurnosti bit ću kažnjen/a	Prilagođeno prema: [67]	
5	AV1	Antivirusni sustav barem jednom tjedno skenira moje računalo	Prilagođeno prema: [153]	
6	AV2	Antivirusni sustav instaliran na mom računalu redovito se ažurira	Prilagođeno prema: [153]	
7	AV3	Antivirusni sustav koji se redovito ažurira i održava značajno doprinosi zaštiti informacijskog sustava	Prilagođeno prema: [344]	
8	AV4	Antivirusni sustav neophodan je za moju organizaciju	Prilagođeno prema: [345]	
9	EDU11	Čak i ako mogu, ne smijem isključiti antivirusni program na svom računalu	Autor	
10	EDU12	Često ostavljam svoje računalo otključano kad napuštam radno mjesto	Prilagođeno prema: [152]	
11	EDU2	Edukacije vezane uz informacijsku sigurnost koje nudi moja organizacija su korisne	Preuzeto iz: [69]	
12		Etičnost zaposlenika nema značajan utjecaj na informacijsku sigurnost	Prilagođeno prema: [346]	Čestica isključena jer je većinski svrstana u čimbenik ETIČNOST koji je isključen jer ne zadovoljava kriterij za n = 11; CVR > 0,59 (CVR = 0,45)

[13] Ponuđeni odgovori na pitanja rbr. 1-97, 106-107 su: (1) u potpunosti se ne slažem; (2) uglavnom se ne slažem; (3) niti se slažem niti ne slažem; (4) uglavnom se slažem; (5) u potpunosti se slažem; n/p - nije primjenjivo u mojoj organizaciji. Ponuđeni odgovori na pitanja rbr. 98-103 su: (1) uopće ne; (2) rijetko; (3) nekoliko puta; (4) često; (5) vrlo često. Ponuđeni odgovori na pitanja rbr. 104-105 su: (1) 0 puta; (2) 1 put; (3) 2 puta; (4) 3 puta; (5) 4 i više puta

Rbr.	Oznaka	Čestica[13]	Izvor	Napomena
13	AV5	Implementacija antivirusne zaštite neophodna je za svaku organizaciju koja u svom poslovanju koristi informacijske sustave	Prilagođeno prema: [345]	
14	AA1	Informacije trebaju biti zaštićene od neovlaštene upotrebe (čitanja, izmjene, brisanja)	Preuzeto iz: [345]	
15		Informacijska sigurnost je gubitak vremena i novca	Preuzeto iz: [346]	Čestica isključena jer ne zadovoljava kriterij za n = 11; CVR > 0,59 (CVR = 0,09)
16	BLF1	Informacijski sustav moje organizacije siguran je toliko koliko ga ja činim sigurnim	Preuzeto iz: [137]	
17		Kako bih brže obavio svoj posao, voljan sam preuzeti rizik nepoštivanja smjernica vezanih uz informacijsku sigurnost	Prilagođeno prema: [67]	Čestica isključena jer je većinski svrstana u čimbenik ETIČNOST koji je isključen jer ne zadovoljava kriterij za n = 11; CVR > 0,59 (CVR = 0,45)
18	CMP1	Kao zaposlenik/ca, imam korist od usklađenosti s pravilima vezanim uz informacijsku sigurnost u mojoj organizaciji	Prilagođeno prema: [77]	
19	CMP2	Moja organizacija provodi periodične provjere radi utvrđivanja usklađenosti sa politikom informacijske sigurnosti	Prilagođeno prema: [67]	
20	BCK1	Moja organizacija redovito provodi izradu sigurnosne kopije (eng. backup) bitnih poslovnih informacija kako bi se smanjila vjerojatnost gubitka podataka	Prilagođeno prema: [60]	
21	POL1	Moja organizacija uspostavila je pravila ponašanja vezanih uz korištenje informacijske imovine	Prilagođeno prema: [67]	
22		Moje nagrađivanje u organizaciji vezano je uz moje poštivanje politike informacijske sigurnosti	Prilagođeno prema: [77]	Čestica isključena jer ne zadovoljava kriterij za n = 11; CVR > 0,59 i AVRI <= 2,00 (CVR = 0,27; AVRI = 2,36)
23	POL12	Namjeravam štititi informacijsku imovinu moje organizacije sukladno odredbama sigurnosne politike	Preuzeto iz: [77]	
24	EDU13	Neću otkriti svoju lozinku za pristup računalu nikome pa čak ni svom nadređenom	Prilagođeno prema: [190]	
25		Nije teško poštivati odredbe sigurnosne politike	Preuzeto iz: [152]	Čestica isključena jer ne zadovoljava kriterij za n = 11; CVR > 0,59 (CVR = 0,27)
26		Nije važno bilježiti tko pristupa kritičnim informacijskim sustavima	Preuzeto iz: [346]	Čestica isključena jer nije bilo konsenzusa između eksperata u svrstavanju čestice većinski u jedan čimbenik

Rbr.	Oznaka	Čestica[13]	Izvor	Napomena
27		Obraćam pažnju na informacijsku sigurnost tijekom dnevnih aktivnosti	Preuzeto iz: [137]	Čestica isključena jer nije bilo konsenzusa između eksperata u svrstavanju čestice većinski u jedan čimbenik
28	EDU14	Osjećam se pouzdano u svoje razumijevanje sigurnosne politike u mojoj organizaciji	Preuzeto iz: [347]	
29		Pogrešno je kršiti odredbe sigurnosne politike, čak i ako mogu proći nekažnjeno	Preuzeto iz: [153]	Čestica isključena jer je većinski svrstana u čimbenik ETIČNOST koji je isključen jer ne zadovoljava kriterij za n = 11; CVR > 0,59 (CVR = 0,45)
30	POL2	Politika informacijske sigurnosti jasno definira ciljeve informacijske sigurnosti moje organizacije	Preuzeto iz: [69]	
31	POL3	Politika informacijske sigurnosti jasno ističe važnost informacijske sigurnosti za organizaciju	Preuzeto iz: [345]	
32	MNG1	Postupci rukovodstva u mojoj organizaciji pokazuju da je sigurnost informacija važan organizacijski prioritet	Prilagođeno prema: [348]	
33		Poštivanje odredbi politike informacijske sigurnosti u mojoj organizaciji je nužnost	Prilagođeno prema: [166]	Čestica isključena jer nije bilo konsenzusa između eksperata u svrstavanju čestice većinski u jedan čimbenik
34		Poštivanje odredbi politike informacijske sigurnosti u mojoj organizaciji smanjuje broj sigurnosnih incidenata	Preuzeto iz: [206]	Čestica isključena jer nije bilo konsenzusa između eksperata u svrstavanju čestice većinski u jedan čimbenik
35	BLF2	Poštivanje politike informacijske sigurnosti u organizaciji usporava moju produktivnost na poslu	Preuzeto iz: [77]	
36	AA2	Prilikom promjene lozinke, ona mora biti određene duljine i kombinacija malih i velikih slova te brojeva	Prilagođeno prema: [345]	
37	BHV2	Primjena dobrih praksi vezanih uz sigurnost informacijske imovine predstavlja prihvaćeni način poslovanja u mojoj organizaciji	Prilagođeno prema: [67]	
38	POL4	Procedure za implementaciju politike informacijske sigurnosti su jasno definirane i dokumentirane	Preuzeto iz: [69]	Na temelju komentara eksperata čestica promijenjena u: *Procedure za implementaciju politike informacijske sigurnosti (npr. procedura upravljanja korisničkim računima, procedura upravljanja promjenama u sustavu, procedura upravljanja sigurnosnim incidentima…) su jasno definirane i dokumentirane*

Rbr.	Oznaka	Čestica[13]	Izvor	Napomena
39	BCK2	Proces redovne izrade sigurnosne kopije (eng. backup) i povrata podataka (eng. restore) značajno doprinosi dostupnosti kritičnih informacija	Prilagođeno prema: [345]	
40	BCK3	Proces redovne izrade sigurnosne kopije (eng. backup) i povrata podataka (eng. restore) značajno doprinosi mogućnosti oporavka poslovanja u slučaju pojave katastrofalnog događaja	Prilagođeno prema: [345]	
41		Provođenje odredbi politike informacijske sigurnosti može utjecati na nepovjerenje među zaposlenicima	Prilagođeno prema: [349]	Čestica isključena jer ne zadovoljava kriterij za n = 11; CVR > 0,59 i AVRI <= 2,00 (CVR = 0,09; AVRI = 2,27)
42		Rukovodstvo moje organizacije smatra da su svi zaposlenici odgovorni za informacijsku sigurnost	Preuzeto iz: [350]	Čestica isključena jer nije bilo konsenzusa između eksperata u svrstavanju čestice većinski u jedan čimbenik
43	MNG2	Rukovodstvo u mojoj organizaciji brine o informacijskoj sigurnosti samo kad se dogodi neki incident	Preuzeto iz: [350]	
44	MNG3	Rukovodstvo u mojoj organizaciji omogućuje dovoljno financijskih i ljudskih resursa za upravljanje informacijskom sigurnošću	Prilagođeno prema: [115]	
45	MNG4	Rukovodstvo u mojoj organizaciji preuzima krajnju odgovornost za informacijsku sigurnost	Prilagođeno prema: [115]	
46	MNG5	Rukovodstvo u mojoj organizaciji pridržava se odredbi politike informacijske sigurnosti	Preuzeto iz: [335]	
47	MNG6	Rukovodstvo u mojoj organizaciji sudjeluje u edukacijama, projektima, radionicama podizanja svijesti i ostalim aktivnostima vezanim uz informacijsku sigurnost	Prilagođeno prema: [115]	
48	POL5	Sadržaj politike informacijske sigurnosti lako je razumljiv	Preuzeto iz: [336]	
49		Sigurnosne kontrole trebale bi omogućiti da informacijski sustav bude siguran, ali i dalje upotrebljiv	Preuzeto iz: [346]	Čestica isključena jer nije bilo konsenzusa između eksperata u svrstavanju čestice većinski u jedan čimbenik
50	POL6	Sigurnosne politike i procedure su lako dostupne u mojoj organizaciji	Prilagođeno prema: [347]	
51		Smatram da je za organizaciju neophodno nadzirati usklađenost sa politikom informacijske sigurnosti	Preuzeto iz: [336]	Čestica isključena jer nije bilo konsenzusa između eksperata u svrstavanju čestice većinski u jedan čimbenik
52		Smatram da je zaštita informacija moje organizacije važna	Preuzeto iz: [166]	Čestica isključena jer nije bilo konsenzusa između eksperata u

Rbr.	Oznaka	Čestica[13]	Izvor	Napomena
				svrstavanju čestice većinski u jedan čimbenik
53	EDU7	Smatram da je znanje o informacijskoj sigurnosti mojih kolega u organizaciji na zadovoljavajućoj razini	Preuzeto iz: [351]	
54	BLF3	Smatram da moja organizacija daje dovoljno pažnje strategiji informacijske sigurnosti s ciljem zaštite informacijske imovine	Prilagođeno prema: [245]	
55	AA3	Sustav me nakon određenog vremena traži da promijenim svoju lozinku	Prilagođeno prema: [345]	
56		Svatko u mojoj organizaciji može doprinijeti povećanju informacijske sigurnosti	Prilagođeno prema: [199]	Čestica isključena jer nije bilo konsenzusa između eksperata u svrstavanju čestice većinski u jedan čimbenik
57		Svi pokušaji pristupa povjerljivim informacijama organizacije trebali bi obavezno biti zabilježeni	Prilagođeno prema: [345]	Čestica isključena jer nije bilo konsenzusa između eksperata u svrstavanju čestice većinski u jedan čimbenik
58	EDU8	Svi zaposlenici su educirani o potrebi zaključavanja svojih računala kad napuštaju svoje radno mjesto	Preuzeto iz: [344]	
59	EDU9	Svi zaposlenici u mojoj organizaciji pravovremeno su obaviješteni o prijetnjama informacijske sigurnosti putem elektroničke pošte ili na neki drugi način	Prilagođeno prema: [347]	
60	AA4	Svim računalima s povjerljivim informacijama treba se moći pristupiti samo s odgovarajućim korisničkim imenom i lozinkom	Prilagođeno prema: [345]	Na temelju komentara eksperata čestica promijenjena u: *Svim povjerljivim informacijama treba se moći pristupiti samo s odgovarajućim korisničkim imenom i lozinkom*
61		Svjestan sam disciplinskih mjera uslijed kršenja odredbi politike informacijske sigurnosti	Prilagođeno prema: [69]	Čestica isključena jer nije bilo konsenzusa između eksperata u svrstavanju čestice većinski u jedan čimbenik
62	BHV3	Svoje znanje o informacijskoj sigurnosti dijelim s kolegama/icama kako bih povećao njihovu svijest o toj tematici	Prilagođeno prema: [351]	
63	POL9	U mojoj organizaciji definirana je osoba kojoj se mogu obratiti s pitanjima vezanim uz informacijsku sigurnost	Prilagođeno prema: [69]	
64	POL10	U mojoj organizaciji jasno su definirane uloge i odgovornosti zaposlenika vezane za informacijsku sigurnost	Preuzeto iz: [344]	

Rbr.	Oznaka	Čestica[13]	Izvor	Napomena
65	EDU15	U mojoj organizaciji koriste se različiti oblici komunikacije (npr. e-mail, plakati, post-it poruke, newsletter,…) za promicanje svijesti o informacijskoj sigurnosti	Prilagođeno prema: [151]	
66	EDU3	U mojoj organizaciji podržava se održavanje periodičkih sigurnosnih radionica za zaposlenike	Preuzeto iz: [350]	Na temelju komentara eksperata čestica promijenjena u: *U mojoj organizaciji podržava se periodično održavanje radionica za zaposlenike na temu informacijske sigurnosti*
67	CMP3	U mojoj organizaciji provjerava se slijede li zaposlenici sigurnosne politike, procedure i smjernice	Prilagođeno prema: [137]	
68	CMP4	U mojoj organizaciji redovno se provjerava učinkovitost i potpunost politike informacijske sigurnosti	Preuzeto iz: [345]	
69	AA5	U mojoj organizaciji uspostavljeni su odgovarajući mehanizmi kojima se osigurava da pristup informacijskom sustavu imaju samo ovlaštene osobe (npr. upotrebom korisničkog imena i lozinke)	Prilagođeno prema: [344]	
70	MNG7	U mojoj organizaciji vidljiva je predanost i potpora od strane rukovodstva vezano za informacijsku sigurnost	Prilagođeno prema: [157]	
71	POL7	U mojoj organizaciji, jasno su definirane disciplinske mjere u slučaju kršenja odredbi sigurnosne politike	Prilagođeno prema: [347]	
72		U mojoj organizaciji, ovlašteni zaposlenik u slučaju poslovne potrebe može u bilo koje doba pristupiti organizacijskim podacima	Prilagođeno prema: [60]	Čestica isključena jer ne zadovoljava kriterij za n = 11; CVR > 0,59 (CVR = 0,27)
73	BLF4	U mojoj organizaciji, provođenje sigurnosnih mjera oduzimalo bi previše vremena	Preuzeto iz: [105]	
74	EDU4	U mojoj organizaciji, svi zaposlenici dobivaju dovoljnu i primjerenu edukaciju o informacijskoj sigurnosti	Prilagođeno prema: [344]	
75	EDU16	U mojoj organizaciji, zaposlenici su upućeni što se smatra (ne)prihvatljivim korištenjem informacijske imovine	Prilagođeno prema: [151]	
76		Ukoliko obrišem neki podatak, IT odjel mi ga može vratiti	Preuzeto iz: [115]	Čestica isključena jer ne zadovoljava kriterij za n = 11; CVR > 0,59 (CVR = 0,45)
77	EDU17	Upoznat/a sam sa sigurnosnim politikama, procedurama i smjernicama moje organizacije	Preuzeto iz: [137]	

Rbr.	Oznaka	Čestica[13]	Izvor	Napomena
78	POL11	Upoznat/a sam sa svojim odgovornostima vezanim uz informacijsku sigurnost	Preuzeto iz: [336]	
79	BLF5	Uvjeren/a sam da drugi zaposlenici poštuju odredbe politike informacijske sigurnosti u mojoj organizaciji	Preuzeto iz: [199]	
80	AA6	Važno je da informacijski sustav ima mogućnost utvrđivanja individualne odgovornosti zaposlenika za poduzete radnje.	Prilagođeno prema: [346]	
81		Veća je vjerojatnost da će etični zaposlenici razumjeti vrijednost informacijske sigurnosti	Prilagođeno prema: [346]	Čestica isključena jer je većinski svrstana u čimbenik ETIČNOST koji je isključen jer ne zadovoljava kriterij za n = 11; CVR > 0,59 (CVR = 0,45)
82		Veća je vjerojatnost da će se odredbi sigurnosne politike pridržavati zaposlenici koji su prošli edukaciju i svjesni su postojanja sigurnosne politike	Preuzeto iz: [157]	Čestica isključena jer nije bilo konsenzusa između eksperata u svrstavanju čestice većinski u jedan čimbenik
83		Vjerujem da moja organizacija aktivno nadzire sadržaj elektroničke pošte svojih zaposlenika	Preuzeto iz: [67]	Čestica isključena jer ne zadovoljava kriterij za n = 11; CVR > 0,59 i AVRI <= 2,00 (CVR = 0,45; AVRI = 2,09)
84		Za mene bi predstavljalo problem ako bi moji kolege saznali da se nisam pridržavao zahtjeva sigurnosne politike	Preuzeto iz: [206]	Čestica isključena jer ne zadovoljava kriterij za AVRI <= 2,00 (AVRI = 2,09)
85		Za mene je pridržavanje zahtjeva sigurnosne politike važno	Preuzeto iz: [77]	Čestica isključena jer nije bilo konsenzusa između eksperata u svrstavanju čestice većinski u jedan čimbenik
86		Zaposlenici ne bi trebali međusobno dijeliti korisničke lozinke za pristup sustavu	Prilagođeno prema: [345]	Čestica isključena jer nije bilo konsenzusa između eksperata u svrstavanju čestice većinski u jedan čimbenik
87	EDU5	Zaposlenici su educirani oko svojih uloga i odgovornosti vezanih za informacijsku sigurnost i toga kako se ponašati na siguran način	Preuzeto iz: [6]	
88		Zaposlenici u mojoj organizaciji percipiraju informacijsku sigurnost kao važnu	Prilagođeno prema: [335]	Čestica isključena jer nije bilo konsenzusa između eksperata u svrstavanju čestice većinski u jedan čimbenik
89	BHV4	Zaposlenici u mojoj organizaciji preuzimaju odgovornost za zaštitu informacija s kojima dolaze u doticaj	Prilagođeno prema: [345]	
90		Zaposlenici u mojoj organizaciji su privrženi organizaciji i međusobno si vjeruju	Preuzeto iz: [60]	Čestica isključena jer ne zadovoljava kriterij za n = 11; CVR > 0,59 (CVR = 0,45)

Rbr.	Oznaka	Čestica[13]	Izvor	Napomena
91	BLF6	Zaposlenik koji krši politiku informacijske sigurnosti šteti svojoj organizaciji	Preuzeto iz: [153]	
92	EDU6	Zbog edukacija vezanih uz informacijsku sigurnost osjećam se bolje pripremljen za potencijalne sigurnosne incidente	Prilagođeno prema: [196]	
93	BCK4	Znam gdje na računalu trebam pohranjivati bitne podatke kako bi se izradila njihova sigurnosna kopija (eng. backup)	Autor	Na temelju komentara eksperata čestica promijenjena u: *Znam gdje trebam pohranjivati bitne podatke kako bi se izradila njihova sigurnosna kopija (eng. backup)*
94	EDU18	Znam što je "incident informacijske sigurnosti"	Preuzeto iz: [336]	
95	EDU19	Znam što podrazumijeva pojam "informacijska sigurnost"	Preuzeto iz: [160]	
96	SS1	Upoznat/a sam s podatkom da se u zadnjih 12 mjeseci u mojoj organizaciji dogodio incident vezan uz informacijsku sigurnost	Prilagođeno prema: [336]	Na temelju komentara eksperata čestica promijenjena u: *Upoznat/a sam s činjenicom da se u zadnjih 12 mjeseci u mojoj organizaciji dogodio incident vezan uz informacijsku sigurnost*
97	SS2	U zadnjih 12 mjeseci bio/bila sam obaviješten/a o promjeni sigurnosne politike ili pravila u svojoj organizaciji	Prilagođeno prema: [336]	
98	SS3	U zadnjih 12 mjeseci sam bio/bila upozoren/a na prijetnje vezane uz otkrivanje povjerljivih informacija	Autor	Na temelju komentara eksperata čestica promijenjena u: *U zadnjih 12 mjeseci bio/bila sam informiran/a o prijetnjama vezanim uz otkrivanje povjerljivih informacija*
99	SS4	U zadnjih 12 mjeseci bio/bila sam upozoren/a na prijetnje vezane uz otvaranje sumnjivih mailova i privitaka u njima	Autor	Na temelju komentara eksperata čestica promijenjena u: *U zadnjih 12 mjeseci bio/bila sam informiran/a o prijetnjama vezanim uz otvaranje sumnjivih elektroničkih poruka i privitaka u njima*
100	SS5	U zadnjih 12 mjeseci bio/bila sam upozoren/a na prijetnje vezane uz razne oblike računalnih virusa	Autor	
101	SS6	U zadnjih 12 mjeseci bio/bila sam upozoren/a na prijetnje vezane uz socijalni inženjering (lažno predstavljanje, slanje poruka s izvora koji djeluju pouzdano u svrhu dobivanja informacija, prikupljanje informacija putem telefona i sl.)	Autor	Na temelju komentara eksperata čestica promijenjena u: *U zadnjih 12 mjeseci bio/bila sam upozoren/a na prijetnje vezane uz socijalni inženjering (lažno predstavljanje, slanje neistinitih poruka koji djeluju pouzdano u svrhu dobivanja informacija, prikupljanje informacija putem telefona i sl.)*
102	SS7	U zadnjih 12 mjeseci uočio/la sam da je, nakon što je moj/a kolega/ica napustio/la svoje radno mjesto,	Autor	

Rbr.	Oznaka	Čestica[13]	Izvor	Napomena
		njegovo/njezino računalo ostalo otključano (mogao/la sam sjesti za to računalo i nastaviti raditi)		
103	SS8	U zadnjih 12 mjeseci uočio/la sam da su moji kolege/ice dijelili korisničke lozinke za pristup informacijskom sustavu	Autor	Na temelju komentara eksperata čestica promijenjena u: *U zadnjih 12 mjeseci uočio/la sam da su moji kolege/ice dijelili vlastite korisničke lozinke za pristup informacijskom sustavu s drugim korisnicima/icama*
104	SS9	U zadnjih 12 mjeseci sustav me tražio da promijenim svoju lozinku	Autor	
105	SS10	U zadnjih 12 mjeseci dobio/la sam poziv za sudjelovanje na edukaciji/radionici za podizanje svijesti o informacijskoj sigurnosti	Autor	
106	SS11	U mojoj organizaciji postoji interna funkcija (jedna ili više osoba ili odjel) zadužena za informacijsku sigurnost	Eksperti	Dodatna čestica predložena od strane eksperata
107	SS12	U zadnjih 12 mjeseci prijavio/la sam incident informacijske sigurnosti ili sumnju na isti	Eksperti	Dodatna čestica predložena od strane eksperata

Izvor: *vlastiti prikaz*

Prilog 2. Elektronička poruka za eksperte s uputama za evaluaciju

Poštovana/i,

Prije svega, želim Vam zahvaliti što ste pristali sudjelovati u mom istraživanju vezanom uz izradu doktorske disertacije pod naslovom „*Radni okvir za procjenu i unapređenje kulture informacijske sigurnosti*" na Fakultetu organizacije i informatike Varaždin Sveučilišta u Zagrebu, pod mentorstvom prof. dr. sc. Maria Spremića i doc. dr. sc. Nikoline Žajdela Hrustek.

