UTJECAJ PERCEPCIJE PRIJETNJE NA NAMJERU UPRAVLJANJA KIBERNETIČKIM RIZICIMA: ULOGA KOGNITIVNIH PRISTRANOSTI I EMOCIJA

Kovač, Dujam

SVEUČILIŠTE U SPLITU
EKONOMSKI FAKULTET

DUJAM KOVAČ

UTJECAJ PERCEPCIJE PRIJETNJE NA NAMJERU UPRAVLJANJA KIBERNETIČKIM RIZICIMA: ULOGA KOGNITIVNIH PRISTRANOSTI I EMOCIJA

DOKTORSKA DISERTACIJA

Split, 2024.

SVEUČILIŠTE U SPLITU
EKONOMSKI FAKULTET

POSLIJEDIPLOMSKI SVEUČILIŠNI STUDIJ
EKONOMIJE I POSLOVNE EKONOMIJE

Dujam Kovač

UTJECAJ PERCEPCIJE PRIJETNJE NA NAMJERU UPRAVLJANJA KIBERNETIČKIM RIZICIMA: ULOGA KOGNITIVNIH PRISTRANOSTI I EMOCIJA

DOKTORSKA DISERTACIJA

Mentorica: prof. dr. sc. Marijana Ćurak

Split, 2024.

SAŽETAK

U digitaliziranom poslovnom okružju, kibernetički rizici pojavljuju se kao značajna prijetnja poslovanju organizacija, potencijalno ugrožavajući njihovu uspješnost, ugled te ostvarenje strateških ciljeva. Uloga glavnih izvršnih menadžera postaje ključna u poticanju promjena koje vode upravljanju kibernetičkim rizicima te integraciji istog u proces upravljanja poslovnim rizicima (*engl. Enterprise risk management – ERM*). Međutim, percepcija i odluke glavnih izvršnih menadžera često nisu pod utjecajem samo objektivnih činjenica, a racionalnost također može biti ograničena kognitivnim pristranostima i emocijama. Prepoznajući navedeno, bitno je razumjeti kako pristranosti i emocije utječu na percepcije menadžera i odlučivanje povezano s kibernetičkim rizicima te kako time oblikuju cjelokupni organizacijski pristup upravljanju kibernetičkim rizicima.

U području namjera i ponašanja u vezi kibernetičkih rizika, kao adekvatan teorijski okvir analize izdvaja se **teorija motivacije za zaštitom** (*engl. Protection motivation theory – PMT*) koja pretpostavlja da je namjera upravljanja kibernetičkim rizicima određena percepcijom kibernetičkih rizika kao prijetnje za poslovanje organizacije (percepcija prijetnje) i percepcijom sposobnosti organizacije u upravljanju kibernetičkim rizicima (percepcija suočavanja). Uočen izostanak empirijske potvrde utjecaja percepcije prijetnje na namjeru upravljanja, motiv je nadogradnje teorije motivacije za zaštitom.

Istraživanje bazirano na teoriji motivacije za zaštitom te njenoj nadogradnji za pretpostavke bihevioralne ekonomije ima za cilj produbiti razumijevanje namjera glavnih izvršnih menadžera prema upravljanju kibernetičkim rizicima u organizacijskom okruženju. Proširenjem tradicionalnog teorijskog okvira naglašava se uloga kognitivnih pristranosti i emocija, pri čemu se nastoji istražiti učinak kognitivnih pristranosti na percepciju prijetnje kibernetičkih rizika te posrednička uloga emocija između percepcije prijetnje i namjere upravljanja kibernetičkim rizicima. S obzirom na obilježja kibernetičkih rizika, kao što su evolucijska priroda, kompleksnost, recentnost te ograničena pouzdanost povijesnih podataka, pristranost optimizma i pristranost dostupnosti izdvojeni su u okviru istraživanja kao utjecajni čimbenici na percepciju kibernetičkih rizika kao prijetnje, dok emocije i žaljenje u modelu preuzimaju posredničku ulogu.

Empirijsko istraživanje temeljeno je na odgovorima 673 glavna izvršna menadžera koji upravljaju poslovnim organizacijama u Republici Hrvatskoj. Odgovori su prikupljeni putem

anketnog upitnika u elektroničkoj formi u razdoblju od 24. svibnja 2023. do 1. srpnja 2023. godine. Primijenjena je **metoda modeliranja strukturalnim jednadžbama** koja je kao složeni analitički pristup utemeljena na kombiniranju faktorske analize, analize puta i analize višestruke regresije. S obzirom na postavljeni cilj istraživanja koji je eksplorativne naravi, složenost konceptualnog modela i distribucijska svojstva prikupljenih podataka, primijenjena je PLS-SEM tehnika za procjenu modela. Analizom je potvrđeno da pristranost optimizma, kao oblik kognitivne pristranosti među glavnim izvršnim menadžerima, značajno negativno utječe na percepciju kibernetičkog rizika kao prijetnje za poslovanje organizacije. Pristranost dostupnosti, kao drugi proučavani oblik kognitivne pristranosti, pozitivno doprinosi percepciji glavnih izvršnih menadžera o kibernetičkim rizicima kao prijetnji za poslovanje organizacija. Emocije, odnosno strah i žaljenje, posreduju u odnosu između percepcije prijetnje i namjere upravljanja kibernetičkim rizicima. Potvrđuje se kako uvjerenje glavnih izvršnih menadžera u sposobnost organizacije da se suoči s kibernetičkim prijetnjama na način da istima upravlja, značajno i pozitivno utječe na namjeru upravljanja kibernetičkim rizicima. Time se potvrđuje kako je namjera upravljanja kibernetičkim rizicima određena percepcijom ekonomske provedivosti upravljanja kibernetičkim rizicima, koja ima značajniji utjecaj nego percepcija prijetnje. Rezultati potvrđuju konzistentnost kroz proširenje osnovnog modela za kontrolne varijable te kroz razmatranje modela višeg reda.