Kao što sam naslov disertacije kaže, cilj ovog istraživanja jest izrada okvira za procjenu i unapređenje kulture informacijske sigurnosti temeljenog na rezultatima empirijskog istraživanja. Upravo iz tog razloga, jedan od najvažnijih dijelova ovog istraživanja je mjerni instrument (upitnik) pomoću kojeg će se prikupljati činjenice vezane uz stanje informacijske sigurnosti u pojedinoj organizaciji te je vrlo važno definirati točan skup čestica koje će moći obuhvatiti relevantne činjenice vezane uz ključne čimbenike koji čine kulturu informacijske sigurnosti.

Iz tog razloga bih Vas zamolio za Vaš vrijedan doprinos ovom istraživanju kroz sljedeće korake:

a) Temeljito pročitajte dokument sa uputama. U slučaju da naiđete na bilo kakvu nejasnoću budite slobodni kontaktirati me na e-mail krunoslav.arbanas@gmail.com ili karbanas@foi.hr
b) Ocijenite jasnoću, razumljivost i cjelovitost čestica, čimbenika i kategorija. Ukoliko smatrate potrebnim, preformulirajte česticu ili čimbenik ili njihov naziv te ukoliko smatrate da određena čestica, čimbenik ili kategorija nedostaju, molim upišite je u mjestu naznačenom za to.
c) Dodijelite razinu važnosti svakoj čestici i čimbeniku.
d) Razvrstajte čestice i čimbenike u predložene (bilo predložene s moje strane ili izmijenjene s Vaše strane) kategorije.
e) Ocijenite jasnoću, razumljivost i cjelovitost pitanja vezanih uz prediktivnu valjanost kako bi se mogao izraditi indeks kulture informacijske sigurnosti čija je svrha utvrditi stupanj do kojeg percepcija zaposlenika predviđa stvarno stanje informacijske sigurnosti u organizaciji. Ukoliko smatrate potrebnim, preformulirajte pojedino pitanje kako mislite da bi bilo ispravnije. Ujedno Vas molim za uključivanje dodatnih pitanja za koje, na temelju Vašeg iskustva, smatrate da se vežu uz mogućnost identificiranja stvarnog stanja informacijske sigurnosti u nekoj organizaciji, a da neće zadirati u

osjetljive informacije organizacije (zbog čega bi postojala opasnost da ispitanici neće odgovoriti).

Svrha prethodno navedenih koraka je osiguranje da:

a) identificirane čestice budu što jasnije i razumljivije potencijalnim sudionicima istraživanja
b) mjerni instrument (upitnik) sadrži sve neophodne i relevantne čestice kojima će se moći prikupiti činjenice vezane uz stanje kulture informacijske sigurnosti
c) svi identificirani čimbenici budu mjereni dostatnim brojem čestica i to česticama koje ih najbolje opisuju
d) prikupljeni podaci budu valjani.

Potrebno vrijeme za evaluaciju je otprilike 90-100 min. Evaluaciju ne trebate napraviti odjednom već dokument možete spremiti na Vaše računalo i nastaviti u bilo koje vrijeme.

Molio bih Vas da mi vratite popunjenu tablicu do **14.06.2019.**

Unaprijed Vam se zahvaljujem na Vašem trudu i vremenu.

S poštovanjem,

Krunoslav Arbanas

UPUTE ZA EVALUACIJU

Evaluaciju molim izvršite u pripremljenom Microsoft Excel dokumentu pod nazivom „Evaluacija domenskih eksperata_v.1.0_KA" koji možete naći u prilogu elektroničke poruke. Molio bih Vas da obratite pozornost da se dokument sastoji od 4 radna lista vezana uz predmetni anketni upitnik: **ČESTICE (MANIFESTNE VARIJABLE), ČIMBENICI, KATEGORIJE i PITANJA – PREDIKTIVNA VALJANOST.** Dodatni, peti radni list sastoji se od nekoliko pitanja koja služe za statistički opis demografskih karakteristika eksperata koji su pomogli u evaluaciji predmetnog upitnika.

Prvi radni list **ČESTICE (MANIFESTNE VARIJABLE)** sastoji se od sljedećih stupaca:

A **– RBR.** – redni broj čestice (manifestne varijable)

B **- ČESTICE (MANIFESTNE VARIJABLE)** – ovaj stupac sastoji se od 95 identificiranih čestica (manifestnih varijabli) vezanih uz kulturu informacijske sigurnosti koje evaluirate.

C **- VAŽNOST ČESTICE –** u ovom stupcu iz padajućeg izbornika odabirete važnost čestice prema Vašem mišljenju, znanju i iskustvu na sljedeći način:

- **0** – ukoliko iz bilo kojeg razloga **ne možete odrediti** važnost pojedine čestice,
- **1** – ukoliko smatrate da je čestica **obavezna,**
- **2** – ukoliko smatrate da je čestica **poželjna,**
- **3** – ukoliko smatrate da je čestica **nepotrebna** i zbog toga bi trebala biti uklonjena iz skupa čestica/mjernog instrumenta.

D **- PRIJEDLOG PROMJENE ČESTICE** – koristite ovaj stupac ukoliko smatrate da određena čestica treba biti preformulirana i u ovaj stupac upišite preformuliranu česticu. Ukoliko smatrate da se ne bi trebalo ništa promijeniti i da je po Vama čestica jasna, razumljiva i cjelovita ostavite stupac prazan.

E **- OBJAŠNJENJE PROMJENE –** ovaj stupac koristite za objašnjenje preformulacije svake pojedine čestice koju smatrate neophodnim. Ukoliko smatrate da se ne bi trebalo ništa promijeniti ostavite stupac prazan.

F – S **– NAZIVI ČIMBENIKA –** koristite oznaku **X** i na taj način pridružite svaku česticu **samo jednom od 13 čimbenika** (Politike i procedure, Podrška rukovodstva, Uloge i

odgovornosti, Edukacija, Sigurnosna osviještenost, Usklađenost, Ponašanje, Etičnost, Uvjerenja, Povjerenje, Antivirusna zaštita, Sigurnosna kopija, Autentikacija i autorizacija).

Ukoliko smatrate da određena čestica (manifestna varijabla) nedostaje, a po Vašem mišljenju neophodna je za kulturu informacijske sigurnosti, molio bih Vas da:

- upišete česticu (manifestnu varijablu) u stupac B počevši od rednog broja 97,
- odredite važnost čestice u stupcu C,
- objasnite važnost uključivanja čestice u stupcu E,
- dodijelite česticu odgovarajućem čimbeniku od stupca F –S,

kako bi se osiguralo da svaki čimbenik bude mjeren sa odgovarajućim brojem čestica, molio bih da svakom čimbeniku dodijelite **barem** 3 do 5 čestica.

C - **VAŽNOST ČIMBENIKA –** u ovom stupcu iz padajućeg izbornika odabirete važnost čimbenika prema Vašem mišljenju, znanju i iskustvu na sljedeći način:

- **0** – ukoliko iz bilo kojeg razloga **ne možete odrediti** važnost pojedinog čimbenika,
- **1** – ukoliko smatrate da je čimbenik **obavezan,**
- **2** – ukoliko smatrate da je čimbenik **poželjan,**
- **3** – ukoliko smatrate da je čimbenik **nepotreban** i zbog toga bi trebao biti uklonjen iz skupa čimbenika.

D **- PRIJEDLOG PROMJENE ČIMBENIKA** – koristite ovaj stupac ukoliko smatrate da određeni čimbenik treba biti preformuliran i u ovaj stupac upišite preformulirani čimbenik. Ukoliko smatrate da se ne bi trebalo ništa promijeniti i da je po Vama čimbenik jasan, razumljiv i cjelovit ostavite stupac prazan.

E - **OBJAŠNJENJE PROMJENE –** ovaj stupac koristite za objašnjenje preformulacije svakog pojedinog čimbenika koju smatrate neophodnim. Ukoliko smatrate da se ne bi trebalo ništa promijeniti ostavite stupac prazan.

F – H **– NAZIVI KATEGORIJE –** koristite oznaku **X** i na taj način pridružite svaki čimbenik **samo jednoj od tri kategorije** (Organizacijske mjere, Sociološki čimbenici, Tehničke mjere).

Ukoliko smatrate da određeni čimbenik nedostaje, a po Vašem mišljenju neophodan je za kulturu informacijske sigurnosti, molio bih Vas da:

- upišete čimbenik u stupac B počevši od rednog broja 15,
- odredite važnost čimbenika u stupcu C,
- objasnite važnost uključivanja čimbenika u stupcu E,
- dodijelite čimbenik odgovarajućoj kategoriji od stupca F-H,
- kako bi se osiguralo da svaki čimbenik bude mjeren sa odgovarajućim brojem čestica, molio bih da svakom čimbeniku dodijelite **barem** 3 do 5 čestica (ukoliko dodajete nove čimbenike).

Treći radni list **KATEGORIJE** sastoji se od stupaca:

A **– RBR.** – redni broj kategorije

B - **NAZIV KATEGORIJE** – ovaj stupac sastoji se od 3 identificirane kategorije vezane uz kulturu informacijske sigurnosti koje evaluirate.

C - **VAŽNOST KATEGORIJE –** u ovom stupcu iz padajućeg izbornika odabirete važnost kategorije prema Vašem mišljenju, znanju i iskustvu na sljedeći način:

- **0** – ukoliko iz bilo kojeg razloga **ne možete odrediti** važnost pojedine kategorije,
- **1** – ukoliko smatrate da je kategorija **obavezna,**
- **2** – ukoliko smatrate da je kategorija **poželjna,**
- **3** – ukoliko smatrate da je kategorija **nepotrebna** i zbog toga bi trebala biti uklonjena iz skupa.

D - **PRIJEDLOG PROMJENE KATEGORIJE** – koristite ovaj stupac ukoliko smatrate da određena kategorija treba biti preformulirana i u ovaj stupac upišite preformulirani naziv kategorije. Ukoliko smatrate da se ne bi trebalo ništa promijeniti i da je po Vama naziv kategorije jasan, razumljiv i cjelovit i da dobro objašnjava kulturu informacijske sigurnosti ostavite stupac prazan.

E - **OBJAŠNJENJE PROMJENE –** ovaj stupac koristite za objašnjenje preformulacije svake pojedine kategorije koju smatrate neophodnom. Ukoliko smatrate da se ne bi trebalo ništa promijeniti ostavite stupac prazan.

Ukoliko smatrate da određena kategorija nedostaje, a po Vašem mišljenju neophodna je za kulturu informacijske sigurnosti molio bih Vas da:

- upišete kategoriju u stupac B počevši od rednog broja 5,

- odredite važnost kategorije u stupcu C,
- objasnite važnost uključivanja kategorije u stupcu E.

Četvrti radni list **PITANJA – PREDIKTIVNA VALJANOST** sastoji se od stupaca:

A **– RBR.** – redni broj pitanja

B **- PITANJE** – ovaj stupac sastoji se od trenutno identificiranih 10 pitanja koja se vežu uz mogućnost identificiranja stvarnog stanja informacijske sigurnosti u nekoj organizaciji (za razliku od ostalih čestica (pitanja) koje čine percipirano stanje pojedinog ispitanika).

C **- PRIJEDLOG PROMJENE PITANJA** – koristite ovaj stupac ukoliko smatrate da određeno pitanje treba biti preformulirano iz razloga što nije dovoljno jasno, gramatički ispravno, razumljivo i sl. i u ovaj stupac upišite preformulirani naziv pitanja. Ukoliko smatrate da se ne bi trebalo ništa promijeniti i da je po Vama pitanje jasno, razumljivo i cjelovito i da se veže uz mogućnost identificiranja stvarnog stanja informacijske sigurnosti u nekoj organizaciji ostavite stupac prazan.

D **- OBJAŠNJENJE PROMJENE –** ovaj stupac koristite za objašnjenje preformulacije svakog pojedinog pitanja koju smatrate neophodnom. Ukoliko smatrate da se ne bi trebalo ništa promijeniti ostavite stupac prazan.

Ukoliko smatrate da bi određeno pitanje koje nije navedeno, a po Vašem mišljenju moglo bi pomoći pri identificiranju stvarnog stanja informacijske sigurnosti u nekoj organizaciji, molio bih Vas da:

- upišete pitanje u stupac B počevši od rednog broja 12,
- objasnite važnost uključivanja pitanja u stupcu D.

OBJAŠNJENJE POJMOVA

ČESTICA (MANIFESTNA VARIJABLA) – tvrdnja u mjernom instrumentu koju ispitanik u istraživanju evaluira prema subjektivnim ili objektivnim kriterijima.

ČIMBENIK – istraživački koncept koji nije moguće izravno mjeriti već se mjeri pomoću čestica.

KATEGORIJA – istraživački koncept koji nije moguće izravno mjeriti već se mjeri pomoću čimbenika.

PITANJA ZA PREDIKTIVNU VALJANOST - pitanja vezana uz mogućnost identificiranja stvarnog stanja informacijske sigurnosti u nekoj organizaciji čija je svrha utvrditi stupanj do kojeg percepcija zaposlenika predviđa stvarno stanje informacijske sigurnosti u organizaciji (npr. Ako je ispitanik na pitanje „*Sustav me nakon određenog vremena traži da promijenim svoju lozinku*" odgovorio da se slaže, odgovor na pitanje „*U zadnjih 12 mjeseci sustav me tražio da promijenim svoju lozinku: 0 puta; 1 put; 2 puta; 3 puta; 4 i više puta*", u pravilu, ne bi trebao biti 0 puta.).

DEFINICIJE RAZINA VAŽNOSTI ČESTICE/ČIMBENIKA/KATEGORIJE

OBAVEZNA - (1) - neophodna/bitna čestica, čimbenik ili kategorija za kulturu informacijske sigurnosti.

POŽELJNA – (2) - važna (ali ne i neophodna/bitna) čestica, čimbenik ili kategorija za kulturu informacijske sigurnosti.

NEPOTREBNA – (3) - čestica, čimbenik ili kategorija za koju se smatra da nema važnosti za kulturu informacijske sigurnosti i stoga bi se trebala izbaciti iz skupa/mjernog instrumenta.

DEFINIRANJE ČIMBENIKA

Politike i procedure – izrađena dokumentacija vezana uz informacijsku sigurnost.

Podrška rukovodstva – aktivnosti, radnje i stavovi rukovodstva organizacije vezani uz informacijsku sigurnost.

Uloge i odgovornosti – pravila, dužnosti i obveze zaposlenika u organizaciji vezana uz zaštitu ili ugrožavanje informacijske sigurnosti.

Edukacija – radnje i aktivnosti vezane uz stjecanje i prenošenje znanja iz domene informacijske sigurnosti.

Sigurnosna osviještenost – znanje, rezultati edukacija, stavovi i ponašanje zaposlenika u kontekstu informacijske sigurnosti.

Usklađenost - pridržavanje organizacijskih sigurnosnih politika, svijest o postojanju takvih politika i sposobnost podsjećanja na suštinu takvih politika kao i sukladnost s primjenjivim zakonskim propisima.

Ponašanje – stvarne ili planirane radnje te mišljenja zaposlenika po pitanju informacijske sigurnosti.

Etičnost - percepcije sigurnosnih ponašanja i praksi koje zaposlenici smatraju normalnim ili devijantnim.

Uvjerenja – stavovi zaposlenika o različitim aktivnostima i radnjama koje se odnose na informacijsku sigurnost.

Povjerenje – stanje u organizaciji po pitanju odnosa, komunikacije, osjećaja pripadnosti te potpore pitanjima vezanim uz informacijsku sigurnost od strane zaposlenika organizacije.

Antivirusna zaštita – radnje, aktivnosti i rješenja za prepoznavanje i zaustavljanje aktivnosti zlonamjernog sadržaja na ICT uređajima.

Sigurnosna kopija – radnje i aktivnosti vezane uz osiguravanje dostupnosti podataka u slučaju oštećenja ili gubitka izvornih podataka.

Autentikacija i autorizacija – radnje i aktivnosti vezane uz proces u kojem se od zaposlenika iziskuje potvrda identiteta radi stjecanja prava korištenja ICT sustava i podataka pohranjenih na njemu.

DEFINIRANJE KATEGORIJA

Organizacijske mjere – kontrole za koje nije potreban nikakav ICT uređaj, sustav ili softverski alat tj. kontrole vezane uz okruženje informacijskog sustava uključujući, između ostalog, pisanu dokumentaciju te definirane uloge i odgovornosti zaposlenika.

Sociološki čimbenici – sve ono što ima važan udio u stavovima, mišljenjima i ponašanju zaposlenika po pitanju informacijske sigurnosti.

Tehničke mjere – logičke i fizičke kontrole koje uključuju upotrebu jednog ili više ICT uređaja, sustava i/ili softverskih alata (primjerice upotreba vatrozida, usmjerivača, preklopnika, antivirusnog softvera, imeničkog direktorija i sl.).

Prilog 3. Zahtjevi za pristup informacijama nadležnim sektorskim tijelima za određivanje operatora ključnih usluga s pripadajućim odgovorima

Obrazac broj 2
ZAHTJEV ZA PRISTUP INFORMACIJAMA

Podnositelj zahtjeva (ime i prezime / naziv, adresa / sjedište, telefon i/ili e-pošta)
Krunoslav Arbanas, [redacted], karbanas@foi.hr

Naziv tijela javne vlasti / sjedište i adresa
Hrvatska narodna banka, Trg hrvatskih velikana 3, 10 000 Zagreb

Informacija koja se traži
Popis identificiranih tvrtki operatora ključnih usluga iz sektora bankarstva sukladno Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/2018) za potrebe provođenja znanstvenog istraživanja u sklopu izrade doktorske disertacije na temu „Razvoj okvira za evaluaciju i uspostavu kulture informacijske sigurnosti“. **Obrazloženje: Popis je potreban isključivo iz razloga kako bi se uspjele identificirati organizacije kojima bi se uputio dopis s objašnjenjem predloženog istraživanja te anketnim upitnikom koji bi zaposlenici tih organizacija mogli dobrovoljno popuniti i ne bi se koristio u druge svrhe. Upitnikom se ne bi prikupljali nikakvi osobni niti povjerljivi podaci, a popunjavanje upitnika bilo bi u potpunosti anonimno. Također, nigdje se ne bi spominjali nazivi organizacija već samo sektor kojem pripadaju sukladno kategorizaciji iz spomenutog Zakona. Rezultati istraživanja koristit će se isključivo u istraživačke svrhe, a sudionici će dobiti sumarne i obrađene rezultate koji im mogu biti korisni za unaprjeđenje upravljanja sigurnošću.**

Način pristupa informaciji *(označiti)*
☐ neposredan pristup informaciji, ☐ pristup informaciji pisanim putem ☐ uvid u dokumente i izrada preslika dokumenata koji sadrže traženu informaciju, ☐ dostavljanje preslika dokumenata koji sadrži traženu informaciju, ☒ na drugi prikladan način (elektronskim putem ili drugo) putem e-maila

Arbanas K.
(vlastoručni potpis podnositelja zahtjeva)

Zagreb, 18.01.2019.
(mjesto i datum)

Napomena: *Tijelo javne vlasti ima pravo na naknadu stvarnih materijalnih troškova od podnositelja zahtjeva u svezi s pružanjem i dostavom tražene informacije.*

Obrazac broj 2 – Obrazac zahtjeva za pristup informaciji

Slika 9.1. Zahtjev za pristup informacijama – sektor bankarstva

Šalje: "Dubravka Budak" <dubravka.budak@hnb.hr>
Naslov: RE: Zahtjev za pristup informacijama
Datum: Uto, siječanj 22, 2019 11:35 am
Prima: "karbanas@foi.hr" <karbanas@foi.hr>
Cc: "Info" <info@hnb.hr>

Poštovani gospodine Arbanas,

nastavno na Vašu zamolbu možemo Vas izvijestiti da je popis identificiranih operatora ključnih usluga u sektoru bankarstva javan.

Naime, operatori ključnih usluga su globalno sistemski važne kreditne institucije i ostale sistemski važne kreditne institucije, sukladno Prilogu I. Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine", 64/2018).

Metoda određivanja ostalih sistemski važnih kreditnih institucija definirana je dokumentom „Postupak određivanja ostalih sistemski važnih kreditnih institucija i zahtjeva za zaštitni sloj za ostale sistemski važne kreditne institucije", a posljednje preispitivanje utvrđivanja ostalih sistemski važnih kreditnih institucija u Republici Hrvatskoj dostupno je u dokumentu „Priopćenje o preispitivanju utvrđivanja ostalih sistemski važnih kreditnih institucija u Republici Hrvatskoj". Oba dokumenta dostupna su na našoj internetskoj stranici na sljedećoj poveznici: https://www.hnb.hr/temeljne-funkcije/financijska-stabilnost/makrobonitetne-mjere/zastitni-sloj-kapitala-za-sistemski-vazne-institucije.

S poštovanjem,
Dubravka Budak

Dubravka Budak
Glavni stručni suradnik • Chief Associate
Direkcija za odnose s javnošću • Public Relations Department

T. +38514590337 • E. dubravka.budak@hnb.hr

HRVATSKA NARODNA BANKA • CROATIAN NATIONAL BANK
Trg hrvatskih velikana 3
HR-10000 Zagreb
www.hnb.hr

-----Original Message-----
From: karbanas@foi.hr [mailto:karbanas@foi.hr]
Sent: Friday, January 18, 2019 12:45 PM
To: Info <info@hnb.hr>
Subject: Zahtjev za pristup informacijama

Poštovani,

u prilogu dostavljam popunjen Zahtjev za pristup informacijama.