Istraživanjem se potvrđuje kako su pristranost optimizma i pristranost dostupnosti te osjećaji straha i žaljenja, čimbenici koji oblikuju odluke glavnih izvršnih menadžera u vezi upravljanja kibernetičkim rizicima. Time se potvrđuje kako je proširenje tradicionalnog koncepta teorije motivacije za zaštitom za pretpostavke bihevioralne ekonomije opravdano. S obzirom na činjenicu da se poslovanje organizacija u sve značajnijoj mjeri oslanja na digitalna rješenja, izloženost kibernetičkom prostoru sve je izraženija, a digitalni svijet postaje sve umreženiji, izloženost kibernetičkim rizicima postaje neizbježna. Postupak identifikacije i kvantifikacije kibernetičkih rizika postaje sve kompleksniji, a donošenje odluka u uvjetima nepotpunih informacija sve izglednije. Stoga, nemogućnost oslanjanja na objektivne pokazatelje ostavlja prostor utjecaju bihevioralnih čimbenika u oblikovanju odluka koje se odnose na upravljanje kibernetičkim rizicima, što je istraživanjem i potvrđeno.

KLJUČNE RIJEČI: Kibernetički rizici, upravljanje kibernetičkim rizicima, teorija motivacije za zaštitom, bihevioralna ekonomija, kognitivne pristranosti, emocije, glavni izvršni menadžeri, PLS-SEM

ABSTRACT

In today's digitized business environment, cyber risks pose a significant threat to operations of organizations, potentially endangering their success, reputation, and the achievement of strategic goals. The role of chief executive officers is crucial in initiating changes that lead to cyber risk management and their integration into the enterprise risk management process (ERM). It's essential to recognize that managers' decisions concerning cyber risks are not solely based on objective facts but can be also influenced by cognitive biases and emotions.

Based on a review of literature in the area of intentions and behaviours related to cyber risks, the protection motivation theory (PMT) emerges as an adequate theoretical framework. This theory posits that the intention to manage cyber risks is influenced by the perception of cyber risks as a threat to an organization's operations (threat perception) and the organization's perceived ability to handle these risks (coping perception). The noticeable absence of empirical evidence regarding the influence of threat perception on management intentions underscores the need to further develop the protection motivation theory.

This research, grounded in the protection motivation theory and enriched with insights from behavioural economics, delves into understanding of the intentions of chief executive officers toward cyber risk management. Aiming to expand upon the conventional theoretical framework, the research delves into the influence of cognitive biases and emotions and considers the unique characteristics of cyber risks such as their evolutionary nature, complexity, recent emergence, and the lack of reliable historical data. It examines how specific biases, such as optimism and recency, shape the perception of cyber threats, and explores the intermediary role of emotions, such as fear and regret, in bridging the gap between threat perception and the intent to manage these risks.

The empirical research is based on the responses of 673 chief executive officers from companies in Croatia and the core research data was collected through an electronic questionnaire in the period from May 24 to July 1, 2023. Structural equation modelling was the primary analytical method, intertwining factor analysis, path analysis, and multiple regression analysis. Given the study's exploratory nature, the complexity of the conceptual model, and the distributional properties of the collected data, the PLS-SEM technique was used to evaluate the model. Findings indicate that optimism bias among chief executive officers diminishes the perception of cyber risk, while recency bias enhances it. Emotions, like fear and regret, act as mediators

between threat perception and risk management intentions. Furthermore, a manager's confidence in an organization's ability to handle cyber threats has a positive correlation with their intention to manage these risks. This confirms that the intention to manage cyber risks is determined by the perception of the economic feasibility of managing cyber risks, which has a more significant impact than the perception of the threat. Results remained consistent even when extending the model for control variables and examining a higher-order model.

The study underscores how biases, like optimism bias and recency bias, along with emotions such as fear and regret, play pivotal roles in shaping chief executive officers' cyber risk management decisions. This reinforces the argument for broadening the traditional protection motivation theory to include elements of behavioural economics. Cyber risk exposure grows as the digital realm becomes more interconnected and organizations lean more on digital solutions. Navigating this complex landscape, often with incomplete information, highlights the increasing influence of behavioural factors in cyber risk management decision-making, as confirmed by the research.

KEYWORDS: Cyber risks, risk cyber management, protection motivation theory, behavioural economics, cognitive biases, emotions, chief executive officers, PLS-SEM.

SADRŽAJ

1. UVOD

Kibernetički rizici sve su veća prijetnja poslovanju organizacija, što je u najznačajnijem dijelu posljedica integracije informacijsko-komunikacijske tehnologije u poslovne procese. Recentni podaci o stanju poslovnog sektora (Allianz 2023; Deloitte, 2023; Ponemon Institute, 2023; Verizon, 2022) potvrđuju da su kibernetički rizici sve učestalija pojava, a prema sugestijama Gale et al. (2022), Strupczewski (2021), Eling et al. (2021), Eling (2020), Eling i Wirfs (2016), istraživanje kibernetičkih rizika aktualno je i relevantno područje proučavanja.

Značajan problem suočavanja poslovnih organizacija s kibernetičkim rizicima proizlazi iz izostanka prakse upravljanja kibernetičkim rizicima, koja kao proces obuhvaća identifikaciju rizika, njihovu kvantifikaciju, integraciju, prioritizaciju, primjenu odgovarajućih metoda upravljanja rizicima te provedbu nadzora cjelokupnog procesa upravljanja. Niži stupanj razvijenosti sustava upravljanja kibernetičkim rizicima, u odnosu na razvijenost sustava upravljanja tradicionalnim rizicima, obilježje je koje dominira unutar poslovnog sektora. Razlika razvijenosti sustava jednim se dijelom može opravdati činjenicom kako je riječ o rizicima koji su recentni te koji, sukladno tehnološkim promjenama, imaju dinamičnu prirodu.

Neizvjesnost i nedostatak potpunih informacija najbolje opisuju odluke u području kibernetičkih rizika, a menadžeri suočeni sa zadatkom donošenja poslovnih odluka, upravo zbog navedenog, skloni su kognitivnim pristranostima koje mogu dovesti do netočnih prosudbi i pojave emocija, koje zajedno postaju važna odrednica procjene, namjere i ponašanja. Ranija istraživanja potvrđuju da profesionalni donositelji odluka odstupaju od racionalnog ponašanja prilikom odlučivanja te da je za potrebe razumijevanja njihovih poslovnih odluka potrebno uvažiti pretpostavke bihevioralne ekonomije (Brundin et al., 2022; Kahneman et al., 2019; Brundin i Liu, 2015; Powell et al., 2011; Hodgkinson i Clarke, 2007).

Činjenica da kibernetički rizici postaju sve učestalija prijetnja te da se istima nedovoljno upravlja iziskuje pristup temeljen na pretpostavkama bihevioralne ekonomije prilikom proučavanja procjene, namjere i u konačnici ponašanja u vezi kibernetičkih rizika. Problem organizacije u suočavanju s kibernetičkim rizicima razmatra se iz perspektive glavnog izvršnog menadžera koji je ključan nositelj organizacijske promjene, pa tako i usvajanja pozitivne prakse upravljanja kibernetičkim rizicima na razini organizacije.

U nastavku uvodnog poglavlja detaljnije se izlažu temeljne postavke istraživanja, predstavljaju se *problem i predmet istraživanja*, *ciljevi istraživanja*, *metodologija istraživanja*, *znanstveni doprinos istraživanja* te *struktura rada*.

1.1. Problem i predmet istraživanja

Kibernetički rizici predstavljaju sve izraženiju prijetnju poslovanju organizacija

Organizacije u sve većoj mjeri koriste podatke kako bi transformirale svoje poslovanje i time unaprijedile poslovni model te razvile nove izvore konkurentske prednosti. U stvarnosti, one egzistiraju u okolini koja je u sve većoj mjeri oslonjena na digitalna rješenja i u kojoj su sve učestalija dijeljenja povjerljivih digitalnih podataka.[1] Oslanjanje poslovnih organizacija na podatke je proces koji će se neprekinuto nastaviti (Rydning et al., 2018).

Pojavom povezanih uređaja i mreža mijenja se količina podataka koju organizacija generira te se istodobno povećava obuhvat i složenost virtualnog okružja, odnosno **kibernetičkog prostora** koji je rezultat interakcije čovjeka, tehnoloških rješenja i usluga (Arbanas, 2021). Razvoj tehnologije prati brz i dinamičan razvoj novih proizvoda i usluga, dok sigurnosni aspekti, u pravilu, imaju malen utjecaj na dinamiku prihvaćanja novih tehnologija. Navedene promjene popraćene su sve većom ranjivosti organizacija na *povjerljivost, cjelovitost i dostupnost* **digitalnih podataka** i **tehnoloških rješenja** koja služe za *pohranjivanje i prijenos* digitalnih podataka.

Prema barometru rizika kojeg objavljuje Allianz (2023) na temelju istraživanja koje je obuhvatilo preko dvije i pol tisuće stručnjaka za područje upravljanja rizicima, kibernetički rizici svrstani su na prvo mjesto među rizicima kojima su izložene poslovne organizacije. Isti su rizici u istraživanju iz 2013. godine zauzeli tek 15. mjesto, temeljem čega se jasno zaključuje kako **raste značajnost kibernetičkih rizika i svijest o kibernetičkim prijetnjama među stručnjacima u području upravljanja rizicima**.

Ponemon Institute (2023) analizira 553 organizacije, iz 17 različitih industrija i 16 različitih zemalja, koje su pretrpjele slučaj povrede podataka (*engl. data breach*) u razdoblju između

[1] Prema Statista (2023), ukupna količina podataka za koju se predviđa da će biti stvorena, snimljena, kopirana i pregledana na globalnoj razini u 2023. godini iznosi 120 zetabajta, a predviđa se da će taj broj porasti na 181 zetabajt do 2025. godine. Dodatno, procjena je kako će do 2025. godine u prosjeku svaka osoba koja koristi prednosti umreženih uređaja imati barem jednu interakciju s podacima svakih 18 sekundi (Reinsel et al., 2018).

ožujka 2022. i ožujka 2023. godine. Među proučavanim organizacijama, prosječni trošak štete uzrokovane povredom podataka iznosi 4,45 mil. USD što je povećanje od 15,3 % u odnosu na izvještaj iz 2020. godine. Deloitte (2023) izvještava o nastavku trenda sve učestalije pojave kibernetičkih incidenata na temelju istraživanja koje obuhvaća organizacije s godišnjim prihodom većim od 500 milijuna USD te s više od tisuću zaposlenih, a koje je provedeno u više od 20 zemalja svijeta. Na osnovi odgovora više od tisuću stručnjaka iz područja kibernetičke sigurnosti uključenih u istraživanje, potvrđuje se kako je 91 % organizacija pretrpjelo barem jedan incident, a kod 55 % organizacija kibernetički rizik uzrokovao je umjerene i ozbiljne posljedice.