Lijep pozdrav,
Krunoslav Arbanas

Slika 9.2. Odgovor na zahtjev za pristup informacijama – sektor bankarstva

Obrazac broj 2
ZAHTJEV ZA PRISTUP INFORMACIJAMA

Podnositelj zahtjeva (ime i prezime / naziv, adresa / sjedište, telefon i/ili e-pošta)
Krunoslav Arbanas, [redacted], karbanas@foi.hr

Naziv tijela javne vlasti / sjedište i adresa
Hrvatska agencija za nadzor financijskih usluga **Miramarska 24b** **10 000 Zagreb**

Informacija koja se traži
Popis identificiranih tvrtki operatora ključnih usluga iz sektora infrastrukture financijskog tržišta sukladno Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/2018) za potrebe provođenja znanstvenog istraživanja u sklopu izrade doktorske disertacije na temu „Razvoj okvira za evaluaciju i uspostavu kulture informacijske sigurnosti“. **Obrazloženje: Popis je potreban isključivo iz razloga kako bi se uspjele identificirati organizacije kojima bi se uputio dopis s objašnjenjem predloženog istraživanja te anketnim upitnikom koji bi zaposlenici tih organizacija mogli dobrovoljno popuniti i ne bi se koristio u druge svrhe. Upitnikom se ne bi prikupljali nikakvi osobni niti povjerljivi podaci, a popunjavanje upitnika bilo bi u potpunosti anonimno. Također, nigdje se ne bi spominjali nazivi organizacija već samo sektor kojem pripadaju sukladno kategorizaciji iz spomenutog Zakona. Rezultati istraživanja koristit će se isključivo u istraživačke svrhe, a sudionici će dobiti sumarne i obrađene rezultate koji im mogu biti korisni za unaprjeđenje upravljanja sigurnošću.**

Način pristupa informaciji *(označiti)*
☐ neposredan pristup informaciji, ☐ pristup informaciji pisanim putem ☐ uvid u dokumente i izrada preslika dokumenata koji sadrže traženu informaciju, ☐ dostavljanje preslika dokumenata koji sadrži traženu informaciju, ☒ na drugi prikladan način (elektronskim putem ili drugo) putem e-maila

Arbanas K.
(vlastoručni potpis podnositelja zahtjeva)

Zagreb, 18.01.2019.
(mjesto i datum)

Napomena: *Tijelo javne vlasti ima pravo na naknadu stvarnih materijalnih troškova od podnositelja zahtjeva u svezi s pružanjem i dostavom tražene informacije.*

Obrazac broj 2 – Obrazac zahtjeva za pristup informaciji

Slika 9.3. Zahtjev za pristup informacijama – sektor infrastrukture financijskog tržišta

Šalje: "Ksenija Veseli" <Ksenija.Veseli@hanfa.hr>
Naslov: FW: Zahtjev za pristup informacijama
Datum: Pet, siječanj 25, 2019 12:29 pm
Prima: "karbanas@foi.hr" <karbanas@foi.hr>

Poštovani g. Arbanas,

Nastavno na dolje priloženi zahtjev podnesen temeljem odredbi Zakona o pravu na pristup informacijama (Narodne novine broj 25/13 i 85/15, dalje: ZPPI), kojim tražite popis operatora ključnih usluga iz sektora infrastrukture financijskog tržišta, materija uređena i propisana odredbama Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (Narodne novine broj 64/18, dalje: Zakon, https://www.uvns.hr/hr/normativni-akti/informacijska-sigurnost/kiberneticka-sigurnost), obavještavamo Vas u skladu sa odredbom članka 23. stavka 1. točke 5. ZPPI-a, da se njegove odredbe ne primjenjuju na informacije za koje postoji obveza čuvanja tajnosti, sukladno zakonu koji uređuje sigurnosno-obavještajni sustav Republike Hrvatske (članak 1. stavak 4. ZPPI-a).

Odredbom članka 40. Zakona propisana je zaštita podataka. Naime istom je u bitnome propisano da u postupanju po zahtjevima za pristup informacijama treba voditi računa da se popisi operatora ključnih usluga, kao i svi drugi podaci koji nastaju u okviru provedbe Zakona koriste isključivo u svrhu izvršavanja zahtjeva iz Zakona (zaštita kibernetičke sigurnosti) i da popis predstavlja informacije u odnosu na koje je moguće ograničiti pravo pristupa korisniku informacija. Isto tako je odredbom članka 41. Zakona propisano da su nadležna tijela dužna s podacima operatora ključnih usluga i davatelja usluga postupati u skladu sa zahtjevima povjerljivosti, ako su utvrđeni posebnim propisom o zaštititi takvih podataka.

Za svaku dodatnu informaciju stojim Vam na raspolaganju.

Srdačan pozdrav.

Ksenija Veseli, službenica za informiranje Hanfe

Hrvatska agencija za nadzor financijskih usluga/Croatian Financial Services Supervisory Agency

Ured za licenciranje/Licensing Office

Viša savjetnica/Senior Adviser

Franje Račkog 6

10 000 Zagreb, Hrvatska

tel/phone +385 1 6173 263

e-mail: ksenija.veseli@hanfa.hr

www.hanfa.hr

-----Original Message-----
From: karbanas@foi.hr [mailto:karbanas@foi.hr]
Sent: Friday, January 18, 2019 12:46 PM
To: Pristup Info <pristupinfo@hanfa.hr>
Subject: Zahtjev za pristup informacijama

Poštovani,

u prilogu dostavljam popunjen Zahtjev za pristup informacijama.

Lijep pozdrav,
Krunoslav Arbanas

Slika 9.4. Odgovor na zahtjev za pristup informacijama – sektor infrastrukture financijskog tržišta

Obrazac broj 2

ZAHTJEV ZA PRISTUP INFORMACIJAMA

Podnositelj zahtjeva (ime i prezime / naziv, adresa / sjedište, telefon i/ili e-pošta)

Krunoslav Arbanas, [redacted], karbanas@foi.hr

Naziv tijela javne vlasti / sjedište i adresa

Ministarstvo zaštite okoliša i energetike, Radnička cesta 80, 10 000 Zagreb

Informacija koja se traži

Popis identificiranih tvrtki operatora ključnih usluga iz sektora energetike sukladno Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/2018) za potrebe provođenja znanstvenog istraživanja u sklopu izrade doktorske disertacije na temu „Razvoj okvira za evaluaciju i uspostavu kulture informacijske sigurnosti".
Obrazloženje: Popis je potreban isključivo iz razloga kako bi se uspjele identificirati organizacije kojima bi se uputio dopis s objašnjenjem predloženog istraživanja te anketnim upitnikom koji bi zaposlenici tih organizacija mogli dobrovoljno popuniti i ne bi se koristio u druge svrhe. Upitnikom se ne bi prikupljali nikakvi osobni niti povjerljivi podaci, a popunjavanje upitnika bilo bi u potpunosti anonimno. Također, nigdje se ne bi spominjali nazivi organizacija već samo sektor kojem pripadaju sukladno kategorizaciji iz spomenutog Zakona. Rezultati istraživanja koristit će se isključivo u istraživačke svrhe, a sudionici će dobiti sumarne i obrađene rezultate koji im mogu biti korisni za unaprjeđenje upravljanja sigurnošću.

Način pristupa informaciji *(označiti)*

- ☐ neposredan pristup informaciji,
- ☐ pristup informaciji pisanim putem
- ☐ uvid u dokumente i izrada preslika dokumenata koji sadrže traženu informaciju,
- ☐ dostavljanje preslika dokumenata koji sadrži traženu informaciju,
- ☑ na drugi prikladan način (elektronskim putem ili drugo)
  putem e-maila

Arbanas K.

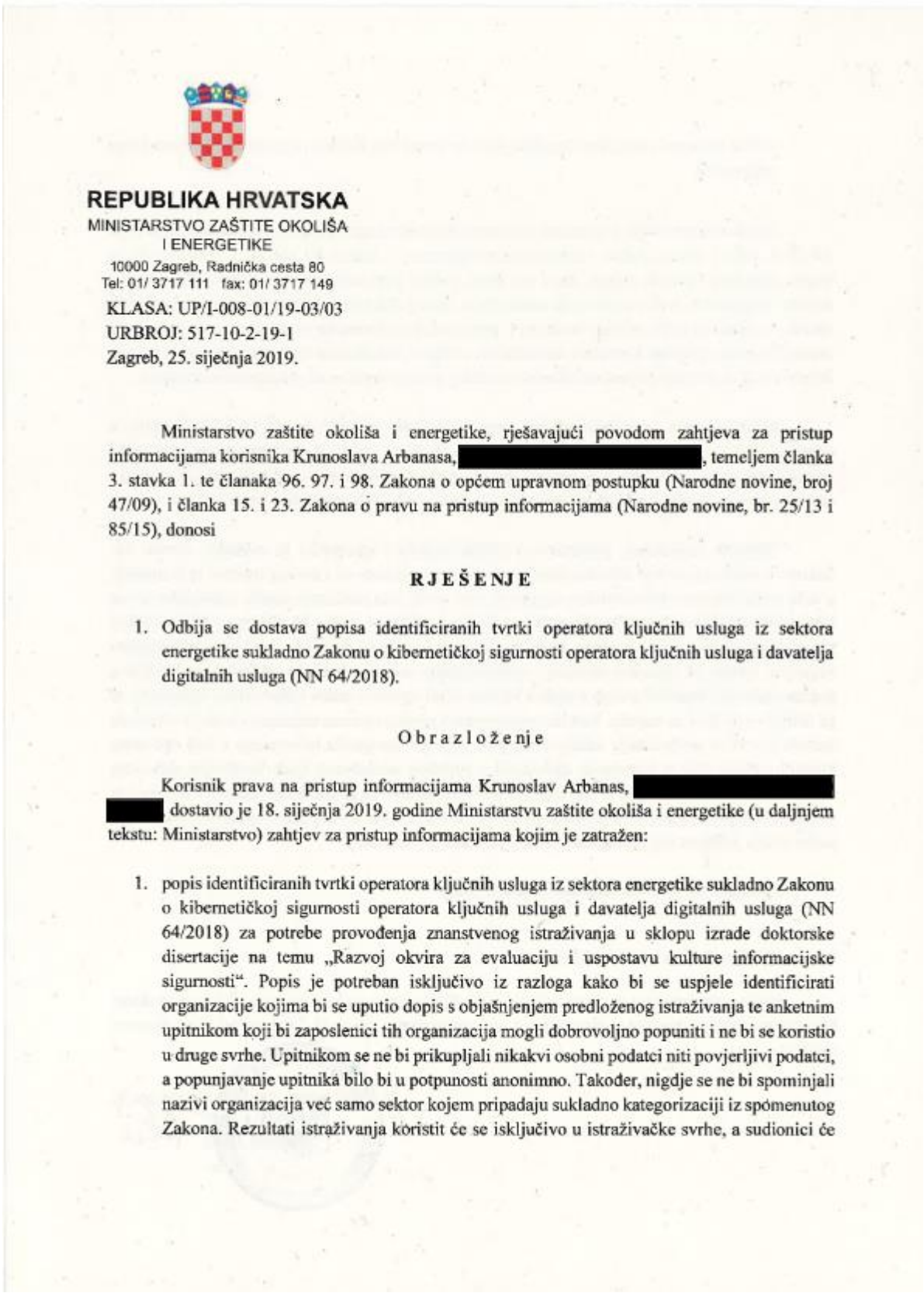
(vlastoručni potpis podnositelja zahtjeva)

Zagreb, 18.01.2019.
(mjesto i datum)

Napomena: *Tijelo javne vlasti ima pravo na naknadu stvarnih materijalnih troškova od podnositelja zahtjeva u svezi s pružanjem i dostavom tražene informacije.*

Obrazac broj 2 – Obrazac zahtjeva za pristup informaciji

Slika 9.5. Zahtjev za pristup informacijama – sektor energetike



REPUBLIKA HRVATSKA
MINISTARSTVO ZAŠTITE OKOLIŠA
I ENERGETIKE
10000 Zagreb, Radnička cesta 80
Tel: 01/ 3717 111 fax: 01/ 3717 149

KLASA: UP/I-008-01/19-03/03
URBROJ: 517-10-2-19-1
Zagreb, 25. siječnja 2019.

Ministarstvo zaštite okoliša i energetike, rješavajući povodom zahtjeva za pristup informacijama korisnika Krunoslava Arbanasa, [redacted], temeljem članka 3. stavka 1. te članaka 96. 97. i 98. Zakona o općem upravnom postupku (Narodne novine, broj 47/09), i članka 15. i 23. Zakona o pravu na pristup informacijama (Narodne novine, br. 25/13 i 85/15), donosi

R J E Š E N J E

1. Odbija se dostava popisa identificiranih tvrtki operatora ključnih usluga iz sektora energetike sukladno Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/2018).

O b r a z l o ž e n j e

Korisnik prava na pristup informacijama Krunoslav Arbanas, [redacted] dostavio je 18. siječnja 2019. godine Ministarstvu zaštite okoliša i energetike (u daljnjem tekstu: Ministarstvo) zahtjev za pristup informacijama kojim je zatražen:

1. popis identificiranih tvrtki operatora ključnih usluga iz sektora energetike sukladno Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/2018) za potrebe provođenja znanstvenog istraživanja u sklopu izrade doktorske disertacije na temu „Razvoj okvira za evaluaciju i uspostavu kulture informacijske sigurnosti". Popis je potreban isključivo iz razloga kako bi se uspjele identificirati organizacije kojima bi se uputio dopis s objašnjenjem predloženog istraživanja te anketnim upitnikom koji bi zaposlenici tih organizacija mogli dobrovoljno popuniti i ne bi se koristio u druge svrhe. Upitnikom se ne bi prikupljali nikakvi osobni podatci niti povjerljivi podatci, a popunjavanje upitnika bilo bi u potpunosti anonimno. Također, nigdje se ne bi spominjali nazivi organizacija već samo sektor kojem pripadaju sukladno kategorizaciji iz spomenutog Zakona. Rezultati istraživanja koristit će se isključivo u istraživačke svrhe, a sudionici će

Slika 9.6. Odgovor na zahtjev za pristup informacijama – sektor energetike

dobiti sumarne i obrađene rezultate koji im mogu biti korisni za unapređenje upravljanja sigurnošću.

Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/2018, dalje u tekstu: Zakon o kibernetičkoj sigurnosti) u članku 40. stavku 1. propisuje da se popisi operatera ključnih usluga, kao i svi drugi podaci koji nastaju u okviru provedbe Zakona koriste isključivo u svrhu izvršavanja zahtijeva iz samog Zakona o kibernetičkoj sigurnosti, dok stavak 2. navodi da popis i podaci iz stavka 1. predstavljaju informacije u odnosu na koje je moguće ograničiti pravo pristupa korisniku informacija, ovisno o rezultatima testa razmjernosti i javnog interesa koji se provodi prema odredbama posebnog zakona o pravu na pristup informacijama.

Zakon o pravu na pristup informacijama („Narodne novine", br. 25/13. i 85/15., dalje u tekstu: Zakona o pravu na pristup informacijama) u članku 5. stavku 7. definira test razmjernosti i javnog interesa kao procjenu razmjernosti između razloga za omogućavanje pristupa informaciji i razloga za ograničenje te omogućavanje pristupa informaciji ako prevladava javni interes.

Slijedom navedenog, Ministarstvo zaštite okoliša i energetike je sukladno članku 16. Zakona o pravu na pristup informacijama provelo test razmjernosti i javnog interesa te je imajući u vidu svrhu Zakona o kibernetičkoj sigurnosti, koji za cilj ima postizanje visoke zajedničke razine kibernetičke sigurnosti te definiciju rizika iz članka 4. stavka 1. točke 15. Zakona o kibernetičkoj sigurnosti kao bilo koje razumno prepoznatljive okolnosti ili događaja koji ima potencijalno negativni učinak na sigurnost mrežnih i informacijskih sustava, donijelo zaključak da bi objava popisa operatora ključnih usluga mogla u velikoj mjeri ugroziti sustav kibernetičke sigurnosti, te ga učiniti ranjivijim za napade. Testom razmjernosti i javnog interesa ocijenjeno je da bi više štete nastalo ako bi se podnositelju zahtjeva odnosno javnosti omogućila informacija o listi operatora ključnih usluga, čije je obavljanje djelatnosti u području nadležnosti tijela Središnjeg državnog ureda za razvoj digitalnog društva, nego što bi štete nastalo za podnositelja zahtjeva koji bez te informacije ne bi mogao provesti namjeravano istraživanje, izravnim upitom organizacijama, stoga podnositelju zahtjeva nije omogućen pristup zatraženoj informaciji.

Sukladno navedenom odlučeno je kao u izreci.

UPUTA O PRAVNOM LIJEKU:

Protiv ovog rješenja može se izjaviti žalba Povjereniku za informiranje. Žalba se podnosi Ministarstvu zaštite okoliša i energetike u dva primjerka u roku od 15 dana od dana dostave rješenja.

REPUBLIKA HRVATSKA
1
ZAGREB

SLUŽBENICA ZA INFORMIRANJE
Kristina Tekić

Slika 9.6. Odgovor na zahtjev za pristup informacijama – sektor energetike (nastavak)

Obrazac broj 2

ZAHTJEV ZA PRISTUP INFORMACIJAMA

Podnositelj zahtjeva (ime i prezime / naziv, adresa / sjedište, telefon i/ili e-pošta)

Krunoslav Arbanas, [redacted], karbanas@foi.hr

Naziv tijela javne vlasti / sjedište i adresa

Ministarstvo mora, prometa i infrastrukture, Prisavlje 14, 10 000 Zagreb

Informacija koja se traži

Popis identificiranih tvrtki operatora ključnih usluga iz sektora prijevoza sukladno Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/2018) za potrebe provođenja znanstvenog istraživanja u sklopu izrade doktorske disertacije na temu „Razvoj okvira za evaluaciju i uspostavu kulture informacijske sigurnosti".
Obrazloženje: Popis je potreban isključivo iz razloga kako bi se uspjele identificirati organizacije kojima bi se uputio dopis s objašnjenjem predloženog istraživanja te anketnim upitnikom koji bi zaposlenici tih organizacija mogli dobrovoljno popuniti i ne bi se koristio u druge svrhe. Upitnikom se ne bi prikupljali nikakvi osobni niti povjerljivi podaci, a popunjavanje upitnika bilo bi u potpunosti anonimno. Također, nigdje se ne bi spominjali nazivi organizacija već samo sektor kojem pripadaju sukladno kategorizaciji iz spomenutog Zakona. Rezultati istraživanja koristit će se isključivo u istraživačke svrhe, a sudionici će dobiti sumarne i obrađene rezultate koji im mogu biti korisni za unaprjeđenje upravljanja sigurnošću.

Način pristupa informaciji *(označiti)*

- ☐ neposredan pristup informaciji,
- ☐ pristup informaciji pisanim putem
- ☐ uvid u dokumente i izrada preslika dokumenata koji sadrže traženu informaciju,
- ☐ dostavljanje preslika dokumenata koji sadrži traženu informaciju,
- ☒ na drugi prikladan način (elektronskim putem ili drugo)

putem e-maila

Arbanas K.

(vlastoručni potpis podnositelja zahtjeva)

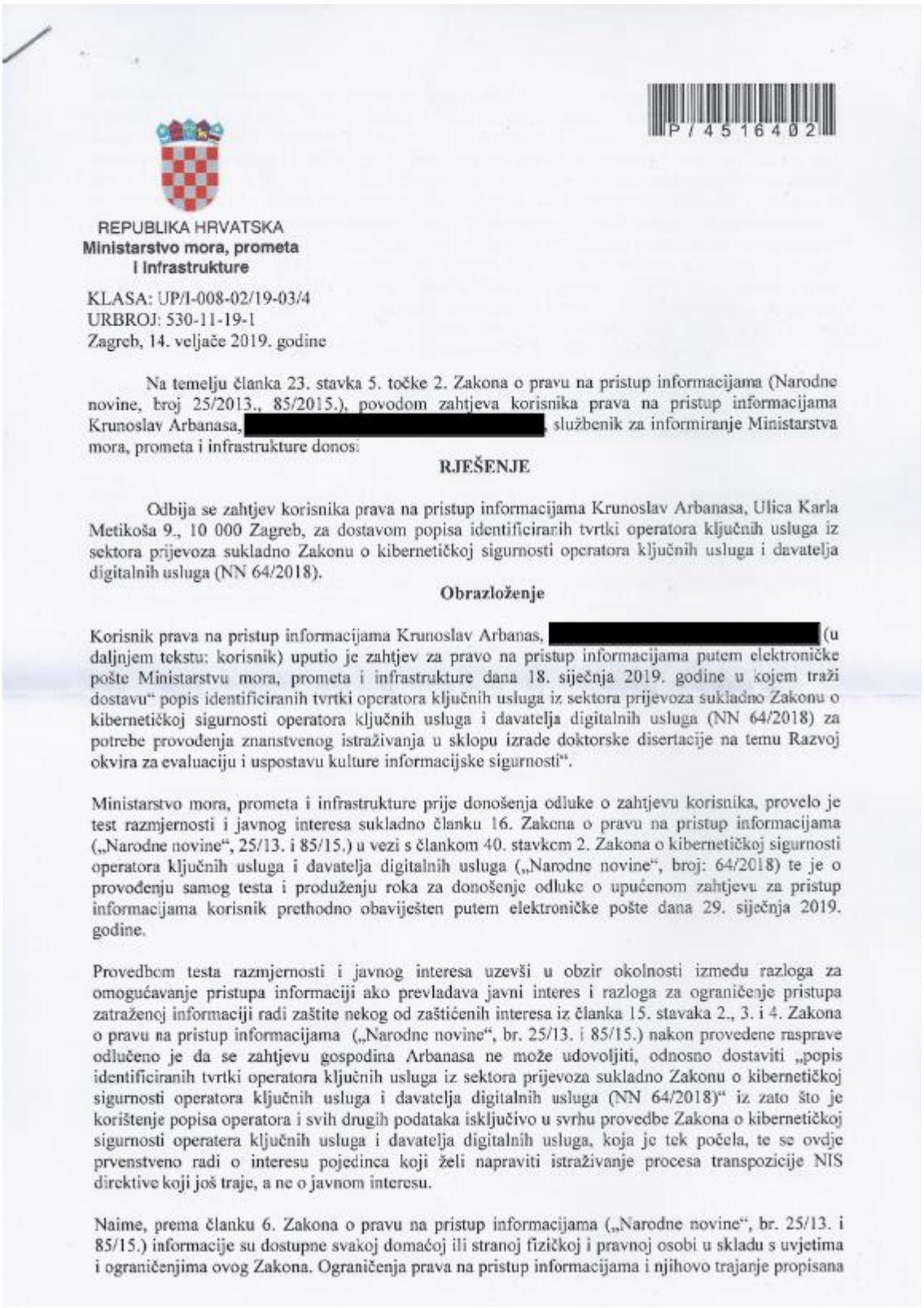
Zagreb, 18.01.2019.