U redovnom godišnjem izvještaju o kibernetičkim incidentima za 2022. godinu, Verizon (2022) je analizirao više od 23 tisuće incidenata, pri čemu je zabilježeno više od 5,2 tisuće slučajeva povrede podataka. Ranjivost iskazuju sve industrije, a najčešći je oblik incidenta socijalni inženjering i to u obliku napada preko elektroničke pošte s ciljem krađe identiteta (*engl. phishing*). Eksterna prijetnja bitno je značajniji uzrok nastalih incidenata, a najčešće su kompromitirani osobni podaci.

Kibernetički kriminal kao oblik kibernetičkog rizika najčešće je predmet izvještavanja te se izdvaja kao ključna prepreka u korištenju prednosti kibernetičkog prostora, pri čemu značajno narušava povjerenje u tehnološke promjene (World Economic Forum, 2020). Realizira se u različitim oblicima, primjerice; *napad s ciljem krađe identiteta, zlonamjerni softver, ucjenjivački softver, špijunski softver, virus,* i napad s različitim motivima. Prema istraživanju Morgan (2022), očekuje se da će kibernetički kriminal u 2023. godini prouzročiti štetu u vrijednosti od 8 trilijuna USD. Provodeći usporedbu veličine štete s veličinom nacionalnih gospodarstava, šteta je manja samo od gospodarstava Sjedinjenih Američkih Država i Kine. Istodobno, očekuje se kako će globalni troškovi kibernetičkog kriminala rasti s godišnjom stopom od 15 %, pri čemu se visina troškova u 2025. godini procjenjuju na 10,5 trilijuna USD.[2] Prema Aiyer et al. (2022) riječ je o porastu od 300 % u odnosu na 2015. godinu.

Kibernetički kriminal postaje organiziran te je sve češće rezultat koordiniranog djelovanja većeg broja pojedinaca. Kriminalci učestalije koriste napredne alate poput umjetne inteligencije

[2] Troškovi uzrokovani kibernetičkim kriminalom, prema istraživanju Morgan (2022), uključuju razne vrste šteta, kao što su *oštećenje i uništavanje podataka*, *otuđenje osobnih podataka, otuđenje novca*, *poremećaj u normalnom tijeku poslovanja* i *pad produktivnosti*, *otuđenje intelektualnog vlasništva*, *pronevjeru, provođenje forenzičke istrage*, *obnovu podataka i sustava te narušen ugled*.

te strojnog učenja, a napadi postaju sve kreativniji, što povećava zahtjeve **kibernetičke sigurnosti** u organizacijama (Trend Micro, 2023).

Nedvojbeno, trenutačni položaj poslovnih organizacija nepovoljan je u smislu izloženosti kibernetičkim rizicima, dok je budućnost uvjetovana činjenicom koliko su organizacije spremne usvojiti promjenu te implementirati napredne tehnologije u promicanju kibernetičke sigurnosti. Creese et al. (2022) izdvajaju pojavu umjetne inteligencije, naprednog strojnog učenja te kvantnih računala, kao realitete kojima se potrebno prilagoditi. Zbog povećane složenosti novih tehnologija te njihove ubrzane implementacije, postavlja se pitanje korisnosti postojećih spoznaja o upravljanju kibernetičkim rizicima. Poseban osvrt pridaje se vodstvu organizacije koje mora biti svjesno na koji način nove tehnologije utječu na upravljanje izloženosti organizacije kibernetičkim rizicima te mora biti spremno napraviti nužne promjene kako bi se kibernetičkim rizikom upravljalo, a time i njihov utjecaj zadržao na prihvatljivoj razini (Boehm et al., 2022).[3]

Izostanak prakse upravljanja kibernetičkim rizicima u poslovnim organizacijama

Upravljanje kibernetičkim rizicima proces je koji objedinjuje *identifikaciju, kvantifikaciju* (procjenu potencijalnih utjecaja na poslovanje), *integraciju* (izradu agregiranog profila rizika za poslovnu organizaciju), *prioritizaciju*, potom *izbor* i *primjenu* određene *metode upravljanja rizikom* prema relevantnom kriteriju te *nadzor* (Stine et al., 2020; Harrington i Niehaus, 2004). Proces upravljanja kibernetičkim rizicima obuhvaća tehnike smanjivanja rizika poduzimanjem mjera kibernetičke sigurnosti te financijske kontrole zadržavanjem rizika i transferom rizika na društvo za osiguranje (Eling et al., 2021; Marotta i McShane, 2018; Gordon et al., 2003). Upravljanje kibernetičkim rizicima način je kojim organizacije mogu smanjiti očekivani trošak kibernetičkih rizika i povećati vrijednost poduzeća (Tatar i Karabacak, 2012; Chen et al., 2011). Stoga, uvažavajući kontekst u kojem organizacije egzistiraju, upravljanje kibernetičkim rizicima treba dobiti na važnosti (Kovač, 2021).[4]

---

[3] Prema Ponemon institute (2022), organizacije koje su implementirale sustav zaštite temeljen na umjetnoj inteligenciji brže su otkrile i zaustavile povredu podataka u usporedbi s organizacijama koje nisu koristile umjetnu inteligenciju, što je značajno utjecalo na smanjenje razine štete. Vrijeme koje je bilo potrebno za identificiranje i zaustavljanje povrede podataka bilo je 74 dana kraće te su troškovi bili za više od 3 mil. USD manji u slučaju organizacija koje su koristile prednosti umjetne inteligencije.

[4] Paralelno s razvojem prijetnje, povećavaju se ulaganja u kibernetičku sigurnost koja će za poslovne organizacije na globalnoj razini u 2023. godini iznositi 188 milijardi USD (Kapko, 2022). Uspoređujući razmjere ulaganja u kibernetičku sigurnost i godišnje štete uzrokovane kibernetičkim rizicima, zaključuje se kako je razina upravljanja nedovoljna (Aiyer et al., 2022.) Dodatno, projicirani godišnji rast ulaganja u

Prema Ashby et al. (2018), sustav upravljanja rizicima kod poslovnih organizacija ne uzima u obzir nove oblike rizika. Posljedica je niži razvoj sustava upravljanja kibernetičkim rizicima naspram prakse i metoda (sustava) upravljanja ostalim rizicima. Naime, kod poslovnih organizacija, koje prihvaćaju sustav integriranog upravljanja rizicima (*ERM*), potvrđuje se kako ERM zanemaruje kibernetičke rizike. Problem je tim veći što nikada nije bilo važnije razmotriti kibernetičke rizike i sigurnost kao integrirani element u okviru ERM-a (Gale et al., 2022).

Stoga, javlja se potreba za integriranjem koncepta upravljanja kibernetičkim rizicima u koncept objedinjenog upravljanja rizicima poslovnih organizacija (Hoppe et al., 2021; Soomro et al., 2016). Potonje bi značilo povećan napor u stjecanju i razmjeni znanja s ciljem postizanja napretka u razumijevanju kibernetičkih rizika i njihovim upravljanjem koje preuzima najviša razina menadžmenta. Globalna anketa o informacijskoj sigurnosti koju je proveo Price Waterhouse Coopers (2018), temeljena na odgovorima više od 9,5 tisuća profesionalaca u području upravljanja rizicima, otkriva kako se kibernetički rizici unutar uprava poduzeća još uvijek razmatraju kao problem niže razine, odnosno funkcijskog odjela. U prilog tome govori studija Ernst & Young (2018) koja otkriva kako preko tri četvrtine ispitanih profesionalaca u području rizika posluje s ograničenom kibernetičkom sigurnošću. Studija Marsh (2019), koja je uključila preko 1,5 tisuća odgovora voditelja ključnih funkcija (*izvršnih direktora, članova uprave, voditelja odjela za upravljanje rizicima*) u različitim organizacijama diljem svijeta, govori o poraznim rezultatima iz kojih je vidljivo kako je tek 17 % ispitanih izvršnih direktora i članova uprava utrošilo više od jednog radnog dana na razmatranje pitanja izloženosti organizacije kibernetičkim rizicima.

RiskOptics (2023) studija obuhvatila je 261 ispitanika koji obavljaju radne zadatke povezane s kibernetičkom sigurnošću i upravljanjem rizicima te je potvrđeno da kod glavnih izvršnih menadžera organizacija u SAD-u izostaje razumijevanje kibernetičkih rizika. Dodatno, potvrđeno je nedovoljno investiranje u kibernetičku sigurnost. Uočeno je kako izostaje adekvatna razina komunikacije voditelja informacijske sigurnosti (*engl. Chief Information Security Officer – CISO*) i voditelja odjela za informacijske tehnologije (*engl. Chief Information Officer – CIO*) s voditeljima ostalih odjela. Stine et al. (2020) ističu komunikaciju između spomenutih subjekata kao ključnu pretpostavku upravljanja rizicima. S obzirom da ERM kao proces predviđa kontinuirano odvijanje komunikacije između ključnih dionika organizacije,

kibernetičku sigurnost od 11 % do 2025. godine ukazuje kako će se zadržati nepovoljan razmjer ulaganja u kibernetičku sigurnosti i razine šteta koju uvjetuju kibernetički rizici.

potvrđuje se teza kako integracija upravljanja kibernetičkim rizicima unutar ERM-a u pravilu izostaje.

Unatoč rastućoj prijetnji kibernetičkih rizika, proračun za kibernetičku sigurnost nizak je u odnosu na ukupnu IT potrošnju (Ernst & Young, 2021). Upravljanje kibernetičkim rizicima nije išlo u korak s digitalnom transformacijom te mnoge organizacije nisu sigurne kako upravljati kibernetičkim rizicima (Boehm et al., 2022). Na tragu istraživanja Price Waterhouse Coopers (2023), koje ističe da su organizacije usmjerene na troškove koje generira upravljanje kibernetičkim rizicima, proizlazi kako je upravljanje kibernetičkim rizicima potrebno razmatrati kao investiciju koja doprinosi poslovanju organizacije u smislu smanjenja rizika i u dugom roku povećava vrijednost poslovnog subjekta.

Isticanje uloge menadžera kao faktora koji mijenja pristup prema upravljanju kibernetičkim rizicima

Ključni elementi procesa upravljanja kibernetičkim rizicima na razini organizacije određeni su čovjekovim djelovanjem (Boehm et al., 2022, Vrhovec i Mihelič, 2021; Siponen et al., 2014). Pored činjenice da poslovna organizacija razvija jasne preporuke ponašanja odnosno implementira politiku i pravila kibernetičke sigurnosti, konačni učinak, odnosno njihova uspješnost, određen je djelovanjem čovjeka. Zaposlenici poslovne organizacije identificirani su kao najveća pojedinačna prijetnja poslovanju organizacije (Dodel i Mesch, 2019; Barlette et al., 2017; Soomro et al., 2016) te je stoga njihovo ponašanje ključni segment kibernetičke sigurnosti koji je potrebno dublje razumjeti, što će organizaciju učiniti otpornijom na kibernetičke prijetnje (Larsen i Lund, 2021). Naglašena važnost zaposlenika organizacije, razlog je istraživanja motivacije i namjera, odnosno stvarnog ponašanja pojedinca u organizaciji.