(mjesto i datum)

Napomena: *Tijelo javne vlasti ima pravo na naknadu stvarnih materijalnih troškova od podnositelja zahtjeva u svezi s pružanjem i dostavom tražene informacije.*

Obrazac broj 2 – Obrazac zahtjeva za pristup informaciji

Slika 9.7. Zahtjev za pristup informacijama – sektor prijevoza



REPUBLIKA HRVATSKA
Ministarstvo mora, prometa i infrastrukture

KLASA: UP/I-008-02/19-03/4
URBROJ: 530-11-19-1
Zagreb, 14. veljače 2019. godine

Na temelju članka 23. stavka 5. točke 2. Zakona o pravu na pristup informacijama (Narodne novine, broj 25/2013., 85/2015.), povodom zahtjeva korisnika prava na pristup informacijama Krunoslav Arbanasa, [redacted], službenik za informiranje Ministarstva mora, prometa i infrastrukture donosi

RJEŠENJE

Odbija se zahtjev korisnika prava na pristup informacijama Krunoslav Arbanasa, Ulica Karla Metikoša 9., 10 000 Zagreb, za dostavom popisa identificiranih tvrtki operatora ključnih usluga iz sektora prijevoza sukladno Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/2018).

Obrazloženje

Korisnik prava na pristup informacijama Krunoslav Arbanas, [redacted] (u daljnjem tekstu: korisnik) uputio je zahtjev za pravo na pristup informacijama putem elektroničke pošte Ministarstvu mora, prometa i infrastrukture dana 18. siječnja 2019. godine u kojem traži dostavu" popis identificiranih tvrtki operatora ključnih usluga iz sektora prijevoza sukladno Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/2018) za potrebe provođenja znanstvenog istraživanja u sklopu izrade doktorske disertacije na temu Razvoj okvira za evaluaciju i uspostavu kulture informacijske sigurnosti".

Ministarstvo mora, prometa i infrastrukture prije donošenja odluke o zahtjevu korisnika, provelo je test razmjernosti i javnog interesa sukladno članku 16. Zakona o pravu na pristup informacijama („Narodne novine", 25/13. i 85/15.) u vezi s člankom 40. stavkom 2. Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine", broj: 64/2018) te je o provođenju samog testa i produženju roka za donošenje odluke o upućenom zahtjevu za pristup informacijama korisnik prethodno obaviješten putem elektroničke pošte dana 29. siječnja 2019. godine.

Provedbom testa razmjernosti i javnog interesa uzevši u obzir okolnosti između razloga za omogućavanje pristupa informaciji ako prevladava javni interes i razloga za ograničenje pristupa zatraženoj informaciji radi zaštite nekog od zaštićenih interesa iz članka 15. stavaka 2., 3. i 4. Zakona o pravu na pristup informacijama („Narodne novine", br. 25/13. i 85/15.) nakon provedene rasprave odlučeno je da se zahtjevu gospodina Arbanasa ne može udovoljiti, odnosno dostaviti „popis identificiranih tvrtki operatora ključnih usluga iz sektora prijevoza sukladno Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/2018)" iz zato što je korištenje popisa operatora i svih drugih podataka isključivo u svrhu provedbe Zakona o kibernetičkoj sigurnosti operatera ključnih usluga i davatelja digitalnih usluga, koja je tek počela, te se ovdje prvenstveno radi o interesu pojedinca koji želi napraviti istraživanje procesa transpozicije NIS direktive koji još traje, a ne o javnom interesu.

Naime, prema članku 6. Zakona o pravu na pristup informacijama („Narodne novine", br. 25/13. i 85/15.) informacije su dostupne svakoj domaćoj ili stranoj fizičkoj i pravnoj osobi u skladu s uvjetima i ograničenjima ovog Zakona. Ograničenja prava na pristup informacijama i njihovo trajanje propisana

Slika 9.8. Odgovor na zahtjev za pristup informacijama – sektor prijevoza

su člankom 15. Zakona o pravu na pristup informacijama („Narodne novine“, br. 25/13. i 85/15.), gdje u članku 15. stavku 2. točci 7. istog Zakona stoji da se može ograničiti pristup informaciji u ostalim slučajevima utvrđenim zakonom. Prema članku 40. stavku 1. Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine“, broj: 64/2018) popisi operatora ključnih usluga, kao i svi drugi podaci koji nastaju u okviru provedbe ovog Zakona koriste se isključivo u svrhu izvršavanja zahtjeva iz ovog Zakona. Člankom 11. stavkom 1. Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine“, broj: 64/2018) propisano je da svaki subjekt koji pruža neku od ključnih usluga dužan je nadležnom sektorskom tijelu, na njegov zahtjev, dostaviti podatke koji su mu potrebni za provođenje postupka identifikacije operatora ključnih usluga. Nadalje, pravo na pristup informacijama pripada svim korisnicima na jednak način i pod jednakim uvjetima i korisnici su ravnopravni u njegovom ostvarivanju, uz nepostojanje zakonske obveze navođenja razloga zbog kojih traže pristup informacijama, te dobivenu informaciju mogu javno iznositi bez ikakvog ograničenja.

Zaključno, uzevši u obzir sve okolnosti između razloga za omogućavanje pristupa informaciji i njenog ograničenja utvrđene samim testom razmjernosti i javnog interesa, odlučeno je da se zahtjevu korisnika ne može udovoljiti, te prevladava potreba na ograničenje pristupa informaciji i sama zaštita iste, a ne javni interes.

Temeljem svega iznijetog, a sukladno članku 23. stavka 5. točke 2., a u vezi s člankom 16. stavkom 1. i 2. Zakona o pravu na pristup informacijama, riješeno je kao u izreci.

Uputa o pravnom lijeku:
Protiv ovog Rješenja može se izjaviti žalba Povjereniku za informiranje (Zagreb, Jurišićeva 19) u roku od 15 dana od dana dostave Rješenja.

REPUBLIKA HRVATSKA
MINISTARSTVO MORA, PROMETA I INFRASTRUKTURE
ZAGREB

SLUŽBENIK ZA INFORMIRANJE

V. Gregurić

Vjekoslav Gregurić

Dostaviti:
1. Krunoslav Arbanas, Ulica Karla Metikoša 9, 10 000 Zagreb (preporučenom poštom s povratnicom)
2. Pismohrana

Slika 9.8. Odgovor na zahtjev za pristup informacijama – sektor prijevoza (nastavak)

Obrazac broj 2

ZAHTJEV ZA PRISTUP INFORMACIJAMA

Podnositelj zahtjeva (ime i prezime / naziv, adresa / sjedište, telefon i/ili e-pošta)
Krunoslav Arbanas, [redacted], karbanas@foi.hr

Naziv tijela javne vlasti / sjedište i adresa
Središnji državni ured za razvoj digitalnog društva, Ivana Lučića 8, 10 000 Zagreb

Informacija koja se traži
Popis identificiranih tvrtki operatora ključnih usluga iz sektora digitalne infrastrukture sukladno Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/2018) za potrebe provođenja znanstvenog istraživanja u sklopu izrade doktorske disertacije na temu „Razvoj okvira za evaluaciju i uspostavu kulture informacijske sigurnosti". **Obrazloženje: Popis je potreban isključivo iz razloga kako bi se uspjele identificirati organizacije kojima bi se uputio dopis s objašnjenjem predloženog istraživanja te anketnim upitnikom koji bi zaposlenici tih organizacija mogli dobrovoljno popuniti i ne bi se koristio u druge svrhe. Upitnikom se ne bi prikupljali nikakvi osobni niti povjerljivi podaci, a popunjavanje upitnika bilo bi u potpunosti anonimno. Također, nigdje se ne bi spominjali nazivi organizacija već samo sektor kojem pripadaju sukladno kategorizaciji iz spomenutog Zakona. Rezultati istraživanja koristit će se isključivo u istraživačke svrhe, a sudionici će dobiti sumarne i obrađene rezultate koji im mogu biti korisni za unaprjeđenje upravljanja sigurnošću.**

Način pristupa informaciji *(označiti)*
☐ neposredan pristup informaciji, ☐ pristup informaciji pisanim putem ☐ uvid u dokumente i izrada preslika dokumenata koji sadrže traženu informaciju, ☐ dostavljanje preslika dokumenata koji sadrži traženu informaciju, ☒ na drugi prikladan način (elektronskim putem ili drugo) putem e-maila

Arbanas K.

(vlastoručni potpis podnositelja zahtjeva)

Zagreb, 18.01.2019.

(mjesto i datum)

Napomena: *Tijelo javne vlasti ima pravo na naknadu stvarnih materijalnih troškova od podnositelja zahtjeva u svezi s pružanjem i dostavom tražene informacije.*

Obrazac broj 2 – Obrazac zahtjeva za pristup informaciji

Slika 9.9. Zahtjev za pristup informacijama – sektor digitalne infrastrukture

REPUBLIKA HRVATSKA
Središnji državni ured
za razvoj digitalnog društva
Zagreb, Ivana Lučića 8

KLASA: 008-02/19-02/03
URBROJ: 520-04-01-1/1-19-05
Zagreb, 18. veljače 2019.

Službenik za informiranje na temelju članka 15. stavak 2. točka 7. i članka 23. stavak 5. točka 2., a u vezi s člankom 16. stavkom 1. Zakona o pravu na pristup informacijama („Narodne novine", broj 25/13, 85/15) i provedenog Testa razmjernosti i javnog interesa, KLASA: 008-02/19-02/03, URBROJ: 520-04-01-1/1-19-04 od dana 14. veljače 2019. godine, u predmetu ostvarivanja prava na pristup informacijama Krunoslava Arbanasa iz [redacted] donosi slijedeće

R J E Š E NJ E

Odbija se zahtjev Krunoslava Arbanasa iz [redacted] za pristup informaciji: popis identificiranih tvrtki operatora ključnih usluga iz sektora digitalne infrastrukture, iz nadležnosti Središnjeg državnog ureda za razvoj digitalnog društva, kao nadležnog sektorskog tijela za odredivanje operatora ključnih usluga iz sektora digitalne infrastrukture, sukladno odredbama Zakona o kibernetičkoj sigurnosti operatera ključnih usluga i davatelja digitalnih usluga („Narodne novine", broj 64/2018), podnesenog dana 18. siječnja 2019. godine.

Obrazloženje:

Dana 18. siječnja 2019. godine, Krunoslav Arbanas iz [redacted], podnio je putem elektroničke pošte zahtjev za pristup informacijama, koji je u ovom tijelu državne uprave zaprimljen istoga dana, KLASA: 008-02/19-02/03, URBROJ: 15-19-01, za dostavom popisa identificiranih operatora ključnih usluga iz sektora digitalne infrastrukture, od Središnjeg državnog ureda za razvoj digitalnog društva, kao nadležnog sektorskog tijela, sukladno odredbama Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine", broj 64/2018), u svrhu provođenja znanstvenog istraživanja.

Korisnik prava na pristup informacijama, traži popis operatora ključnih usluga u cilju izrade doktorske disertacije „Razvoj okvira za evaluaciju i uspostavu kulture informacijske sigurnosti", u svojstvu doktoranda na poslijediplomskom doktorskom studiju Informacijske znanosti na Fakultetu organizacije i informatike u Varaždinu Sveučilišta u Zagrebu, a koji mu je potreban u svrhu identifikacije organizacija kojima bi uputio dopis s namjerom provođenja empirijskog istraživanja o razini kulture informacijske sigurnosti, odnosno procjeni elemenata koji čine kulturu informacijske sigurnosti u kontekstu nacionalne kritične infrastrukture, odnosno pružanja ključnih usluga. Anketni upitnik bi uputio na adrese iz popisa, zajedno s objašnjenjem predloženog istraživanja, koji bi zaposlenici tih organizacija mogli dobrovoljno popuniti, a kojim upitnikom se ne bi prikupljali nikakvi osobni niti povjerljivi podaci, popunjavanje bi bilo u potpunosti anonimno, a nigdje se ne bi spominjali nazivi organizacija

Slika 9.10. Odgovor na zahtjev za pristup informacijama – sektor digitalne infrastrukture

već samo sektor kojem pripadaju. Rezultati istraživanja bi se koristili isključivo u istraživačke svrhe, a sudionici bi dobili sumarne i obrađene rezultate koji bi im mogli biti korisni za unaprjeđenje upravljanja sigurnošću.

Službenica za informiranje je zaprimila i evidentirala zahtjev za pristup informacijama u službeni upisnik te je utvrdila da je zahtjev potpun i razumljiv, te da sadrži osnovne podatke o korisniku i podatke na osnovu kojih se može jasno utvrditi koju informaciju korisnik traži. Utvrđeno je i da se na zahtjev primjenjuje Zakon o pravu na pristup informacijama („Narodne novine“, broj 25/2013, 85/2015), te da podnositelj zahtjeva traži informaciju u smislu članka 5. stavka 1. točke 3. Zakona. Službenica za informiranje utvrdila je da se ne radi o zlouporabi prava na pristup informacijama, određeno člankom 23. stavkom 5. točke 5. Zakona. Također je utvrđeno da tražena informacija nije javno objavljena te da se informacija nalazi u posjedu Središnjeg državnog ureda za razvoj digitalnog društva, u Sektoru za planiranje i strategiju razvoja digitalnog društva. Prilikom razmatranja zahtjeva i razgovora s osobama iz nadležne ustrojstvene jedinice, službenica za informiranje je utvrdila da postoji relativno zakonsko ograničenje pristupa informaciji iz članka 15. stavka 2. točke 7. Zakona.

S obzirom na utvrđeno, zaključak službenice za informiranje jest da treba provesti test razmjernosti i javnog interesa, temeljem članka 16. Zakona i u ovisnosti o rezultatima donijeti odluku. Sukladno navedenom, u otvorenom zakonskom roku, službenik za informiranje obavijestio je podnositelja zahtjeva da se rok za ostvarivanje prava na pristup informacijama produžava, sukladno odredbi članka 22. stavka 1. točke 4. Zakona o pravu na pristup informacijama (KLASA: 008-02/19-02/03, URBROJ: 520-04-01-1/1-19-02). Temeljem članka 45. Zakona o sustavu državne uprave ("Narodne novine", broj 150/2011, 12/2013, 93/2016, 104/2016), državni tajnik Središnjeg državnog ureda za razvoj digitalnog društva je, dana 8. veljače 2019. godine, donio Odluku o imenovanju radne skupine za provedbu testa razmjernosti i javnog interesa u predmetu zahtjeva za pristup informacijama, u predmetu KLASA: 008-02/19-02/03, URBROJ: 520-04-01-1/1-19-03. Radna skupina za provođenje testa razmjernosti i javnog interesa provela je, dana 14. veljače 2019. godine, Test razmjernosti i javnog interesa u predmetu zahtjeva za pristup informacijama, u rubriciranom predmetu.

Pristup informacijama u smislu Zakona o pravu na pristup informacijama obuhvaća pravo korisnika na traženje i dobivanje informacije kao i obvezu tijela javne vlasti da omogući pristup zatraženoj informaciji, odnosno da objavljuje informacije neovisno o postavljenom zahtjevu kada takvo objavljivanje proizlazi iz obveze određene zakonom ili drugim propisom.

Člankom 6. Zakona o pravu na pristup informacijama propisano je da su informacije dostupne svakoj domaćoj ili stranoj fizičkoj i pravnoj osobi u skladu s uvjetima i ograničenjima ovoga Zakona.

Članak 9. navodi da korisnik koji raspolaže informacijom sukladno ovom Zakonu, ima pravo tu informaciju javno iznositi.

Odredbom članka 23. stavka 5. točke 2. istog Zakona propisano je da će tijelo javne vlasti rješenjem odbiti zahtjev ako se ispune uvjeti propisani u članku 15. stavcima 2., 3. i 4., a u vezi s člankom 16. stavkom 1. tog Zakona.

Člankom 16. stavkom 1. istog Zakona propisano je da je tijelo javne vlasti nadležno za postupanje po zahtjevu za pristup informaciji iz članka 15. stavka 2. točke 2., 3., 4., 5., 6. i 7. i

Slika 9.10. Odgovor na zahtjev za pristup informacijama – sektor digitalne infrastrukture (nastavak)

stavaka 3. i 4. ovoga Zakona, dužno prije donošenja odluke, provesti test razmjernosti i javnog interesa.

Test razmjernosti i javnog interesa je procjena razmjernosti između razloga za omogućavanje pristupa informaciji i razloga za ograničenje te omogućavanje pristupa informaciji ako prevladava javni interes.

Stavkom 2. članka 16. istog Zakona propisano je da je kod provođenja testa razmjernosti i javnog interesa tijelo javne vlasti dužno utvrditi da li se pristup informaciji može ograničiti radi zaštite nekog od zaštićenih interesa iz članka 15. stavaka 2., 3. i 4. Zakona, gdje u članku 15. stavku 2. točki 7. istog Zakona stoji da se može ograničiti pristup informaciji u ostalim slučajevima utvrđenim zakonom.

Korisnik prava na pristup informacijama u svom zahtjevu traži popis identificiranih operatora ključnih usluga iz sektora digitalne infrastrukture za državna tijela, iz nadležnosti ovog tijela državne uprave, sukladno odredbama Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine“, broj 64/2018).

Slijedom navedenog, odredbama Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga propisano je i utvrđivanje popisa operatora ključnih usluga od strane nadležnog sektorskog tijela, za koje je, u području digitalne infrastrukture i poslovnih usluga za državna tijela, nadležan Središnji državni ured za razvoj digitalnog društva, sukladno Popisu nadležnih tijela iz Priloga III. Zakona.

Članak 40. Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga u stavku 1., određuje da se popisi operatora ključnih usluga, kao i svi drugi podaci koji nastaju u okviru provedbe tog Zakona koriste isključivo u svrhu izvršavanja zahtjeva iz tog Zakona.

Zakonom o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, uređuju se postupci i mjere za postizanje visoke zajedničke razine kibernetičke sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, nadležnosti i ovlasti nadležnih sektorskih tijela, jedinstvene nacionalne kontaktne točke, tijela nadležnih za prevenciju i zaštitu od incidenata i tehničkog tijela za ocjenu sukladnosti, nadzor nad operatorima ključnih usluga i davateljima digitalnih usluga u provedbi tog Zakona i prekršajne odredbe (članak 1. stavak 1.).

Cilj ovoga Zakona je osigurati provedbu mjera za postizanje visoke zajedničke razine kibernetičke sigurnosti u davanju usluga koje su od posebne važnosti za odvijanje ključnih društvenih i gospodarskih aktivnosti, uključujući i funkcioniranje digitalnog tržišta, što je sadržano u odredbi članka 1. stavka 2. Zakona.

Sigurnost mrežnih i informacijskih sustava je sposobnost mrežnih i informacijskih sustava da, na određenoj razini pouzdanosti, odolijevaju bilo kojoj radnji koja ugrožava dostupnost, autentičnost, cjelovitost ili povjerljivost, pohranjenih, prenesenih ili obrađenih podataka, ili srodnih usluga koje ti mrežni i informacijski sustavi nude ili kojima omogućuju pristup (članak 5. stavak 1. točka 4.).

Radna skupina je, provodeći Test razmjernosti i javnog interesa utvrdila da je razlog da se informacija učini dostupnom spoznavanje razine kulture informacijske sigurnosti, odnosno

Slika 9.10. Odgovor na zahtjev za pristup informacijama – sektor digitalne infrastrukture (nastavak)

procjene elemenata koji čine kulturu informacijske sigurnosti u kontekstu nacionalne, kritične informatičke strukture odnosno pružanja ključnih usluga od strane podnositelja zahtjeva.

Radna skupina je, također, utvrdila da je razlog protiv omogućavanja pristupa informaciji sadržaj odredbe članka 40. stavak 1. Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine", broj: 64/2018), koja propisuje da se popisi operatora ključnih usluga, kao i svi drugi podaci koji nastaju u okviru provedbe tog Zakona koriste isključivo u svrhu izvršavanja zahtjeva iz tog Zakona, a u svezi sa stavkom 2. članka 40. citiranog Zakona, kojom je propisano da popis i podaci iz stavka 1. toga članka predstavljaju informacije u odnosu na koje je moguće ograničiti pravo pristupa korisniku informacija, ovisno o rezultatima testa razmjernosti i javnog interesa koji se provodi prema odredbama posebnog zakona o pravu na pristup informacijama, a koji je kao razlog ograničenja prava na pristup informacijama sadržan u odredbi članka 15. stavak 2. točka 7. Zakona o pravu na pristup informacijama.

Slijedom navedenog, Radna skupina za provođenje Testa razmjernosti i javnog interesa, zaključila je da interes javnosti da dođe do informacije o popisu operatora ključnih usluga u cilju izrade disertacije „Razvoj okvira za evaluaciju i uspostavu kulture informacijska sigurnosti" ne prevladava nad štetom koja bi nastala zbog povrede zaštićenog interesa, na temelju utvrđenog:

- Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga određuje da se popis operatora ključnih usluga koristi isključivo u svrhu izvršavanja zahtjeva iz tog Zakona, a da pri tom Zakonom nije nigdje propisana obveza javne objave toga popisa, a nije naznačena niti druga svrha korištenja predmetnog popisa i drugih podataka koji nastaju u okviru provedbe toga Zakona, osim navedene,

- objavom popisa operatora ključnih usluga, postoji vjerojatnost smanjenja uspješnosti odolijevanja radnjama koje ugrožavaju dostupnost, autentičnost, cjelovitost ili povjerljivost podatka ili srodnih usluga, odnosno može se smatrati rizikom, koji pojam Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga definira u članku 5. stavku 1. točki 15., kao razumno prepoznatljivu okolnost ili događaj koji ima potencijalno negativni učinak na sigurnost mrežnih i informacijskih sustava,

- omogućavanje informacije nije na tragu ostvarenja cilja Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, postizanja visoke zajedničke razine kibernetičke sigurnosti, koju bi objava popisa operatora ključnih usluga mogla u određenoj mjeri ugroziti, te učiniti ranjivijima za napade,

- traženi popis predstavlja osjetljivu informaciju, a korisnik koji ostvari pristup informaciji, sukladno Zakonu o pravu na pristup informacijama, ima pravo tu informaciju javno iznositi,

- ne postoji zainteresiranost šireg kruga ljudi, a predmetni popis sadrži operativno osjetljive podatke, čije bi iznošenje moglo dovesti u pitanje uspješno obavljanje zakonom utvrđenih zadaća, gdje javnost, pri tom, ne bi bila ništa jasnije informirana,

- omogućavanje pristupa informaciji doprinijelo bi javnom interesu u smislu ostvarivanja temeljnih vrijednosti društvenog poretka i specifičnim načelima funkcioniranja tijela javne vlasti, kao što su kontrola rada tijela javne vlasti i pravilnost provedbe zakona, međutim isti u konkretnom slučaju ne prevladava. Javni interes bi, primjerice, bio u tome da je javnost

Slika 9.10. Odgovor na zahtjev za pristup informacijama – sektor digitalne infrastrukture (nastavak)

upoznata s informacijom jesu li identificirani operatori ključnih usluga, a ne javna objava utvrđenog popisa operatora ključnih usluga.