Međutim, postojeća istraživanja nisu bazirana na uzorku homogenih skupina, što bi se postiglo razmatranjem točno definiranih predstavnika jedinstvenog radnog mjesta. Primjerice, da se u istraživanju razmatraju isključivo menadžeri za sigurnost ili isključivo glavni izvršni menadžeri. Potonja skupina glavnih izvršnih menadžera u ranijim se studijama potvrđuje kao ključna u postizanju privrženosti zaposlenika informacijskoj sigurnosti (Johnston i Hale, 2009). Naime, sudjelovanje najvišeg menadžmenta organizacije u upravljanju rizicima izravno i značajno utječe na stavove zaposlenika prema politikama informacijske sigurnosti te određuje organizacijsku kulturu koja izravno određuje namjere zaposlenika u pogledu pridržavanja politika informacijske sigurnosti (Hu et al., 2012).

Ukoliko menadžment prida važnost pitanju kibernetičke sigurnosti i postupa u skladu s istim, postiže se veći stupanj kibernetičke sigurnosti na razini organizacije (Hwang et al., 2021; Tu i Yuan, 2014). Stoga, u cilju postizanja kibernetičke sigurnosti, poslovne organizacije nužno trebaju razvijati primjenu tehničkih rješenja[5] obrane od kibernetičke prijetnje. Međutim, uspješnost primjene tehnološkog rješenja ovisi o politici kibernetičke sigurnosti i organizacijskim strategijama pa ih je potrebno istražiti u širem aspektu iz menadžerske perspektive (Moody et al., 2018).

Upravljanje kibernetičkim rizicima zahtijeva uspostavu procesa upravljanja kibernetičkim rizicima koji je integriran u ukupne poslovne procese, što podrazumijeva da ključnu odgovornost na sebe preuzima vodstvo poslovne organizacije. Zbog toga se kibernetička sigurnost organizacije treba razmatrati na razini uprave.

Upravljanje kibernetičkim rizicima zahtijeva jasnu ulogu vodstva u iniciranju promjena što je ključno za sigurnost organizacije (Ahmed Shaikh i Siponen, 2023; Soomro et al. 2016). Kada su menadžeri slabo uključeni u pitanje informacijske sigurnosti poslovne organizacije, to dovodi do posljedica koje mogu biti katastrofalne (Barlett et al., 2015). S obzirom da je pridržavanje mjera sigurnosti kod zaposlenika određeno postupanjem najvišeg menadžmenta (Hu et la. 2012; Dong et al., 2008), sugerira se **dublje razumjeti ponašanje najvišeg menadžmenta**. Stoga se, na tragu Barlett et al. (2015) i Hu et al. (2012) u okviru ovog istraživanja, **glavni izvršni menadžeri razmatraju kao ključ usvajanja pozitivne prakse upravljanja kibernetičkim rizicima na razini organizacije. Navedeno posebno dobiva na vrijednosti budući da se u postojećim istraživanjima malo pozornosti pridavalo vodstvu poslovnih organizacija (**Sharifi, 2023; Triplett et al., 2022; Hakami i Alshaikh, 2022; Guhr et al., 2018)**.**

Prisutnost problema nedovoljne angažiranosti vodstva organizacije u izazove kibernetičke sigurnosti, odnosno upravljanja kibernetičkim rizicima, ukazuje Enterprise Strategy Group (2020) koja je analizirala 365 iskusnih profesionalaca u vezi informacijske i kibernetičke sigurnosti na području Sjeverne Amerike, Zapadne Europe (*UK, Francuska, Njemačka*). Istraživanje je provedeno u poslovnim organizacijama s više od 100 zaposlenih, a gotovo 70 % ispitanika izjasnilo se da se **kibernetička sigurnost primarno razmatra kao tehničko pitanje** na razini najvišeg vodstva organizacije, pri čemu postoji **znatan prostor za povećanje**

[5] Navedeno je predviđeno standardima upravljanja kibernetičkim rizicima, a više detalja o standardima upravljanja dostupno je u istraživanju Fenz et al. (2014).

angažiranosti uprava poduzeća za navedeno pitanje. **Problem je posebice izražen kod vodstva organizacije koje nema temeljito razumijevanje kibernetičke sigurnosti** (Ernst & Young i Institute of Internal Auditors, 2021), a prema nalazima Price Waterhouse Coopers (2021), više od 50 % lidera u organizacijama razumije kibernetičku sigurnost u ograničenom opsegu.

Dosadašnja istraživanja bavila su se razmatranjem usklađenosti zaposlenika s politikom kibernetičke i informacijske sigurnosti. Primijenjen je niz različitih teorija kako bi se razumjela namjera, odnosno motivacija, zaposlenika poslovne organizacije za poduzimanje aktivnosti koje doprinose kibernetičkoj sigurnosti. **Među teorijskim konceptima prednjači teorija motivacije za zaštitom (PMT)** (Almansoori et al., 2023; Haag et al., 2021; Kianpour et al., 2019; Li et al., 2019; Boss et al., 2015), **koja je u predloženom istraživanju osnova razumijevanja ponašanja ključnih izvršnih menadžera**. **Prema Connelly i Shi (2022), PMT treba dati obol menadžerskoj teoriji, odnosno treba je primjenjivati u menadžerskom odlučivanju**. Nužno je da istraživači u području menadžerskih odluka odgovore koji su to čimbenici koji određuju odluke menadžera, u pogledu upravljanja kibernetičkim rizicima, koje posljedično više ili manje izlažu organizacije rizicima, pri čemu je nužno promatrati fenomen odlučivanja kroz prizmu organizacijske prijetnje i odgovora.

Zaključuje se da je angažman **vodstva poslovne organizacije ključan za postizanje otpornosti organizacije na kibernetičke rizike odnosno upravljanje istima**. Međutim, niz je prepreka u postizanju integracije upravljanja kibernetičkim rizicima u okviru ERM-a i zauzimanju aktivne uloge vodstva organizacije u upravljanju kibernetičkim rizicima.