Testom razmjernosti i javnog interesa je ocijenjeno da bi više štete nastalo ako bi se podnositelju zahtjeva odnosno javnosti omogućila informacija o popisu operatora ključnih usluga, čije obavljanje djelatnosti u području za koje je nadležno tijelo Središnji državni ured za razvoj digitalnog društva, nego što bi štete nastalo za podnositelja zahtjeva koji bez te informacije ne bi mogao provesti namjeravano istraživanje izravnim upitom organizacijama, stoga podnositelju zahtjeva nije omogućen pristup zatraženoj informaciji.

Slijedom svega navedenog, a temeljem članka 23. stavak 5. točka 2. Zakona o pravu na pristup informacijama („Narodne novine", broj 25/13, 85/15), odlučeno je kao u izreci ovog rješenja.

UPUTA O PRAVNOM LIJEKU:

Protiv ovog rješenja može se izjaviti žalba Povjereniku za informiranje u roku od 15 dana od dana dostave rješenja. Žalba se izjavljuje putem tijela javne vlasti. Sukladno članku 19. Zakona o pravu na pristup informacijama u postupcima ostvarivanja prava na pristup informacijama se ne plaćaju upravne pristojbe.

SLUŽBENICA ZA INFORMIRANJE

Tamara Horvat Klemen

DOSTAVITI:
1. Krunoslav Arbanas, [redacted]
2. Pismohrana, ovdje

Slika 9.10. Odgovor na zahtjev za pristup informacijama – sektor digitalne infrastrukture (nastavak)

Obrazac broj 2

ZAHTJEV ZA PRISTUP INFORMACIJAMA

Podnositelj zahtjeva (ime i prezime / naziv, adresa / sjedište, telefon i/ili e-pošta)
Krunoslav Arbanas, [redacted], karbanas@foi.hr

Naziv tijela javne vlasti / sjedište i adresa
Središnji državni ured za razvoj digitalnog društva, Ivana Lučića 8, 10 000 Zagreb

Informacija koja se traži
Popis identificiranih tvrtki operatora ključnih usluga iz sektora poslovnih usluga za državna tijela sukladno Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/2018) za potrebe provođenja znanstvenog istraživanja u sklopu izrade doktorske disertacije na temu „Razvoj okvira za evaluaciju i uspostavu kulture informacijske sigurnosti". **Obrazloženje: Popis je potreban isključivo iz razloga kako bi se uspjele identificirati organizacije kojima bi se uputio dopis s objašnjenjem predloženog istraživanja te anketnim upitnikom koji bi zaposlenici tih organizacija mogli dobrovoljno popuniti i ne bi se koristio u druge svrhe. Upitnikom se ne bi prikupljali nikakvi osobni niti povjerljivi podaci, a popunjavanje upitnika bilo bi u potpunosti anonimno. Također, nigdje se ne bi spominjali nazivi organizacija već samo sektor kojem pripadaju sukladno kategorizaciji iz spomenutog Zakona. Rezultati istraživanja koristit će se isključivo u istraživačke svrhe, a sudionici će dobiti sumarne i obrađene rezultate koji im mogu biti korisni za unaprjeđenje upravljanja sigurnošću.**

Način pristupa informaciji *(označiti)*
☐ neposredan pristup informaciji, ☐ pristup informaciji pisanim putem ☐ uvid u dokumente i izrada preslika dokumenata koji sadrže traženu informaciju, ☐ dostavljanje preslika dokumenata koji sadrži traženu informaciju, ☒ na drugi prikladan način (elektronskim putem ili drugo) putem e-maila

Arbanas K.

(vlastoručni potpis podnositelja zahtjeva)

Zagreb, 18.01.2019.

(mjesto i datum)

Napomena: *Tijelo javne vlasti ima pravo na naknadu stvarnih materijalnih troškova od podnositelja zahtjeva u svezi s pružanjem i dostavom tražene informacije.*

Obrazac broj 2 – Obrazac zahtjeva za pristup informaciji

Slika 9.11. Zahtjev za pristup informacijama – sektor poslovnih usluga za državna tijela

REPUBLIKA HRVATSKA
Središnji državni ured
za razvoj digitalnog društva
Zagreb, Ivana Lučića 8

KLASA: 008-02/19-02/02
URBROJ: 520-04-01-1/1-19-05
Zagreb, 18. veljače 2019.

Službenik za informiranje na temelju članka 15. stavak 2. točka 7. i članka 23. stavak 5. točka 2., a u vezi s člankom 16. stavkom 1. Zakona o pravu na pristup informacijama („Narodne novine", broj 25/13, 85/15) i provedenog Testa razmjernosti i javnog interesa, KLASA: 008-02/19-02/02, URBROJ: 520-04-01-1/1-19-04 od dana 14. veljače 2019. godine, u predmetu ostvarivanja prava na pristup informacijama Krunoslava Arbanasa iz [redacted], donosi slijedeće

R J E Š E NJ E

Odbija se zahtjev Krunoslava Arbanasa iz [redacted] za pristup informaciji: popis identificiranih tvrtki operatora ključnih usluga iz sektora poslovnih usluga za državna tijela, iz nadležnosti Središnjeg državnog ureda za razvoj digitalnog društva, kao nadležnog sektorskog tijela za određivanje operatora ključnih usluga iz sektora poslovnih usluga, sukladno odredbama Zakona o kibernetičkoj sigurnosti operatera ključnih usluga i davatelja digitalnih usluga („Narodne novine", broj 64/2018), podnesenog dana 18. siječnja 2019. godine.

Obrazloženje:

Dana 18. siječnja 2019. godine, Krunoslav Arbanas iz [redacted], podnio je putem elektroničke pošte zahtjev za pristup informacijama, koji je u ovom tijelu državne uprave zaprimljen istoga dana, KLASA: 008-02/19-02/02, URBROJ: 15-19-01, za dostavom popisa identificiranih operatora ključnih usluga iz sektora poslovnih usluga za državna tijela, od Središnjeg državnog ureda za razvoj digitalnog društva, kao nadležnog sektorskog tijela, sukladno odredbama Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine", broj 64/2018), u svrhu provođenja znanstvenog istraživanja.

Korisnik prava na pristup informacijama, traži popis operatora ključnih usluga u cilju izrade doktorske disertacije „Razvoj okvira za evaluaciju i uspostavu kulture informacijske sigurnosti", u svojstvu doktoranda na poslijediplomskom doktorskom studiju Informacijske znanosti na Fakultetu organizacije i informatike u Varaždinu Sveučilišta u Zagrebu, a koji mu je potreban u svrhu identifikacije organizacija kojima bi uputio dopis s namjerom provođenja empirijskog istraživanja o razini kulture informacijske sigurnosti, odnosno procjeni elemenata koji čine kulturu informacijske sigurnosti u kontekstu nacionalne kritične infrastrukture, odnosno pružanja ključnih usluga. Anketni upitnik bi uputio na adrese iz popisa, zajedno s objašnjenjem predloženog istraživanja, koji bi zaposlenici tih organizacija mogli dobrovoljno popuniti, a kojim upitnikom se ne bi prikupljali nikakvi osobni niti povjerljivi podaci, popunjavanje bi bilo u potpunosti anonimno, a nigdje se ne bi spominjali

Slika 9.12. Odgovor na zahtjev za pristup informacijama – sektor poslovnih usluga za državna tijela

nazivi organizacija već samo sektor kojem pripadaju. Rezultati istraživanja bi se koristili isključivo u istraživačke svrhe, a sudionici bi dobili sumarne i obrađene rezultate koji bi im mogli biti korisni za unaprjeđenje upravljanja sigurnošću.

Službenica za informiranje je zaprimila i evidentirala zahtjev za pristup informacijama u službeni upisnik te je utvrdila da je zahtjev potpun i razumljiv, te da sadrži osnovne podatke o korisniku i podatke na osnovu kojih se može jasno utvrditi koju informaciju korisnik traži. Utvrđeno je i da se na zahtjev primjenjuje Zakon o pravu na pristup informacijama („Narodne novine“, broj 25/2013, 85/2015), te da podnositelj zahtjeva traži informaciju u smislu članka 5. stavka 1. točke 3. Zakona. Službenica za informiranje utvrdila je da se ne radi o zlouporabi prava na pristup informacijama, određeno člankom 23. stavkom 5. točke 5. Zakona. Također je utvrđeno da tražena informacija nije javno objavljena te da se informacija nalazi u posjedu Središnjeg državnog ureda za razvoj digitalnog društva, u Sektoru za planiranje i strategiju razvoja digitalnog društva. Prilikom razmatranja zahtjeva i razgovora s osobama iz nadležne ustrojstvene jedinice, službenica za informiranje je utvrdila da postoji relativno zakonsko ograničenje pristupa informaciji iz članka 15. stavka 2. točke 7. Zakona.

S obzirom na utvrđeno, zaključak službenice za informiranje jest da treba provesti test razmjernosti i javnog interesa, temeljem članka 16. Zakona i u ovisnosti o rezultatima donijeti odluku. Sukladno navedenom, u otvorenom zakonskom roku, službenik za informiranje obavijestio je podnositelja zahtjeva da se rok za ostvarivanje prava na pristup informacijama produžava, sukladno odredbi članka 22. stavka 1. točke 4. Zakona o pravu na pristup informacijama (KLASA: 008-02/19-02/02, URBROJ: 520-04-01-1/1-19-02). Temeljem članka 45. Zakona o sustavu državne uprave ("Narodne novine", broj 150/2011, 12/2013, 93/2016, 104/2016), državni tajnik Središnjeg državnog ureda za razvoj digitalnog društva je, dana 8. veljače 2019. godine, donio Odluku o imenovanju radne skupine za provedbu testa razmjernosti i javnog interesa u predmetu zahtjeva za pristup informacijama, u predmetu KLASA: 008-02/19-02/02, URBROJ: 520-04-01-1/1-19-03. Radna skupina za provođenje testa razmjernosti i javnog interesa provela je, dana 14. veljače 2019. godine, Test razmjernosti i javnog interesa u predmetu zahtjeva za pristup informacijama, u rubriciranom predmetu.

Pristup informacijama u smislu Zakona o pravu na pristup informacijama obuhvaća pravo korisnika na traženje i dobivanje informacije kao i obvezu tijela javne vlasti da omogući pristup zatraženoj informaciji, odnosno da objavljuje informacije neovisno o postavljenom zahtjevu kada takvo objavljivanje proizlazi iz obveze određene zakonom ili drugim propisom.

Člankom 6. Zakona o pravu na pristup informacijama propisano je da su informacije dostupne svakoj domaćoj ili stranoj fizičkoj i pravnoj osobi u skladu s uvjetima i ograničenjima ovoga Zakona.

Članak 9. navodi da korisnik koji raspolaže informacijom sukladno ovom Zakonu, ima pravo tu informaciju javno iznositi.

Odredbom članka 23. stavka 5. točke 2. istog Zakona propisano je da će tijelo javne vlasti rješenjem odbiti zahtjev ako se ispune uvjeti propisani u članku 15. stavcima 2., 3. i 4., a u vezi s člankom 16. stavkom 1. tog Zakona.

Člankom 16. stavkom 1. istog Zakona propisano je da je tijelo javne vlasti nadležno za postupanje po zahtjevu za pristup informaciji iz članka 15. stavka 2. točke 2., 3., 4., 5., 6. i 7.

Slika 9.12. Odgovor na zahtjev za pristup informacijama – sektor poslovnih usluga za državna tijela (nastavak)

i stavaka 3. i 4. ovoga Zakona, dužno prije donošenja odluke, provesti test razmjernosti i javnog interesa.

Test razmjernosti i javnog interesa je procjena razmjernosti između razloga za omogućavanje pristupa informaciji i razloga za ograničenje te omogućavanje pristupa informaciji ako prevladava javni interes.

Stavkom 2. članka 16. istog Zakona propisano je da je kod provođenja testa razmjernosti i javnog interesa tijelo javne vlasti dužno utvrditi da li se pristup informaciji može ograničiti radi zaštite nekog od zaštićenih interesa iz članka 15. stavaka 2., 3. i 4. Zakona, gdje u članku 15. stavku 2. točki 7. istog Zakona stoji da se može ograničiti pristup informaciji u ostalim slučajevima utvrđenim zakonom.

Korisnik prava na pristup informacijama u svom zahtjevu traži popis identificiranih operatora ključnih usluga iz sektora poslovnih usluga za državna tijela, iz nadležnosti ovog tijela državne uprave, sukladno odredbama Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine“, broj 64/2018).

Slijedom navedenog, odredbama Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga propisano je i utvrđivanje popisa operatora ključnih usluga od strane nadležnog sektorskog tijela, za koje je, u području digitalne infrastrukture i poslovnih usluga za državna tijela, nadležan Središnji državni ured za razvoj digitalnog društva, sukladno Popisu nadležnih tijela iz Priloga III. Zakona.

Članak 40. Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga u stavku 1., određuje da se popisi operatora ključnih usluga, kao i svi drugi podaci koji nastaju u okviru provedbe tog Zakona koriste isključivo u svrhu izvršavanja zahtjeva iz tog Zakona.

Zakonom o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, uređuju se postupci i mjere za postizanje visoke zajedničke razine kibernetičke sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, nadležnosti i ovlasti nadležnih sektorskih tijela, jedinstvene nacionalne kontaktne točke, tijela nadležnih za prevenciju i zaštitu od incidenata i tehničkog tijela za ocjenu sukladnosti, nadzor nad operatorima ključnih usluga i davateljima digitalnih usluga u provedbi tog Zakona i prekršajne odredbe (članak 1. stavak 1.).

Cilj ovoga Zakona je osigurati provedbu mjera za postizanje visoke zajedničke razine kibernetičke sigurnosti u davanju usluga koje su od posebne važnosti za odvijanje ključnih društvenih i gospodarskih aktivnosti, uključujući i funkcioniranje digitalnog tržišta, što je sadržano u odredbi članka 1. stavka 2. Zakona.

Sigurnost mrežnih i informacijskih sustava je sposobnost mrežnih i informacijskih sustava da, na određenoj razini pouzdanosti, odolijevaju bilo kojoj radnji koja ugrožava dostupnost, autentičnost, cjelovitost ili povjerljivost, pohranjenih, prenesenih ili obrađenih podataka, ili srodnih usluga koje ti mrežni i informacijski sustavi nude ili kojima omogućuju pristup (članak 5. stavak 1. točka 4.).

Radna skupina je, provodeći Test razmjernosti i javnog interesa utvrdila da je razlog da se informacija učini dostupnom spoznavanje razine kulture informacijske sigurnosti, odnosno

Slika 9.12. Odgovor na zahtjev za pristup informacijama – sektor poslovnih usluga za državna tijela (nastavak)

procjene elemenata koji čine kulturu informacijske sigurnosti u kontekstu nacionalne, kritične informatičke strukture odnosno pružanja ključnih usluga od strane podnositelja zahtjeva.

Radna skupina je, također, utvrdila da je razlog protiv omogućavanja pristupa informaciji sadržaj odredbe članka 40. stavak 1. Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine“, broj: 64/2018), koja propisuje da se popisi operatora ključnih usluga, kao i svi drugi podaci koji nastaju u okviru provedbe tog Zakona koriste isključivo u svrhu izvršavanja zahtjeva iz tog Zakona, a u svezi sa stavkom 2. članka 40. citiranog Zakona, kojom je propisano da popis i podaci iz stavka 1. toga članka predstavljaju informacije u odnosu na koje je moguće ograničiti pravo pristupa korisniku informacija, ovisno o rezultatima testa razmjernosti i javnog interesa koji se provodi prema odredbama posebnog zakona o pravu na pristup informacijama, a koji je kao razlog ograničenja prava na pristup informacijama sadržan u odredbi članka 15. stavak 2. točka 7. Zakona o pravu na pristup informacijama.

Slijedom navedenog, Radna skupina za provođenje Testa razmjernosti i javnog interesa, zaključila je da interes javnosti da dođe do informacije o popisu operatora ključnih usluga u cilju izrade disertacije „Razvoj okvira za evaluaciju i uspostavu kulture informacijska sigurnosti“ ne prevladava nad štetom koja bi nastala zbog povrede zaštićenog interesa, na temelju utvrđenog:

- Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga određuje da se popis operatora ključnih usluga koristi isključivo u svrhu izvršavanja zahtjeva iz tog Zakona, a da pri tom Zakonom nije nigdje propisana obveza javne objave toga popisa, a nije naznačena niti druga svrha korištenja predmetnog popisa i drugih podataka koji nastaju u okviru provedbe toga Zakona, osim navedene,

- objavom popisa operatora ključnih usluga, postoji vjerojatnost smanjenja uspješnosti odolijevanja radnjama koje ugrožavaju dostupnost, autentičnost, cjelovitost ili povjerljivost podatka ili srodnih usluga, odnosno može se smatrati rizikom, koji pojam Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga definira u članku 5. stavku 1. točki 15., kao razumno prepoznatljivu okolnost ili događaj koji ima potencijalno negativni učinak na sigurnost mrežnih i informacijskih sustava,

- omogućavanje informacije nije na tragu ostvarenja cilja Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, postizanja visoke zajedničke razine kibernetičke sigurnosti, koju bi objava popisa operatora ključnih usluga mogla u određenoj mjeri ugroziti, te učiniti ranjivijima za napade,

- traženi popis predstavlja osjetljivu informaciju, a korisnik koji ostvari pristup informaciji, sukladno Zakonu o pravu na pristup informacijama, ima pravo tu informaciju javno iznositi,

- ne postoji zainteresiranost šireg kruga ljudi, a predmetni popis sadrži operativno osjetljive podatke, čije bi iznošenje moglo dovesti u pitanje uspješno obavljanje zakonom utvrđenih zadaća, gdje javnost, pri tom, ne bi bila ništa jasnije informirana,

- omogućavanje pristupa informaciji doprinijelo bi javnom interesu u smislu ostvarivanja temeljnih vrijednosti društvenog poretka i specifičnim načelima funkcioniranja tijela javne vlasti, kao što su kontrola rada tijela javne vlasti i pravilnost provedbe zakona, međutim isti u konkretnom slučaju ne prevladava. Javni interes bi, primjerice, bio u tome da je javnost

Slika 9.12. Odgovor na zahtjev za pristup informacijama – sektor poslovnih usluga za državna tijela (nastavak)

upoznata s informacijom jesu li identificirani operatori ključnih usluga, a ne javna objava utvrđenog popisa operatora ključnih usluga.

Testom razmjernosti i javnog interesa je ocijenjeno da bi više štete nastalo ako bi se podnositelju zahtjeva odnosno javnosti omogućila informacija o popisu operatora ključnih usluga, čije obavljanje djelatnosti u području za koje je nadležno tijelo Središnji državni ured za razvoj digitalnog društva, nego što bi štete nastalo za podnositelja zahtjeva koji bez te informacije ne bi mogao provesti namjeravano istraživanje izravnim upitom organizacijama, stoga podnositelju zahtjeva nije omogućen pristup zatraženoj informaciji.

Slijedom svega navedenog, a temeljem članka 23. stavak 5. točka 2. Zakona o pravu na pristup informacijama („Narodne novine", broj 25/13, 85/15), odlučeno je kao u izreci ovog rješenja.

UPUTA O PRAVNOM LIJEKU:

Protiv ovog rješenja može se izjaviti žalba Povjereniku za informiranje u roku od 15 dana od dana dostave rješenja. Žalba se izjavljuje putem tijela javne vlasti. Sukladno članku 19. Zakona o pravu na pristup informacijama u postupcima ostvarivanja prava na pristup informacijama se ne plaćaju upravne pristojbe.

SLUŽBENICA ZA INFORMIRANJE

Tamara Horvat Klemen

DOSTAVITI:
1. Krunoslav Arbanas, [redacted]
2. Pismohrana, ovdje

Slika 9.12. Odgovor na zahtjev za pristup informacijama – sektor poslovnih usluga za državna tijela (nastavak)

Obrazac broj 2

ZAHTJEV ZA PRISTUP INFORMACIJAMA

Podnositelj zahtjeva (ime i prezime / naziv, adresa / sjedište, telefon i/ili e-pošta)
Krunoslav Arbanas, [redacted], karbanas@foi.hr

Naziv tijela javne vlasti / sjedište i adresa
Ministarstvo zaštite okoliša i energetike, Radnička cesta 80, 10 000 Zagreb

Informacija koja se traži
Popis identificiranih tvrtki operatora ključnih usluga iz sektora opskrbe vodom za piće i njezine distribucije sukladno Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/2018) za potrebe provođenja znanstvenog istraživanja u sklopu izrade doktorske disertacije na temu „Razvoj okvira za evaluaciju i uspostavu kulture informacijske sigurnosti“. **Obrazloženje: Popis je potreban isključivo iz razloga kako bi se uspjele identificirati organizacije kojima bi se uputio dopis s objašnjenjem predloženog istraživanja te anketnim upitnikom koji bi zaposlenici tih organizacija mogli dobrovoljno popuniti i ne bi se koristio u druge svrhe. Upitnikom se ne bi prikupljali nikakvi osobni niti povjerljivi podaci, a popunjavanje upitnika bilo bi u potpunosti anonimno. Također, nigdje se ne bi spominjali nazivi organizacija već samo sektor kojem pripadaju sukladno kategorizaciji iz spomenutog Zakona. Rezultati istraživanja koristit će se isključivo u istraživačke svrhe, a sudionici će dobiti sumarne i obrađene rezultate koji im mogu biti korisni za unaprjeđenje upravljanja sigurnošću.**

Način pristupa informaciji *(označiti)*
☐ neposredan pristup informaciji, ☐ pristup informaciji pisanim putem ☐ uvid u dokumente i izrada preslika dokumenata koji sadrže traženu informaciju, ☐ dostavljanje preslika dokumenata koji sadrži traženu informaciju, ☒ na drugi prikladan način (elektronskim putem ili drugo) putem e-maila

Arbanas K.