Problematizacija razloga izostanka angažmana izvršnih menadžera u pogledu upravljanja kibernetičkim rizicima te izostanak zadovoljavajuće prakse upravljanja rizicima

Područje kibernetičkih rizika je tehničko i kompleksno područje (Gordon et al., 2015, Cambpbell et al., 2003), a prema Redseal (2016) predstavlja poseban izazov za vodstvo organizacije koje nema iskustvo ili znanja o kibernetičkim rizicima. Posljedice nedostatka tehničkog razumijevanja protežu se od neadekvatne prakse do izostanka prakse upravljanja kibernetičkim rizicima na razini organizacije. Značajna prepreka u svladavanju tehnički zahtjevnog i kompleksnog pitanja kibernetičkih rizika popraćeno je nedostatkom stručnog

kadra[6] za navedeno područje te nedostatkom adekvatne komunikacije između stručnih odjela za područje kibernetičkih rizika i vodstva organizacije[7].

U okviru ovoga istraživanja, kao ključni faktor koji onemogućava sudjelovanje vodstva organizacije u upravljanju kibernetičkim rizicima, ističe se nedovoljno razumijevanje i svijest o kibernetičkim rizicima kao prijetnji za poslovanje. **Prisutan je raskorak između stvarne kibernetičke prijetnje i prijetnje kakvu percipira vodstvo organizacije, na način da je stvarna prijetnja podcijenjena**. Kada se kibernetički rizici podcijene, manje je vjerojatno da će se s njima na odgovarajući način upravljati te da će biti integrirani u strategiju upravljanja rizicima poslovne organizacije. Budući da navedeno dovodi do većeg stupnja ranjivosti organizacija te se povećava ukupni rizični profil poslovne organizacije, u okviru ovoga istraživanja traga se za dodatnim objašnjenjem negativnog odstupanja. Bihevioralne odrednice ponašanja glavnih izvršnih menadžera, primarno kognitivne pristranosti i emocije, razmatraju se kao faktori koji određuju percepciju kibernetičkih rizika kao prijetnje odnosno namjeru upravljanja kibernetičkim rizicima na razini poslovne organizacije.

U kontekstu proučavanih bihevioralnih odrednica, a u cilju pružanja argumenta zašto se iste razmatraju, važno se osvrnuti na **karakteristike kibernetičkih rizika**. Česta prepreka u razumijevanju kibernetičkih rizika jest njihova istaknuta tehnička priroda[8](Soomro et al., 2016), ali i značajan broj otvorenih pitanja u vezi njihovih karakteristika koje se odnose na teškoće identifikacije. Kibernetički rizici često su nematerijalni[9] što otežava njihovu kvantifikaciju i razumijevanje (Biener et al., 2016; Crossler et al., 2013). Nadalje, kibernetičke rizike, zbog višestrukih izvora i prijetnji te premreženog kibernetičkog okružja, karakterizira velika složenost (Loebbecke i Picot, 2015). Međuovisnost kibernetičke sigurnosti organizacija uvjetuje stanje u kojem izloženost poslovne organizacije kibernetičkim rizicima ne ovisi isključivo o promatranom poduzeću (Heal et al., 2006), već i o drugim subjektima aktivnim u kibernetičkom prostoru, a posebice organizacijama s kojima je intenzivirano poslovanje. Potencijalno katastrofalan učinak kibernetičkih incidenata, poput značajnog financijskog gubitka ili teške reputacijske štete, karakteristika je kibernetičkih rizika. Dodatno, kontinuirano

[6] Prema Boehm et al. (2022) organizacijama nedostaju talenti, znanje i stručnost u području kibernetičke sigurnosti te se jaz povećava.

[7] Prema World Economic Forum (2023) učinkovita komunikacija temelj je uspjeha bilo kojeg programa kibernetičke otpornosti, a osobe odgovorne za upravljanje kibernetičkom sigurnosti trebale bi koristiti manje tehničkih termina kada komuniciraju s vodstvom organizacije.

[8] Rothrock et al. (2018) ukazuje kako su kibernetički rizici hipertehničkih obilježja.

[9] Sukladno ENISA (2012), prisutna su ograničenja s aspekta vremena nastanka, mjesta i uzroka kibernetičkih rizika.

prisutan tehnološki napredak uvjetuje nastanak rizika, a istodobno smanjuje relevantnost postojećih spoznaja u vezi upravljanja rizicima (Marotta et al., 2017; Biener et al., 2016). Tehnološkim napretkom, podaci i ranija iskustava s kibernetičkim rizicima manje doprinose upravljanju rizicima organizacije. Sve istaknuto u vezi karakteristika kibernetičkih rizika navodi nas na zaključak kako je mjerenje učestalosti pojavljivanja i ozbiljnosti utjecaja kibernetičkih rizika na poslovanje organizacije izrazito složeno (Ćurak et al., 2019; Marotta et al., 2017, Eling i Wirfs, 2016; Herath i Herath, 2011), te se postavlja pitanje pouzdanosti procjene frekvencije i intenziteta.

Suočavanje s kibernetičkim rizicima postavlja donositelje odluka u organizacijama u **kontekst oskudnih informacija**. U takvim uvjetima **kognitivne pristranosti** i **emocije** dolaze do izražaja te potencijalno utječu na procjenu kibernetičkih rizika kao prijetnje kao i na donošenje odluke u vezi upravljanja kibernetičkim rizicima. Složenost i promjenjiva priroda kibernetičkih rizika suprotstavljaju se pretpostavci koju zagovara klasična ekonomska škola, a riječ je o potpunoj informiranosti kao uvjetu racionalnih odluka. Stoga, nedostatak informacija može potaknuti oslanjanje na kognitivnu pristranost kako bi se nadomjestio nedostatak razumijevanja (Tversky i Kahneman, 1974), a apstraktna priroda kibernetičkih rizika može pobuditi emocije te utjecati na odluke o upravljanju rizicima (Slovic et al., 2004).