(vlastoručni potpis podnositelja zahtjeva)

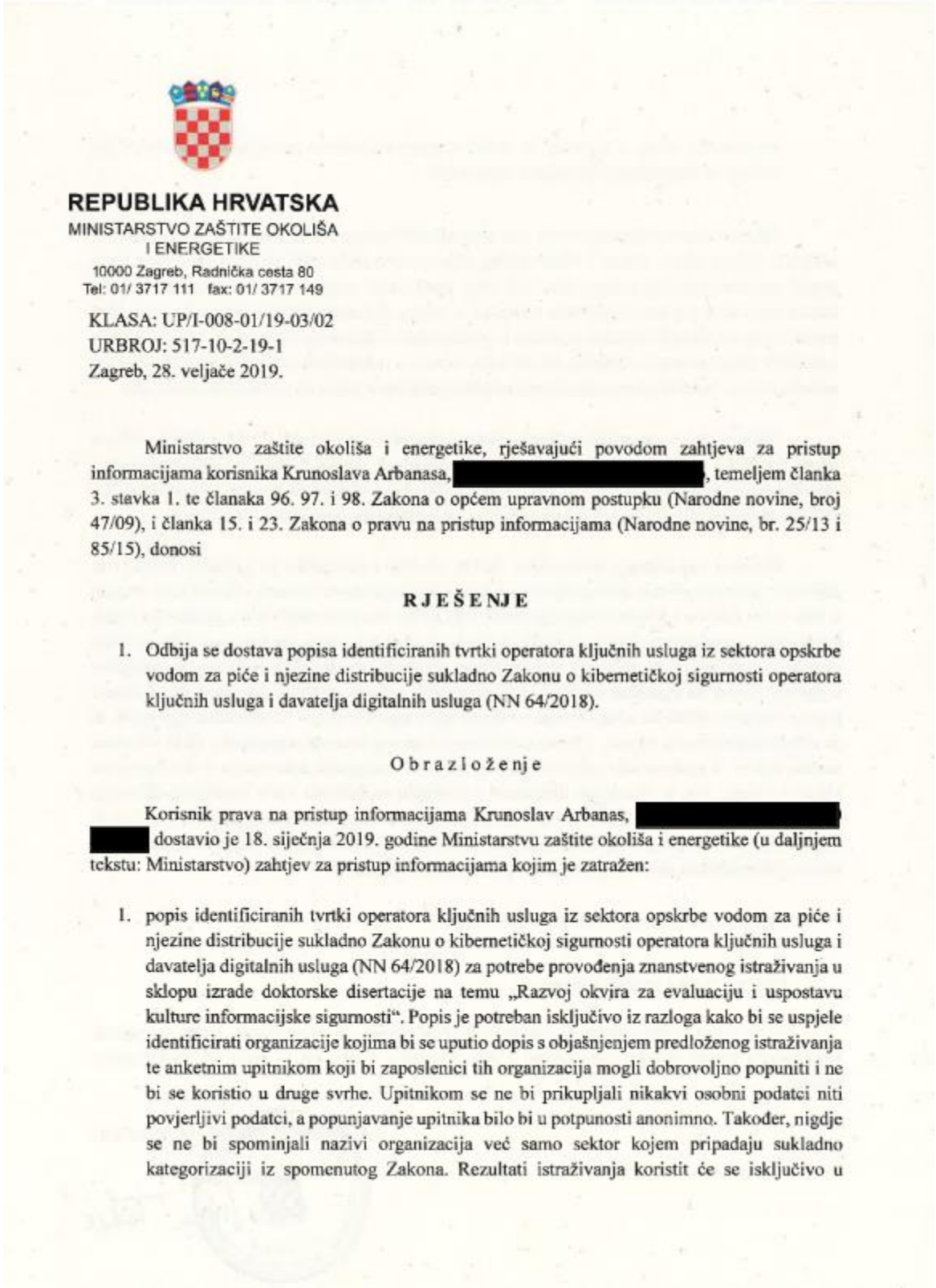
Zagreb, 18.01.2019.

(mjesto i datum)

Napomena: *Tijelo javne vlasti ima pravo na naknadu stvarnih materijalnih troškova od podnositelja zahtjeva u svezi s pružanjem i dostavom tražene informacije.*

Obrazac broj 2 – Obrazac zahtjeva za pristup informaciji

Slika 9.13. Zahtjev za pristup informacijama – sektor opskrbe vodom za piće i njezine distribucije



REPUBLIKA HRVATSKA
MINISTARSTVO ZAŠTITE OKOLIŠA
I ENERGETIKE
10000 Zagreb, Radnička cesta 80
Tel: 01/ 3717 111 fax: 01/ 3717 149

KLASA: UP/I-008-01/19-03/02
URBROJ: 517-10-2-19-1
Zagreb, 28. veljače 2019.

Ministarstvo zaštite okoliša i energetike, rješavajući povodom zahtjeva za pristup informacijama korisnika Krunoslava Arbanasa, [redacted], temeljem članka 3. stavka 1. te članaka 96. 97. i 98. Zakona o općem upravnom postupku (Narodne novine, broj 47/09), i članka 15. i 23. Zakona o pravu na pristup informacijama (Narodne novine, br. 25/13 i 85/15), donosi

R J E Š E N J E

1. Odbija se dostava popisa identificiranih tvrtki operatora ključnih usluga iz sektora opskrbe vodom za piće i njezine distribucije sukladno Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/2018).

O b r a z l o ž e n j e

Korisnik prava na pristup informacijama Krunoslav Arbanas, [redacted] dostavio je 18. siječnja 2019. godine Ministarstvu zaštite okoliša i energetike (u daljnjem tekstu: Ministarstvo) zahtjev za pristup informacijama kojim je zatražen:

1. popis identificiranih tvrtki operatora ključnih usluga iz sektora opskrbe vodom za piće i njezine distribucije sukladno Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/2018) za potrebe provođenja znanstvenog istraživanja u sklopu izrade doktorske disertacije na temu „Razvoj okvira za evaluaciju i uspostavu kulture informacijske sigurnosti". Popis je potreban isključivo iz razloga kako bi se uspjele identificirati organizacije kojima bi se uputio dopis s objašnjenjem predloženog istraživanja te anketnim upitnikom koji bi zaposlenici tih organizacija mogli dobrovoljno popuniti i ne bi se koristio u druge svrhe. Upitnikom se ne bi prikupljali nikakvi osobni podatci niti povjerljivi podatci, a popunjavanje upitnika bilo bi u potpunosti anonimno. Također, nigdje se ne bi spominjali nazivi organizacija već samo sektor kojem pripadaju sukladno kategorizaciji iz spomenutog Zakona. Rezultati istraživanja koristit će se isključivo u

Slika 9.14. Odgovor na zahtjev za pristup informacijama – sektor opskrbe vodom za piće i njezine distribucije

istraživačke svrhe, a sudionici će dobiti sumarne i obrađene rezultate koji im mogu biti korisni za unapređenje upravljanja sigurnošću.

Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/2018, dalje u tekstu: Zakon o kibernetičkoj sigurnosti) u članku 40. stavku 1. propisuje da se popisi operatera ključnih usluga, kao i svi drugi podaci koji nastaju u okviru provedbe Zakona koriste isključivo u svrhu izvršavanja zahtijeva iz samog Zakona o kibernetičkoj sigurnosti, dok stavak 2. navodi da popis i podaci iz stavka 1. predstavljaju informacije u odnosu na koje je moguće ograničiti pravo pristupa korisniku informacija, ovisno o rezultatima testa razmjernosti i javnog interesa koji se provodi prema odredbama posebnog zakona o pravu na pristup informacijama.

Zakon o pravu na pristup informacijama („Narodne novine", br. 25/13. i 85/15., dalje u tekstu: Zakona o pravu na pristup informacijama) u članku 5. stavku 7. definira test razmjernosti i javnog interesa kao procjenu razmjernosti između razloga za omogućavanje pristupa informaciji i razloga za ograničenje te omogućavanje pristupa informaciji ako prevladava javni interes.

Slijedom navedenog, Ministarstvo zaštite okoliša i energetike je sukladno članku 16. Zakona o pravu na pristup informacijama provelo test razmjernosti i javnog interesa te je imajući u vidu svrhu Zakona o kibernetičkoj sigurnosti, koji za cilj ima postizanje visoke zajedničke razine kibernetičke sigurnosti te definiciju rizika iz članka 4. stavka 1. točke 15. Zakona o kibernetičkoj sigurnosti kao bilo koje razumno prepoznatljive okolnosti ili događaja koji ima potencijalno negativni učinak na sigurnost mrežnih i informacijskih sustava, donijelo zaključak da bi objava popisa operatora ključnih usluga mogla u velikoj mjeri ugroziti sustav kibernetičke sigurnosti, te ga učiniti ranjivijima za napade. Testom razmjernosti i javnog interesa ocijenjeno je da bi više štete nastalo ako bi se podnositelju zahtjeva odnosno javnosti omogućila informacija o listi operatora ključnih usluga, čije je obavljanje djelatnosti u području nadležnosti tijela Središnjeg državnog ureda za razvoj digitalnog društva, nego što bi štete nastalo za podnositelja zahtjeva koji bez te informacije ne bi mogao provesti namjeravano istraživanje, izravnim upitom organizacijama, stoga podnositelju zahtjeva nije omogućen pristup zatraženoj informaciji.

Sukladno navedenom odlučeno je kao u izreci.

UPUTA O PRAVNOM LIJEKU:

Protiv ovog rješenja može se izjaviti žalba Povjereniku za informiranje. Žalba se podnosi Ministarstvu zaštite okoliša i energetike u dva primjerka u roku od 15 dana od dana dostave rješenja.

SLUŽBENICA ZA INFORMIRANJE

Kristina Tekić

Slika 9.14. Odgovor na zahtjev za pristup informacijama – sektor opskrbe vodom za piće i njezine distribucije (nastavak)

Obrazac broj 2

ZAHTJEV ZA PRISTUP INFORMACIJAMA

Podnositelj zahtjeva (ime i prezime / naziv, adresa / sjedište, telefon i/ili e-pošta)
Krunoslav Arbanas, [redacted], karbanas@foi.hr

Naziv tijela javne vlasti / sjedište i adresa
Ministarstvo zdravstva **Ksaver 200a** **10 000 Zagreb**

Informacija koja se traži
Popis identificiranih tvrtki operatora ključnih usluga iz zdravstvenog sektora sukladno Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/2018) za potrebe provođenja znanstvenog istraživanja u sklopu izrade doktorske disertacije na temu „Razvoj okvira za evaluaciju i uspostavu kulture informacijske sigurnosti". **Obrazloženje: Popis je potreban isključivo iz razloga kako bi se uspjele identificirati organizacije kojima bi se uputio dopis s objašnjenjem predloženog istraživanja te anketnim upitnikom koji bi zaposlenici tih organizacija mogli dobrovoljno popuniti i ne bi se koristio u druge svrhe. Upitnikom se ne bi prikupljali nikakvi osobni niti povjerljivi podaci, a popunjavanje upitnika bilo bi u potpunosti anonimno. Također, nigdje se ne bi spominjali nazivi organizacija već samo sektor kojem pripadaju sukladno kategorizaciji iz spomenutog Zakona. Rezultati istraživanja koristit će se isključivo u istraživačke svrhe, a sudionici će dobiti sumarne i obrađene rezultate koji im mogu biti korisni za unaprjeđenje upravljanja sigurnošću.**

Način pristupa informaciji *(označiti)*
☐ neposredan pristup informaciji, ☐ pristup informaciji pisanim putem ☐ uvid u dokumente i izrada preslika dokumenata koji sadrže traženu informaciju, ☐ dostavljanje preslika dokumenata koji sadrži traženu informaciju, ☑ na drugi prikladan način (elektronskim putem ili drugo) putem e-maila

Arbanas K.

(vlastoručni potpis podnositelja zahtjeva)

Zagreb, 18.01.2019.

(mjesto i datum)

Napomena: *Tijelo javne vlasti ima pravo na naknadu stvarnih materijalnih troškova od podnositelja zahtjeva u svezi s pružanjem i dostavom tražene informacije.*

Obrazac broj 2 – Obrazac zahtjeva za pristup informaciji

Slika 9.15. Zahtjev za pristup informacijama – zdravstveni sektor

REPUBLIKA HRVATSKA
MINISTARSTVO ZDRAVSTVA

KLASA: UP/I-008-01/19-01/05
URBROJ: 534-1/10-19-1
Zagreb, 19. lipnja 2019.g.

Na temelju članka 23. stavka 5. točke 2. Zakona o pravu na pristup informacijama („Narodne novine" broj 25/2013 i 85/15), te članka 96. Zakona o općem upravnom postupku („Narodne novine" broj 47/2009.g.) povodom zahtjeva korisnika prava na informaciju Krunoslava Arbanasa, [redacted] (dalje: korisnik), ministar zdravstva donosi

R J E Š E N J E

Odbija se zahtjev korisnika za ostvarivanje prava na pristup informaciji kojim se traži dostava popisa operatora ključnih usluga i davatelja digitalnih usluga iz zdravstvenog sustava.

O b r a z l o ž e n j e

Ministarstvo zdravstva zaprimilo je 18. siječnja 2019. godine zahtjev korisnika kojim se traži dostava popisa operatora ključnih usluga i davatelja digitalnih usluga iz zdravstvenog sustava.

Članak 23. stavak 5. točka 2. Zakona o pravu na pristup informacijama (NN br. 25/13 i 85/15) propisuje kako će tijelo javne vlasti rješenjem odbiti zahtjev ako se ispune uvjeti propisani u članku 15. stavcima 2., 3. i 4. a u vezi s člankom 16. stavkom 1. ovog Zakona.
Članak 16. stavak 1. Zakona o pravu na pristup informacijama propisuje kako je tijelo javne vlasti nadležno za postupanje po zahtjevu za pristup informaciji iz članka 15. stavka 2. točke 2.,, 3., 4., 5., 6., i 7. i stavaka 3. i 4. ovog Zakona dužno, prije donošenja odluke, provesti test razmjernosti i javnog interesa.
Ministarstvo zdravstva obavijestilo je korisnika dopisom Klasa:008-01/19-01/08 Urbroj: 534-01/10-19-02 od 29. siječnja 2019.g. o produženju roka za rješavanje zahtjeva zbog obaveze provedbe testa razmjernosti i javnog interesa.
Ministarstvo zdravstva, sukladno članku 16. stavku 1. Zakona o pravu na pristup informacijama provelo je test razmjernosti i javnog interesa te je zaključeno sljedeće.

Ksaver 200a, 10 000 Zagreb, Republika Hrvatska, T +385 1 46 07 555, F +385 1 46 77 076

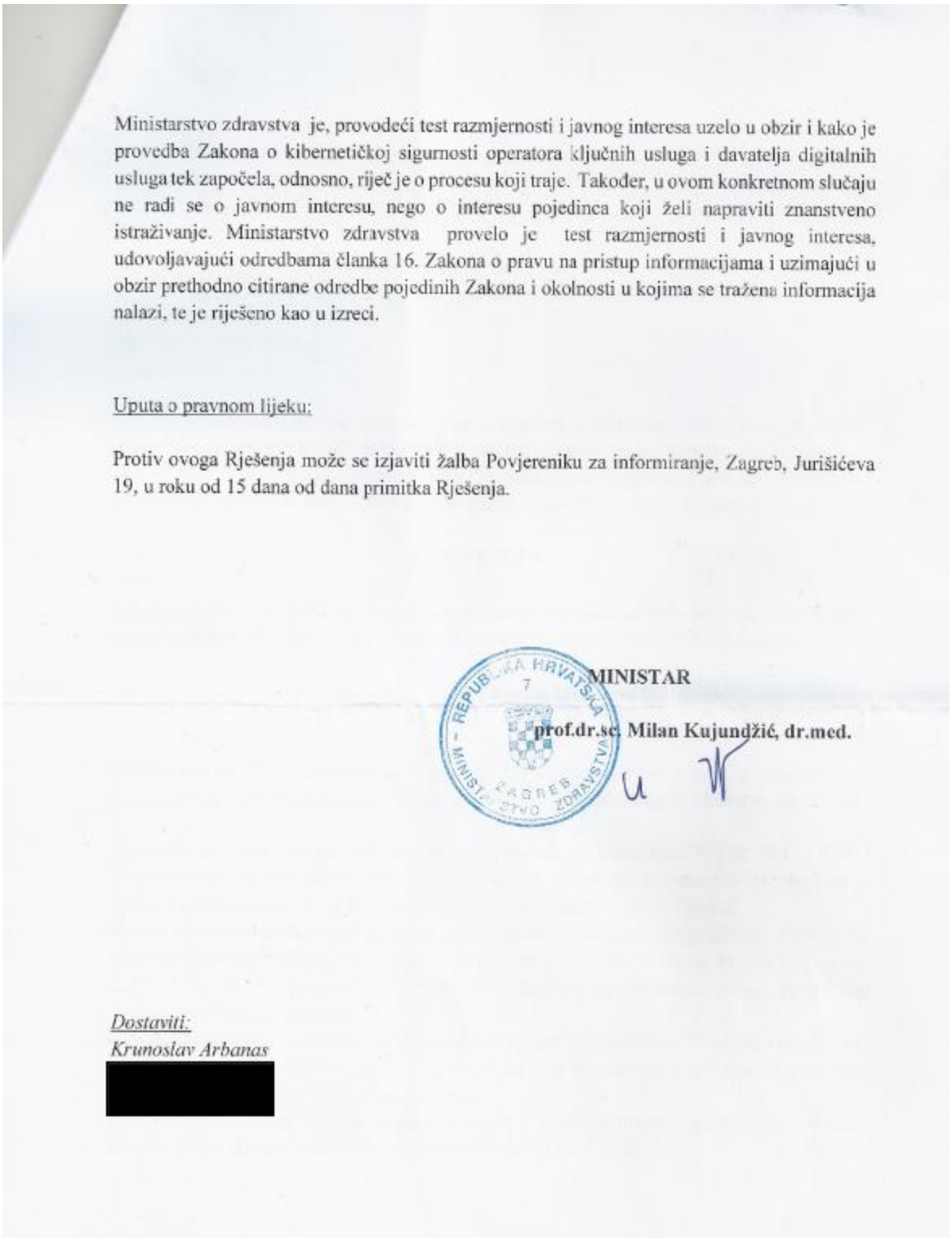
Slika 9.16. Odgovor na zahtjev za pristup informacijama – zdravstveni sektor

Članak 23. stavak 5. točka 2. Zakona o pravu na pristup informacijama (NN br. 25/13 i 85/15) propisuje kako će tijelo javne vlasti rješenjem odbiti zahtjev ako se ispune uvjeti propisani u članku 15. stavcima 2., 3. i 4. a u vezi s člankom 16. stavkom 1. ovog Zakona.

Zahtjevom g. Krunoslava Arbanasa tražio se popis operatora ključnih usluga i davatelja digitalnih usluga iz zdravstvenog sustava, a za čije je određivanje nadležno Ministarstvo zdravstva. Slijedom članka 40. Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, predviđena je mogućnost uskrate traženih informacija. Ministarstvo zdravstva zatražilo je o ovom zahtjevu mišljenje Ureda Vijeća za nacionalnu sigurnost, koji je uputio na članak 40. Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN br. 64/18) u kojem je navedeno sljedeće:
(1) Popisi operatora ključnih usluga, kao i svi drugi podaci koji nastaju u okviru provedbe ovog Zakona koriste se isključivo u svrhu izvršavanja zahtjeva iz ovog Zakona.
(2) Popis i podaci iz stavka 1. ovog članka predstavljaju informacije u odnosu na koje je moguće ograničiti pravo pristupa korisniku informacija, ovisno o rezultatima testa razmjernosti i javnog interesa koji se provodi prema odredbama posebnog zakona o pravu na pristup informacijama.
Članak 15.stavak 2. točka 7. propisuje kako tijela javne vlasti mogu ograničiti pristup informaciji u slučajevima utvrđenim zakonom.

Sukladno odredbama članka 40. Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine 64/18), koji propisuje da se podaci koji nastaju u provedbi toga propisa koriste isključivo u svrhu izvršavanja zahtjeva iz toga Zakona, moguće je ograničiti pravo pristupa korisniku informacija, a nastavno na rezultate provedenoga testa razmjernosti prema odredbama Zakona o pravu na pristup informacijama („Narodne novine" 25/13 i 85/15). Osim toga, nastavno na članak 48. stavak 1. Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, identificirani operatori ključnih usluga dužni su provesti mjere za osiguravanje visoke razine kibernetičke sigurnosti u roku od godine dana nakon što su zaprimili obavijesti da su identificirani kao operatori ključnih usluga. To razdoblje od godine dana ostavljeno je operatorima ključnih usluga za provedbu procesa prilagodbe poslovanja u smislu poduzimanja mjera za postizanje visoke razine kibernetičke sigurnosti svojih usluga, radi osiguranja kontinuiteta u obavljanju tih usluga, pa se stoga može smatrati da je proces u tijeku.
S obzirom da je razvitak sposobnosti kibernetičkog djelovanja u okviru sustava domovinske sigurnosti jedan od specifičnih ciljeva u Godišnjem planu rada Koordinacije za sustav domovinske sigurnosti za 2019. godinu gdje je ovo Ministarstvo dioničko tijelo i koji je odobren na 4. sjednici Koordinacije u prosincu 2018. godine, a u koji se ubrajaju i procesi u smislu Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, te je postupak izrade i usuglašavanja u tijeku, članak 15. stavak 4, podstavci 1, 2. i 8. Zakona o pravu na pristup informacijama omogućavaju tijelima javne vlasti ograničavanje pristupa informaciji.

Slika 9.16. Odgovor na zahtjev za pristup informacijama – zdravstveni sektor (nastavak)



Ministarstvo zdravstva je, provodeći test razmjernosti i javnog interesa uzelo u obzir i kako je provedba Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga tek započela, odnosno, riječ je o procesu koji traje. Također, u ovom konkretnom slučaju ne radi se o javnom interesu, nego o interesu pojedinca koji želi napraviti znanstveno istraživanje. Ministarstvo zdravstva provelo je test razmjernosti i javnog interesa, udovoljavajući odredbama članka 16. Zakona o pravu na pristup informacijama i uzimajući u obzir prethodno citirane odredbe pojedinih Zakona i okolnosti u kojima se tražena informacija nalazi, te je riješeno kao u izreci.

Uputa o pravnom lijeku:

Protiv ovoga Rješenja može se izjaviti žalba Povjereniku za informiranje, Zagreb, Jurišićeva 19, u roku od 15 dana od dana primitka Rješenja.

MINISTAR

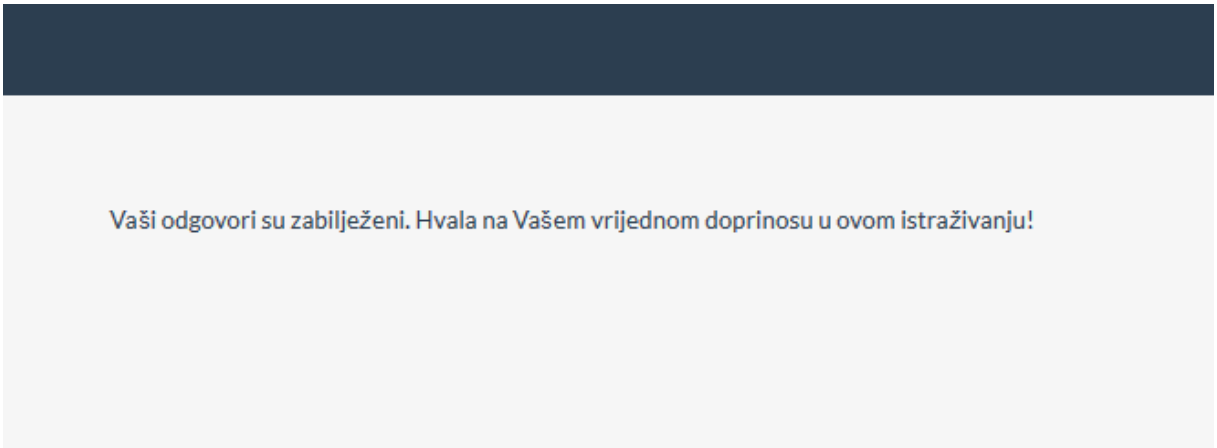
prof.dr.sc. Milan Kujundžić, dr.med.

Dostaviti:
Krunoslav Arbanas
[redacted]

Slika 9.16. Odgovor na zahtjev za pristup informacijama – zdravstveni sektor (nastavak)

Prilog 4. Slike ekrana mjernog instrumenta u online sustavu Limesurvey

U nastavku su prikazane slike ekrana finalne verzije mjernog instrumenta implementiranog putem online sustava Limesurvey, koji je predstavljao temelj empirijskog istraživanja.
Na prvoj stranici prikazani su početni i završni ekran, dok se u nastavku nalaze slike ekrana triju glavnih cjelina: pitanja vezanih uz percepciju zaposlenika o čimbenicima kulture informacijske sigurnosti, pitanja vezana uz stvarno stanje implementiranih sigurnosnih mjera u organizaciji te pitanja vezanih uz demografska obilježja sudionika istraživanja.



0%

Politike i procedure

*

Odaberite jedan od ponuđenih odgovora na sljedeće tvrdnje imajući u vidu koliko se pojedina tvrdnja odnosi na Vas i Vaše stavove u kontekstu informacijske sigurnosti u Vašoj organizaciji:

1 – u potpunosti se ne slažem
2 – uglavnom se ne slažem
3 – niti se slažem niti ne slažem
4 – uglavnom se slažem
5 – u potpunosti se slažem
n/p - odaberite samo u slučaju da pitanje nije primjenjivo na Vašu organizaciju

	1	2	3	4	5	n/p
Moja organizacija uspostavila je pravila ponašanja vezanih uz korištenje informacijske imovine	○	○	○	○	○	○
Politika informacijske sigurnosti jasno definira ciljeve informacijske sigurnosti moje organizacije	○	○	○	○	○	○
Politika informacijske sigurnosti jasno ističe važnost informacijske sigurnosti za organizaciju	○	○	○	○	○	○
Procedure za implementaciju politike informacijske sigurnosti (npr. procedura upravljanja korisničkim računima, procedura upravljanja promjenama u sustavu, procedura upravljanja sigurnosnim incidentima…) su jasno definirane i dokumentirane	○	○	○	○	○	○
Sadržaj politike informacijske sigurnosti lako je razumljiv	○	○	○	○	○	○
Sigurnosne politike i procedure su lako dostupne u mojoj organizaciji	○	○	○	○	○	○
U mojoj organizaciji, jasno su definirane disciplinske mjere u slučaju kršenja odredbi sigurnosne politike	○	○	○	○	○	○
Ako se otkrije da sam kršio/la organizacijske politike informacijske sigurnosti bit ću kažnjen/a	○	○	○	○	○	○
U mojoj organizaciji definirana je osoba kojoj se mogu obratiti s pitanjima vezanim uz informacijsku sigurnost	○	○	○	○	○	○
U mojoj organizaciji jasno su definirane uloge i odgovornosti zaposlenika vezane za informacijsku sigurnost	○	○	○	○	○	○
Upoznat/a sam sa svojim odgovornostima vezanim uz informacijsku sigurnost	○	○	○	○	○	○
Namjeravam štititi informacijsku imovinu moje organizacije sukladno odredbama sigurnosne politike	○	○	○	○	○	○

Prethodno Sljedeće

9%

Podrška rukovodstva

*

Odaberite jedan od ponuđenih odgovora na sljedeće tvrdnje imajući u vidu koliko se pojedina tvrdnja odnosi na Vas i Vaše stavove u kontekstu informacijske sigurnosti u Vašoj organizaciji:

1 – u potpunosti se ne slažem
2 – uglavnom se ne slažem
3 – niti se slažem niti ne slažem
4 – uglavnom se slažem
5 – u potpunosti se slažem
n/p - odaberite samo u slučaju da pitanje nije primjenjivo na Vašu organizaciju

	1	2	3	4	5	n/p
Postupci rukovodstva u mojoj organizaciji pokazuju da je sigurnost informacija važan organizacijski prioritet	○	○	○	○	○	○
Rukovodstvo u mojoj organizaciji brine o informacijskoj sigurnosti samo kad se dogodi neki incident	○	○	○	○	○	○
Rukovodstvo u mojoj organizaciji omogućuje dovoljno financijskih i ljudskih resursa za upravljanje informacijskom sigurnošću	○	○	○	○	○	○
Rukovodstvo u mojoj organizaciji preuzima krajnju odgovornost za informacijsku sigurnost	○	○	○	○	○	○
Rukovodstvo u mojoj organizaciji pridržava se odredbi politike informacijske sigurnosti	○	○	○	○	○	○
Rukovodstvo u mojoj organizaciji sudjeluje u edukacijama, projektima, radionicama podizanja svijesti i ostalim aktivnostima vezanim uz informacijsku sigurnost	○	○	○	○	○	○
U mojoj organizaciji vidljiva je predanost i potpora od strane rukovodstva vezano za informacijsku sigurnost	○	○	○	○	○	○

Prethodno Sljedeće

18%

Edukacija i osviještenost

*

Odaberite jedan od ponuđenih odgovora na sljedeće tvrdnje imajući u vidu koliko se pojedina tvrdnja odnosi na Vas i Vaše stavove u kontekstu informacijske sigurnosti u Vašoj organizaciji:

1 – u potpunosti se ne slažem
2 – uglavnom se ne slažem
3 – niti se slažem niti ne slažem
4 – uglavnom se slažem
5 – u potpunosti se slažem
n/p - odaberite samo u slučaju da pitanje nije primjenjivo na Vašu organizaciju

	1	2	3	4	5	n/p
Ako imam priliku, sudjelovat ću na edukacijama i radionicama vezanim uz informacijsku sigurnost	○	○	○	○	○	○
Edukacije vezane uz informacijsku sigurnost koje nudi moja organizacija su korisne	○	○	○	○	○	○
U mojoj organizaciji podržava se periodično održavanje radionica za zaposlenike na temu informacijske sigurnosti	○	○	○	○	○	○
U mojoj organizaciji svi zaposlenici dobivaju dovoljnu i primjerenu edukaciju o informacijskoj sigurnosti	○	○	○	○	○	○
Zaposlenici su educirani oko svojih uloga i odgovornosti vezanih za informacijsku sigurnost i toga kako se ponašati na siguran način	○	○	○	○	○	○
Zbog edukacija vezanih uz informacijsku sigurnost osjećam se bolje pripremljen/a za potencijalne sigurnosne incidente	○	○	○	○	○	○
Smatram da je znanje o informacijskoj sigurnosti mojih kolega u organizaciji na zadovoljavajućoj razini	○	○	○	○	○	○
Svi zaposlenici su educirani o potrebi zaključavanja svojih računala kad napuštaju svoje radno mjesto	○	○	○	○	○	○
Svi zaposlenici u mojoj organizaciji pravovremeno su obaviješteni o prijetnjama informacijske sigurnosti putem elektroničke pošte ili na neki drugi način	○	○	○	○	○	○
Ako ja ne pridajem dovoljno pažnje odredbama politike informacijske sigurnosti, informacijska imovina moje organizacije je podložna riziku	○	○	○	○	○	○
Čak i ako mogu, ne smijem isključiti antivirusni program na svom računalu	○	○	○	○	○	○
Često ostavljam svoje računalo otključano kad napuštam radno mjesto	○	○	○	○	○	○
Neću otkriti svoju lozinku za pristup računalu nikome, pa čak ni svom nadređenom	○	○	○	○	○	○
Osjećam se pouzdano u svoje razumijevanje sigurnosne politike u mojoj organizaciji	○	○	○	○	○	○
U mojoj organizaciji koriste se različiti oblici komunikacije (npr. e-mail, plakati, post-it poruke, newsletter,...) za promicanje svijesti o informacijskoj sigurnosti	○	○	○	○	○	○
U mojoj organizaciji zaposlenici su upućeni što se smatra (ne)prihvatljivim korištenjem informacijske imovine	○	○	○	○	○	○
Upoznat/a sam sa sigurnosnim politikama, procedurama i smjernicama moje organizacije	○	○	○	○	○	○
Znam što je "incident informacijske sigurnosti"	○	○	○	○	○	○
Znam što podrazumijeva pojam "informacijska sigurnost"	○	○	○	○	○	○

Prethodno

Sljedeće

27%

Usklađenost

*
Odaberite jedan od ponuđenih odgovora na sljedeće tvrdnje imajući u vidu koliko se pojedina tvrdnja odnosi na Vas i Vaše stavove u kontekstu informacijske sigurnosti u Vašoj organizaciji:

1 – u potpunosti se ne slažem
2 – uglavnom se ne slažem
3 – niti se slažem niti ne slažem
4 – uglavnom se slažem
5 – u potpunosti se slažem
n/p - odaberite samo u slučaju da pitanje nije primjenjivo na Vašu organizaciju

	1	2	3	4	5	n/p
Kao zaposlenik/ca, imam korist od usklađenosti s pravilima vezanim uz informacijsku sigurnost u mojoj organizaciji	○	○	○	○	○	○
Moja organizacija provodi periodične provjere radi utvrđivanja usklađenosti sa politikom informacijske sigurnosti	○	○	○	○	○	○
U mojoj organizaciji provjerava se slijede li zaposlenici sigurnosne politike, procedure i smjernice	○	○	○	○	○	○
U mojoj organizaciji redovno se provjerava učinkovitost i potpunost politike informacijske sigurnosti	○	○	○	○	○	○

Prethodno

Sljedeće

36%

Ponašanje

*
Odaberite jedan od ponuđenih odgovora na sljedeće tvrdnje imajući u vidu koliko se pojedina tvrdnja odnosi na Vas i Vaše stavove u kontekstu informacijske sigurnosti u Vašoj organizaciji:

1 – u potpunosti se ne slažem
2 – uglavnom se ne slažem
3 – niti se slažem niti ne slažem
4 – uglavnom se slažem
5 – u potpunosti se slažem
n/p - odaberite samo u slučaju da pitanje nije primjenjivo na Vašu organizaciju

	1	2	3	4	5	n/p
Ako poštujem pravila vezana uz informacijsku sigurnost, mogu pomoći u zaštiti informacijske imovine svoje organizacije	○	○	○	○	○	○
Primjena dobrih praksi vezanih uz sigurnost informacijske imovine predstavlja prihvaćeni način poslovanja u mojoj organizaciji	○	○	○	○	○	○
Svoje znanje o informacijskoj sigurnosti dijelim s kolegama/icama kako bih povećao/la njihovu svijest o toj tematici	○	○	○	○	○	○
Zaposlenici u mojoj organizaciji preuzimaju odgovornost za zaštitu informacija s kojima dolaze u doticaj	○	○	○	○	○	○

Prethodno

Sljedeće

45%

Uvjerenja

*

Odaberite jedan od ponuđenih odgovora na sljedeće tvrdnje imajući u vidu koliko se pojedina tvrdnja odnosi na Vas i Vaše stavove u kontekstu informacijske sigurnosti u Vašoj organizaciji:

1 – u potpunosti se ne slažem
2 – uglavnom se ne slažem
3 – niti se slažem niti ne slažem
4 – uglavnom se slažem
5 – u potpunosti se slažem
n/p - odaberite samo u slučaju da pitanje nije primjenjivo na Vašu organizaciju

	1	2	3	4	5	n/p
Informacijski sustav moje organizacije siguran je toliko koliko ga ja činim sigurnim	○	○	○	○	○	○
Poštivanje politike informacijske sigurnosti u organizaciji usporava moju produktivnost na poslu	○	○	○	○	○	○
Smatram da moja organizacija daje dovoljno pažnje strategiji informacijske sigurnosti s ciljem zaštite informacijske imovine	○	○	○	○	○	○
U mojoj organizaciji, provođenje sigurnosnih mjera oduzimalo bi previše vremena	○	○	○	○	○	○
Uvjeren/a sam da drugi zaposlenici poštuju odredbe politike informacijske sigurnosti u mojoj organizaciji	○	○	○	○	○	○
Zaposlenik koji krši politiku informacijske sigurnosti šteti svojoj organizaciji	○	○	○	○	○	○

Prethodno Sljedeće

54%

Antivirusna zaštita

*

Odaberite jedan od ponuđenih odgovora na sljedeće tvrdnje imajući u vidu koliko se pojedina tvrdnja odnosi na Vas i Vaše stavove u kontekstu informacijske sigurnosti u Vašoj organizaciji:

1 – u potpunosti se ne slažem
2 – uglavnom se ne slažem
3 – niti se slažem niti ne slažem
4 – uglavnom se slažem
5 – u potpunosti se slažem
n/p - odaberite samo u slučaju da pitanje nije primjenjivo na Vašu organizaciju

	1	2	3	4	5	n/p
Antivirusni sustav barem jednom tjedno skenira moje računalo	○	○	○	○	○	○
Antivirusni sustav instaliran na mom računalu redovito se ažurira	○	○	○	○	○	○
Antivirusni sustav koji se redovito ažurira i održava značajno doprinosi zaštiti informacijskog sustava	○	○	○	○	○	○
Antivirusni sustav neophodan je za moju organizaciju	○	○	○	○	○	○
Implementacija antivirusne zaštite neophodna je za svaku organizaciju koja u svom poslovanju koristi informacijske sustave	○	○	○	○	○	○

Prethodno Sljedeće

63%

Sigurnosna kopija

*
Odaberite jedan od ponuđenih odgovora na sljedeće tvrdnje imajući u vidu koliko se pojedina tvrdnja odnosi na Vas i Vaše stavove u kontekstu informacijske sigurnosti u Vašoj organizaciji:

1 – u potpunosti se ne slažem
2 – uglavnom se ne slažem
3 – niti se slažem niti ne slažem
4 – uglavnom se slažem
5 – u potpunosti se slažem
n/p - odaberite samo u slučaju da pitanje nije primjenjivo na Vašu organizaciju

	1	2	3	4	5	n/p
Moja organizacija redovito provodi izradu sigurnosne kopije (eng. backup) bitnih poslovnih informacija kako bi se smanjila vjerojatnost gubitka podataka	○	○	○	○	○	○
Proces redovne izrade sigurnosne kopije (eng. backup) i povrata podataka (eng. restore) značajno doprinosi dostupnosti kritičnih informacija	○	○	○	○	○	○
Proces redovne izrade sigurnosne kopije (eng. backup) i povrata podataka (eng. restore) značajno doprinosi mogućnosti oporavka poslovanja u slučaju pojave katastrofalnog događaja	○	○	○	○	○	○
Znam gdje trebam pohranjivati bitne podatke kako bi se izradila njihova sigurnosna kopija (eng. backup)	○	○	○	○	○	○

Prethodno

Sljedeće

72%

Autentikacija i autorizacija

*
Odaberite jedan od ponuđenih odgovora na sljedeće tvrdnje imajući u vidu koliko se pojedina tvrdnja odnosi na Vas i Vaše stavove u kontekstu informacijske sigurnosti u Vašoj organizaciji:

1 – u potpunosti se ne slažem
2 – uglavnom se ne slažem
3 – niti se slažem niti ne slažem
4 – uglavnom se slažem
5 – u potpunosti se slažem
n/p - odaberite samo u slučaju da pitanje nije primjenjivo na Vašu organizaciju

	1	2	3	4	5	n/p
Informacije trebaju biti zaštićene od neovlaštene upotrebe (čitanja, izmjene, brisanja)	○	○	○	○	○	○
Prilikom promjene lozinke, ona mora biti određene duljine i kombinacija malih i velikih slova te brojeva	○	○	○	○	○	○
Sustav me nakon određenog vremena traži da promijenim svoju lozinku	○	○	○	○	○	○
Svim povjerljivim informacijama treba se moći pristupiti samo s odgovarajućim korisničkim imenom i lozinkom	○	○	○	○	○	○
U mojoj organizaciji uspostavljeni su odgovarajući mehanizmi kojima se osigurava da pristup informacijskom sustavu imaju samo ovlaštene osobe (npr. upotrebom korisničkog imena i lozinke)	○	○	○	○	○	○
Važno je da informacijski sustav ima mogućnost utvrđivanja individualne odgovornosti zaposlenika za poduzete radnje	○	○	○	○	○	○

Prethodno

Sljedeće

81%

Stvarno stanje

*
Odaberite jedan od ponuđenih odgovora na sljedeće tvrdnje imajući u vidu koliko se pojedina tvrdnja odnosi na Vas i Vaše znanje u kontekstu informacijske sigurnosti u Vašoj organizaciji:

1 – u potpunosti se ne slažem
2 – uglavnom se ne slažem
3 – niti se slažem niti ne slažem
4 – uglavnom se slažem
5 – u potpunosti se slažem
n/p - odaberite samo u slučaju da pitanje nije primjenjivo na Vašu organizaciju

	1	2	3	4	5	n/p
Upoznat/a sam s činjenicom da se u zadnjih 12 mjeseci u mojoj organizaciji dogodio incident vezan uz informacijsku sigurnost	○	○	○	○	○	○
U zadnjih 12 mjeseci bio/bila sam obaviješten/a o promjeni sigurnosne politike ili pravila u svojoj organizaciji	○	○	○	○	○	○
U mojoj organizaciji postoji interna funkcija (jedna ili više osoba ili odjel) zadužena za informacijsku sigurnost	○	○	○	○	○	○
U zadnjih 12 mjeseci prijavio/la sam incident informacijske sigurnosti ili sumnju na isti	○	○	○	○	○	○

*
Odaberite jedan od ponuđenih odgovora na sljedeće tvrdnje koji najbolje oslikava Vaše znanje o pojedinoj tvrdnji u kontekstu informacijske sigurnosti u Vašoj organizaciji:

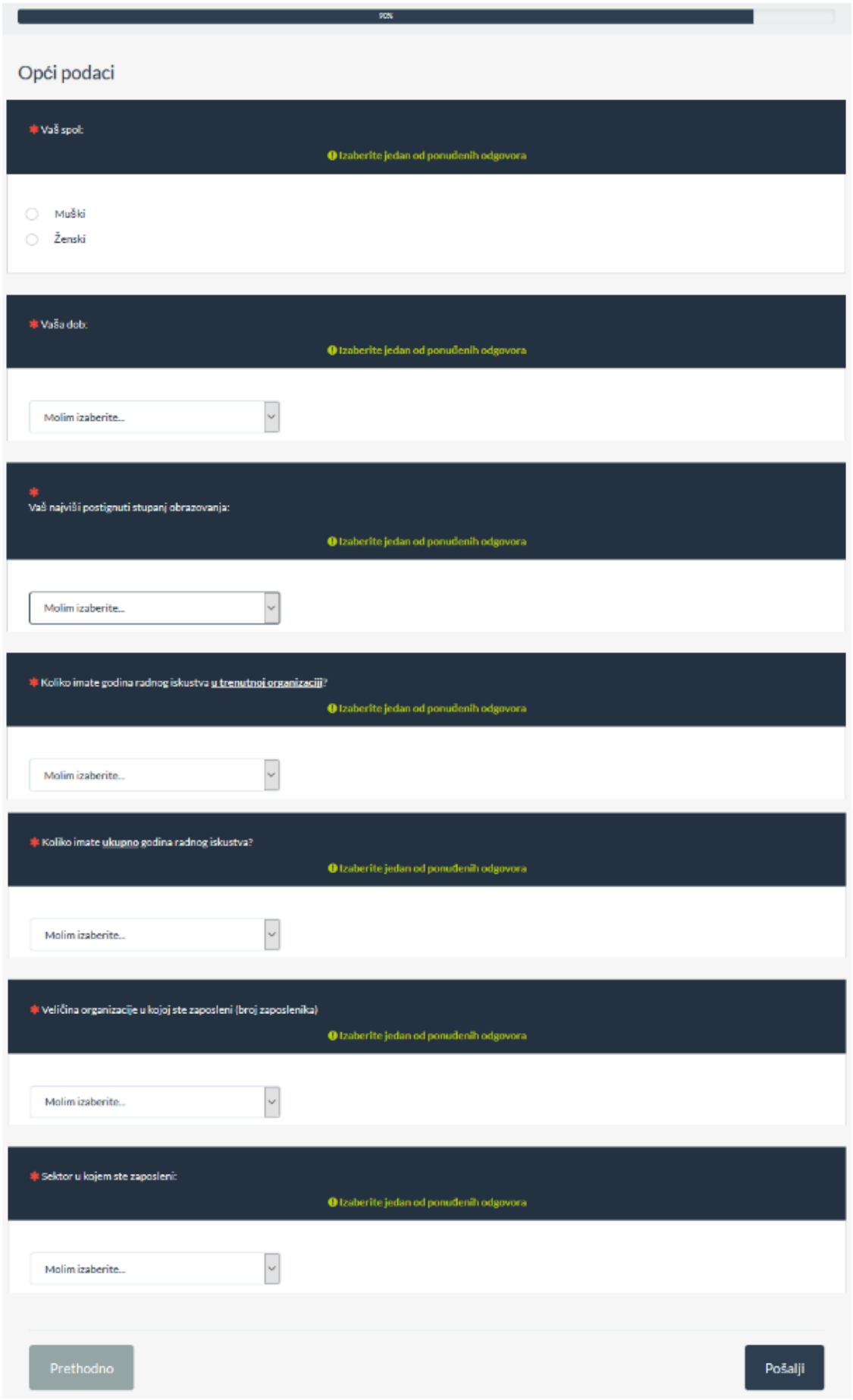
	uopće ne	rijetko	nekoliko puta	često	vrlo često
U zadnjih 12 mjeseci bio/bila sam informiran/a o prijetnjama vezanim uz otkrivanje povjerljivih informacija	○	○	○	○	○
U zadnjih 12 mjeseci bio/bila sam informiran/a o prijetnjama vezanim uz otvaranje sumnjivih elektroničkih poruka i privitaka u njima	○	○	○	○	○
U zadnjih 12 mjeseci bio/bila sam upozoren/a na prijetnje vezane uz razne oblike računalnih virusa	○	○	○	○	○
U zadnjih 12 mjeseci bio/bila sam upozoren/a na prijetnje vezane uz socijalni inženjering (lažno predstavljanje, slanje neistinitih poruka koje djeluju pouzdano u svrhu dobivanja informacija, prikupljanje informacija putem telefona i sl.)	○	○	○	○	○
U zadnjih 12 mjeseci uočio/la sam da je, nakon što je moj/a kolega/ica napustio/la svoje radno mjesto, njegovo/njezino računalo ostalo otključano (mogao/la sam sjesti za to računalo i nastaviti raditi)	○	○	○	○	○
U zadnjih 12 mjeseci uočio/la sam da su moji kolege/ice dijelili vlastite korisničke lozinke za pristup informacijskom sustavu s drugim korisnicima/cama	○	○	○	○	○

*
Odaberite jedan od ponuđenih odgovora na sljedeće tvrdnje koji najbolje oslikava Vaše znanje o pojedinoj tvrdnji u kontekstu informacijske sigurnosti u Vašoj organizaciji:

	0 puta	1 put	2 puta	3 puta	4 i više puta
U zadnjih 12 mjeseci sustav me tražio da promijenim svoju lozinku:	○	○	○	○	○
U zadnjih 12 mjeseci dobio/la sam poziv za sudjelovanje na edukaciji/radionici za podizanje svijesti o informacijskoj sigurnosti:	○	○	○	○	○

Prethodno

Sljedeće


Opći podaci
* Vaš spol:
Izaberite jedan od ponuđenih odgovora
Muški
Ženski
* Vaša dob:
Izaberite jedan od ponuđenih odgovora
Molim izaberite...
*
Vaš najviši postignuti stupanj obrazovanja:
Izaberite jedan od ponuđenih odgovora
Molim izaberite...
* Koliko imate godina radnog iskustva u trenutnoj organizaciji?
Izaberite jedan od ponuđenih odgovora
Molim izaberite...
* Koliko imate ukupno godina radnog iskustva?
Izaberite jedan od ponuđenih odgovora
Molim izaberite...
* Veličina organizacije u kojoj ste zaposleni (broj zaposlenika)
Izaberite jedan od ponuđenih odgovora
Molim izaberite...
* Sektor u kojem ste zaposleni:
Izaberite jedan od ponuđenih odgovora
Molim izaberite...
Prethodno
Pošalji

Prilog 5. Poruke elektroničke pošte s molbom za sudjelovanje u empirijskom istraživanju

Poštovani,

moje ime je Krunoslav Arbanas i zaposlen sam u Hrvatskoj energetskoj regulatornoj agenciji (HERA) kao osoba zadužena za informacijsku sigurnost, a pišem Vam u svojstvu doktoranda na poslijediplomskom doktorskom studiju Informacijske znanosti na Fakultetu organizacije i informatike u Varaždinu gdje su mi mentori prof. dr. sc. Mario Spremić s Ekonomskog fakulteta Sveučilišta u Zagrebu i doc. dr. sc. Nikolina Žajdela Hrustek s Fakulteta organizacije i informatike Sveučilišta u Zagrebu.

U sklopu izrade disertacije pod nazivom *„Radni okvir za procjenu i unapređenje kulture informacijske sigurnosti"* planirano je provođenje empirijskog istraživanja o razini kulture informacijske sigurnosti odnosno procjeni elemenata koji čine kulturu informacijske sigurnosti, a na preporuku mentora razvijeni mjerni instrument (anketni upitnik), koji predstavlja temelj za taj radni okvir, testirao bih na zaposlenicima organizacija koje su prepoznate kao operatori ključnih usluga, sukladno Prilogu I. Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/2018). Budući da Vaša organizacija zadovoljava kriterije za operatore ključnih usluga iz spomenutog Zakona, ovim putem bih Vas zamolio za pomoć oko provođenja znanstvenog istraživanja i prikupljanja dovoljnog uzorka ispitanika.

Pomoć bi se sastojala u prosljeđivanju mog e-maila koji sadrži link na anketni upitnik na Vaše kolege, zaposlenike Vaše organizacije koji koriste informacijski sustav (uzimajući u obzir širu definiciju pojma „informacijski sustav" to bi bili svi zaposlenici, neovisno o poslu koji obavljaju, koji koriste službenu elektroničku poštu). Na taj način, oni koji to žele, mogu dobrovoljno popuniti anketni upitnik, a njihov identitet je zaštićen jer ja nemam uvid u to tko je sve zaprimio poslani e-mail tj. tko sve radi u Vašoj organizaciji. Popunjavanje upitnika trajalo bi okvirno 15 minuta.

Također, potrebno je naglasiti kako se upitnikom ne bi prikupljali nikakvi osobni niti povjerljivi podaci, a popunjavanje upitnika bilo bi u potpunosti anonimno. Također, nigdje se ne bi spominjali nazivi organizacija već samo sektor kojem pripadaju, sukladno spomenutom Zakonu.

Molio bih Vas povratnu informaciju jeste li voljni uključiti se u ovo istraživanje na način da proslijedite e-mail s linkom na anketni upitnik na zaposlenike Vaše organizacije.

U nadi da ćete mi izaći u susret u vezi ove zamolbe, srdačno Vas pozdravljam.

S poštovanjem,
Krunoslav Arbanas
(krunoslav.arbanas@gmail.com; karbanas@foi.hr)

Arbanas K.

Poštovani/a,

Ovim putem zamolio bih Vas za sudjelovanje u popunjavanju anketnog upitnika u sklopu istraživanja za doktorsku disertaciju pod nazivom "*Radni okvir za procjenu i unapređenje kulture informacijske sigurnosti*". Autor doktorske disertacije je Krunoslav Arbanas, a mentori su prof. dr. sc. Mario Spremić s Ekonomskog fakulteta Sveučilišta u Zagrebu i doc. dr. sc. Nikolina Žajdela Hrustek s Fakulteta organizacije i informatike Varaždin Sveučilišta u Zagrebu.

Podaci prikupljeni ovim upitnikom omogućit će potpuniji uvid u čimbenike kulture informacijske sigurnosti unutar organizacije te koristiti za postavljanje temelja predloženog radnog okvira.

Budući da nije moguće pohraniti djelomično popunjen upitnik, molim Vas da cijeli upitnik ispunite odjednom. Upitnik je podijeljen na 11 dijelova, a vrijeme potrebno za ispunjavanje upitnika je okvirno 15 minuta.

Vaši odgovori u ovoj anketi su anonimni i ne mogu se povezati s Vama, a bit će korišteni samo u svrhu ovog istraživanja.

Link na anketni upitnik: **http://limesurvey.srce.hr/652878**

Hvala Vam na susretljivosti i strpljenju!

Krunoslav Arbanas (karbanas@foi.hr)

Prilog 6. Deskriptivna statistička analiza

KATEGORIJA ORGANIZACIJSKE MJERE									
ČIMBENIK POLITIKE I ULOGE									
Čestice		u potpunosti se ne slažem	uglavnom se ne slažem	niti se slažem niti ne slažem	uglavnom se slažem	u potpunosti se slažem	nije primjenjivo	$\bar{x}$	σ
POL1	Moja organizacija uspostavila je pravila ponašanja vezanih uz korištenje informacijske imovine	3,77	3,35	10,46	27,20	54,39	0,84	4,26	1,03
POL3	Politika informacijske sigurnosti jasno ističe važnost informacijske sigurnosti za organizaciju	4,18	4,18	12,13	26,36	51,88	1,26	4,19	1,07
POL4	Procedure za implementaciju politike informacijske sigurnosti (npr. procedura upravljanja korisničkim računima, procedura upravljanja promjenama u sustavu, procedura upravljanja sigurnosnim incidentima…) su jasno definirane i dokumentirane	5,86	5,86	14,23	32,22	40,59	1,26	3,97	1,15
POL5	Sadržaj politike informacijske sigurnosti lako je razumljiv	5,02	6,28	21,34	35,98	29,71	1,67	3,80	1,09
POL6	Sigurnosne politike i procedure su lako dostupne u mojoj organizaciji	6,28	9,62	17,15	28,87	36,82	1,26	3,81	1,21
POL7	U mojoj organizaciji, jasno su definirane disciplinske mjere u slučaju kršenja odredbi sigurnosne politike	8,79	8,37	28,03	28,45	24,27	2,09	3,52	1,20
POL8	Ako se otkrije da sam kršio/la organizacijske politike informacijske sigurnosti bit ću kažnjen/a	6,28	9,21	27,20	25,10	28,87	3,35	3,63	1,17
POL9	U mojoj organizaciji definirana je osoba kojoj se mogu obratiti s pitanjima vezanim uz informacijsku sigurnost	4,60	3,77	15,06	14,64	59,83	2,09	4,24	1,12
POL10	U mojoj organizaciji jasno su definirane uloge i odgovornosti zaposlenika vezane za informacijsku sigurnost	2,93	12,55	16,32	27,20	39,75	1,26	3,89	1,15
POL11	Upoznat/a sam sa svojim odgovornostima vezanim uz informacijsku sigurnost	3,77	8,37	14,23	24,69	46,03	2,93	4,04	1,13
ČIMBENIK EDUKACIJA									
Čestice		u potpunosti se ne slažem	uglavnom se ne slažem	niti se slažem niti ne slažem	uglavnom se slažem	u potpunosti se slažem	nije primjenjivo	$\bar{x}$	σ
EDU2	Edukacije vezane uz informacijsku sigurnost koje nudi moja organizacija su korisne	3,35	8,79	23,43	28,03	29,29	7,11	3,77	1,06
EDU3	U mojoj organizaciji podržava se periodično održavanje radionica za zaposlenike na temu informacijske sigurnosti	14,23	16,74	21,76	27,20	16,74	3,35	3,16	1,29
EDU5	Zaposlenici su educirani oko svojih uloga i odgovornosti vezanih za informacijsku sigurnost i toga kako se ponašati na siguran način	7,95	17,57	24,27	30,54	18,83	0,84	3,35	1,20

EDU6	Zbog edukacija vezanih uz informacijsku sigurnost osjećam se bolje pripremljen/a za potencijalne sigurnosne incidente	7,53	12,55	25,10	28,45	23,01	3,35	3,48	1,19
EDU7	Smatram da je znanje o informacijskoj sigurnosti mojih kolega u organizaciji na zadovoljavajućoj razini	10,04	17,99	28,87	25,94	16,74	0,42	3,21	1,21
EDU15	U mojoj organizaciji koriste se različiti oblici komunikacije (npr. e-mail, plakati, post-it poruke, newsletter,…) za promicanje svijesti o informacijskoj sigurnosti	10,88	13,81	20,92	25,94	27,62	0,84	3,46	1,32
ČIMBENIK SIGURNOSNA OSVIJEŠTENOST									
Čestice		u potpunosti se ne slažem	uglavnom se ne slažem	niti se slažem niti ne slažem	uglavnom se slažem	u potpunosti se slažem	nije primjenjivo	$\bar{x}$	σ
EDU1	Ako imam priliku, sudjelovat ću na edukacijama i radionicama vezanim uz informacijsku sigurnost	2,51	2,51	7,95	32,22	53,97	0,84	4,34	0,91
EDU10	Ako ja ne pridajem dovoljno pažnje odredbama politike informacijske sigurnosti, informacijska imovina moje organizacije je podložna riziku	2,09	2,93	12,13	26,36	54,81	1,67	4,31	0,94
EDU11	Čak i ako mogu, ne smijem isključiti antivirusni program na svom računalu	3,77	2,09	6,28	10,04	74,48	3,35	4,55	0,97
EDU13	Neću otkriti svoju lozinku za pristup računalu nikome pa čak ni svom nadređenom	12,55	8,79	13,81	14,64	49,37	0,84	3,80	1,44
EDU14	Osjećam se pouzdano u svoje razumijevanje sigurnosne politike u mojoj organizaciji	2,93	10,04	20,08	31,38	34,73	0,84	3,86	1,09
EDU17	Upoznat/a sam sa sigurnosnim politikama, procedurama i smjernicama moje organizacije	4,60	10,04	13,39	30,13	41,84	0,00	3,95	1,17
EDU18	Znam što je "incident informacijske sigurnosti"	9,21	5,86	8,37	31,38	44,77	0,42	3,97	1,26
EDU19	Znam što podrazumijeva pojam "informacijska sigurnost"	2,09	4,60	9,62	30,13	53,14	0,42	4,28	0,96
ČIMBENIK PODRŠKA RUKOVODSTVA									
Čestice		u potpunosti se ne slažem	uglavnom se ne slažem	niti se slažem niti ne slažem	uglavnom se slažem	u potpunosti se slažem	nije primjenjivo	$\bar{x}$	σ
MNG3	Rukovodstvo u mojoj organizaciji omogućuje dovoljno financijskih i ljudskih resursa za upravljanje informacijskom sigurnošću	6,69	10,46	28,87	29,71	22,18	2,09	3,51	1,14
MNG4	Rukovodstvo u mojoj organizaciji preuzima krajnju odgovornost za informacijsku sigurnost	5,86	14,23	28,87	28,45	20,92	1,67	3,45	1,14
MNG5	Rukovodstvo u mojoj organizaciji pridržava se odredbi politike informacijske sigurnosti	5,02	7,11	27,20	29,29	29,71	1,67	3,73	1,11
MNG7	U mojoj organizaciji vidljiva je predanost i potpora od strane rukovodstva vezano za informacijsku sigurnost	6,28	13,39	22,18	32,22	25,10	0,84	3,57	1,18

KATEGORIJA SOCIOLOŠKI ČIMBENICI									
ČIMBENIK UVJERENJA									
Čestice		u potpunosti se ne slažem	uglavnom se ne slažem	niti se slažem niti ne slažem	uglavnom se slažem	u potpunosti se slažem	nije primjenjivo	$\bar{x}$	σ
BHV2	Primjena dobrih praksi vezanih uz sigurnost informacijske imovine predstavlja prihvaćeni način poslovanja u mojoj organizaciji	4,60	5,44	18,41	28,87	41,84	0,84	3,99	1,11
BHV4	Zaposlenici u mojoj organizaciji preuzimaju odgovornost za zaštitu informacija s kojima dolaze u doticaj	5,86	9,21	23,01	33,05	27,62	1,26	3,68	1,14
BLF3	Smatram da moja organizacija daje dovoljno pažnje strategiji informacijske sigurnosti s ciljem zaštite informacijske imovine	6,69	11,72	21,76	35,98	23,43	0,42	3,58	1,16
BLF5	Uvjeren/a sam da drugi zaposlenici poštuju odredbe politike informacijske sigurnosti u mojoj organizaciji	7,95	14,23	29,29	33,05	15,06	0,42	3,33	1,14
ČIMBENIK PONAŠANJE									
Čestice		u potpunosti se ne slažem	uglavnom se ne slažem	niti se slažem niti ne slažem	uglavnom se slažem	u potpunosti se slažem	nije primjenjivo	$\bar{x}$	σ
BHV1	Ako poštujem pravila vezana uz informacijsku sigurnost, mogu pomoći u zaštiti informacijske imovine svoje organizacije	2,09	1,67	5,86	17,99	72,38	0,00	4,57	0,85
BHV3	Svoje znanje o informacijskoj sigurnosti dijelim s kolegama/icama kako bih povećao/la njihovu svijest o toj tematici	5,02	5,02	11,30	37,24	41,00	0,42	4,05	1,09
BLF1	Informacijski sustav moje organizacije siguran je toliko koliko ga ja činim sigurnim	4,18	4,60	23,43	32,22	34,31	1,26	3,89	1,06
BLF6	Zaposlenik koji krši politiku informacijske sigurnosti šteti svojoj organizaciji	2,09	2,51	3,35	23,01	68,62	0,42	4,54	0,85
KATEGORIJA TEHNIČKE MJERE									
ČIMBENIK OČUVANJE POVJERLJIVOSTI I DOSTUPNOSTI									
Čestice		u potpunosti se ne slažem	uglavnom se ne slažem	niti se slažem niti ne slažem	uglavnom se slažem	u potpunosti se slažem	nije primjenjivo	$\bar{x}$	σ
BCK2	Proces redovne izrade sigurnosne kopije (eng. backup) i povrata podataka (eng. restore) značajno doprinosi dostupnosti kritičnih informacija	3,35	1,67	7,11	21,76	63,18	2,93	4,44	0,94
BCK3	Proces redovne izrade sigurnosne kopije (eng. backup) i povrata podataka (eng. restore) značajno doprinosi mogućnosti oporavka poslovanja u slučaju pojave katastrofalnog događaja	2,09	0,84	3,35	18,83	73,22	1,67	4,63	0,77
AA1	Informacije trebaju biti zaštićene od neovlaštene upotrebe (čitanja, izmjene, brisanja)	1,26	1,26	2,93	11,72	82,85	0,00	4,74	0,69

AA2	Prilikom promjene lozinke, ona mora biti određene duljine i kombinacija malih i velikih slova te brojeva	2,51	0,84	4,18	12,13	80,33	0,00	4,67	0,81
AA4	Svim povjerljivim informacijama treba se moći pristupiti samo s odgovarajućim korisničkim imenom i lozinkom	2,51	1,67	1,67	12,13	82,01	0,00	4,69	0,81
AA5	U mojoj organizaciji uspostavljeni su odgovarajući mehanizmi kojima se osigurava da pristup informacijskom sustavu imaju samo ovlaštene osobe (npr. upotrebom korisničkog imena i lozinke)	3,35	1,67	6,28	15,90	72,38	0,42	4,53	0,94
AA6	Važno je da informacijski sustav ima mogućnost utvrđivanja individualne odgovornosti zaposlenika za poduzete radnje	1,26	1,67	7,53	17,57	71,55	0,42	4,57	0,81
ČIMBENIK OČUVANJE INTEGRITETA									
Čestice		u potpunosti se ne slažem	uglavnom se ne slažem	niti se slažem niti ne slažem	uglavnom se slažem	u potpunosti se slažem	nije primjenjivo	$\bar{x}$	σ
AV1	Antivirusni sustav barem jednom tjedno skenira moje računalo	2,09	4,60	19,67	20,50	51,46	1,67	4,17	1,03
AV2	Antivirusni sustav instaliran na mom računalu redovito se ažurira	2,09	2,51	11,72	20,50	62,76	0,42	4,40	0,94
BCK4	Znam gdje trebam pohranjivati bitne podatke kako bi se izradila njihova sigurnosna kopija (eng. backup)	5,86	9,62	8,37	17,15	57,32	1,67	4,12	1,25

Životopis

Krunoslav Arbanas rođen je 06. svibnja 1983. godine u Požegi gdje je i završio Prirodoslovno-matematičku gimnaziju. Diplomirao je 2007.g. na Fakultetu organizacije i informatike, smjer Informacijski sustavi. 2008.g. zapošljava se u Zagrebu kao mlađi konzultant iz područja upravljanja informacijskom sigurnošću i kontinuitetom poslovanja, najprije u tvrtki Trilix d.o.o. te potom u tvrtki ECS d.o.o. u kojima ostaje zajedno nešto više od 2 i pol godine. Nakon toga, 2011.g. zapošljava se kao savjetnik za informacijsku sigurnost u Uredu ravnatelja u Agenciji za plaćanja u poljoprivredi, ribarstvu i ruralnom razvoju gdje radi do 2019. godine nakon čega se zapošljava kao osoba zadužena za informacijsku sigurnost u Uredu predsjednika Upravnog vijeća u Hrvatskoj energetskoj regulatornoj agenciji, gdje radi do danas.

Područja interesa su mu informacijska sigurnost, zaštita privatnosti, usklađenost s normativnom i zakonskom regulativom (engl. *Compliance*) te ICT vještine i kompetencije. Koautor je jedne knjige i nekoliko znanstvenih članaka.

Posjeduje nekoliko svjetski relevantnih certifikata s područja sigurnosti i revizije informacijskih sustava: Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), Certified in Risk and Information Systems Control (CRISC) te Certified in the Governance of Enterprise IT (CGEIT).

Popis objavljenih radova

Knjige

1. Krakar Zdravko, Tomić Rotim Silvana, Žgela Mario, **Arbanas Krunoslav**, Kišasondi Tonimir, „Korporativna informacijska sigurnost“, Fakultet organizacije i informatike, Varaždin, 2014. (udžbenik)

Znanstveni članci objavljeni u časopisima s međunarodnom recenzijom

1. **Arbanas Krunoslav**, Nikolina Žajdela Hrustek, „Key Success Factors of Information Systems Security“, *Journal of Information and Organizational Sciences 43(2)*:131-144, 2019.

2. Mekovec Renata, Pažur Aničić Katarina, **Arbanas Krunoslav**, „Developing undergraduate IT students's generic competencies through problem-based learning“, *TEM Journal 7(1)*:193-200, 2018.

3. Pažur Aničić Katarina, Divjak Blaženka, **Arbanas Krunoslav**, „Preparing ICT Graduates for Real World Challenges: Results of a Meta-Analysis“, *IEEE Transactions on Education 60(3)*:191-197, 2017.

4. Pažur Aničić Katarina, Divjak Blaženka, **Arbanas Krunoslav**, „Prestige and Collaboration Among Researchers in the Field of Education and Career Development of ICT Graduates: Is There a Cross-Fertilization of Research and Knowledge?“, *Journal of Information and Organizational Sciences 41(2)*:231-262, 2017.

5. **Arbanas Krunoslav**, Mirko Čubrilo, „Ontology in Information Security“, *Journal of Information and Organizational Sciences 39(2)*: 107-136, 2015.

6. Pažur Aničić Katarina, **Arbanas Krunoslav**, „Right Competencies for the right ICT Jobs – case study of the Croatian Labor Market“, *TEM Journal 4(3)*:236-243, 2015.

Znanstveni članci objavljeni u zbornicima konferencija s međunarodnom recenzijom

1. Alagić Dino, **Arbanas Krunoslav**, „Analysis and comparison of algorithms in advanced web clusters solutions“, *Proceedings of the 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pages 205-213, Opatija, Croatia, 2016.

2. **Arbanas Krunoslav**, Alagić Dino, „Requirements of practice in relation to the existing information technology and security management competencies“, *Proceedings of the 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pages 1411-1416, Opatija, Croatia, 2014.