Pri suočavanju s kompleksnim zadacima procjene rizika, koji zahtijevaju ocjenu vjerojatnosti, primjećuje se upotreba heuristika i izloženost kognitivnim pristranostima, što može dovesti do neispravnih zaključaka (Gellman i Turner, 2013). S druge strane, Pereira-Henriques i Lima (2003, u Breakwell, 2014) ističu kako je emotivna dimenzija u nepoznatim uvjetima važnija odrednica procjena i odluka, a upravo je ta činjenica u skladu s fokusom istraživanja koje se odnosi na kibernetičke rizike, a koje s obzirom na svojstva, odlikuje nepoznatost (izostanak relevantnih činjenica).

Istraživanja u području informacijske i kibernetičke sigurnosti usredotočena su na korištenje racionalnih modela odlučivanja. S obzirom da su odluke u vezi kibernetičke sigurnosti povezane s rizikom, često su narušene temeljene pretpostavke racionalnog modela odlučivanja (Young et al., 2012). Stoga, na tragu zaključka Bulgurcu et al. (2010) te Kim i Kankanhalli (2009), u ovom se istraživanju pretpostavlja da odluke u vezi kibernetičke sigurnosti nisu potpunosti racionalne te je potrebno uvažiti pretpostavku o ograničenoj racionalnosti te prisutnosti emocija.

Studija De Smidt i Botzen (2018) uočava da profesionalni donositelji odluka odstupaju od očekivane odluke transferiranja rizika na društva za osiguranje što se može opravdati teorijom očekivane korisnosti. Isti autori za nastavak istraživanja sugeriraju novi pristup i uvođenje teorija koje pripadaju bihevioralnoj ekonomiji, a koje mogu doprinijeti razumijevanju pristrano donošenju odluka u poslovnim organizacijama.

Razumijevanje uloge kognitivnih pristranosti i emocija u donošenju odluka ključno je za učinkovito upravljanje kibernetičkim rizicima. Navedeno vrijedi i u situaciji kada odluke donose glavni izvršni menadžeri, s obzirom na karakteristike kibernetičkih rizika.

Nastavno na izloženi problem istraživanja, uvažavajući ključne koncepte iz postojećih istraživanja o pristranostima i emocijama koje se pojavljuju prilikom donošenja odluka, ovim istraživanjem se u okviru teorije motivacije za zaštitom (PMT teorije) integriraju pretpostavke ograničene racionalnosti i to u smislu **uvođenja varijabli kognitivne pristranosti** *(pristranost optimizma, pristranost dostupnosti)* **i emocija** *(strah i žaljenje)* koje se primjenjuju u kontekstu kibernetičke prijetnje u poslovnim organizacijama nad populacijom ključnih izvršnih menadžera. Integriranjem pretpostavki ograničene racionalnosti uvažava se spoznaja da neracionalni čimbenici također mogu oblikovati ponašanje (Nehme et al., 2022).

Na tragu navedenog, **predmet istraživanja je utjecaj kognitivnih pristranosti na percepciju kibernetičkih rizika kao prijetnje za poslovanje organizacija i utjecaj percipirane prijetnje kibernetičkih rizika na namjeru upravljanja kibernetičkim rizicima posredstvom emocija**.

1.2. Svrha i ciljevi istraživanja

Svrha istraživanja je doprinijeti razumijevanju namjera glavnih izvršnih menadžera da ostvare zaštitu od kibernetičkih rizika odnosno da njima upravljaju u organizacijskom kontekstu pri čemu se kognitivne pristranosti i emocije integriraju unutar modela motivacije za zaštitom. U nastavku se izdvajaju ciljevi istraživanja.

Osnovni znanstveni cilj istraživanja je, u kontekstu menadžerskog odlučivanja, integrirati pretpostavke bihevioralne ekonomije unutar teorije motivacije za zaštitom, kako bi se razvio teorijski utemeljen model koji doprinosi razumijevanju namjere glavnog izvršnog menadžera u

pogledu upravljanja kibernetičkim rizicima na razini organizacije. U skladu s navedenim, **empirijski ciljevi istraživanja** su:

- Istražiti **utjecaj** *pristranosti optimizma* (*engl. Optimism bias*) i *pristranosti dostupnosti* (*engl. Recency bias*) kao oblika **kognitivnih pristranosti** na razinu **percepcije prijetnje** koju predstavljaju kibernetički rizici;
- Istražiti **ulogu emocija straha i žaljenja kao medijatora između percepcije prijetnje i namjere upravljanja** kibernetičkim rizicima;
- Istražiti **utjecaj percepcije o sposobnosti suočavanja organizacije s kibernetičkim rizicima na namjeru upravljanja kibernetičkim rizicima**.

Dodatni znanstveni ciljevi:

- Sistematizirati i kritički analizirati relevantne znanstvene spoznaje u području kibernetičkih rizika, njihovog upravljanja te bihevioralnih odrednica donošenja odluka;
- Istaknuti ograničenja provedenog istraživanja, ukazati na nova područja i potrebna buduća istraživanja.

Operacionalni cilj istraživanja obuhvaća empirijsku provjeru teorijskog modela koji integrira pretpostavke bihevioralne ekonomije u razumijevanju namjere upravljanja kibernetičkim rizicima na uzorku glavnih izvršnih menadžera koji upravljaju trgovačkim društvima na prostoru Republike Hrvatske. Temeljem rezultata istraživanja cilj je:

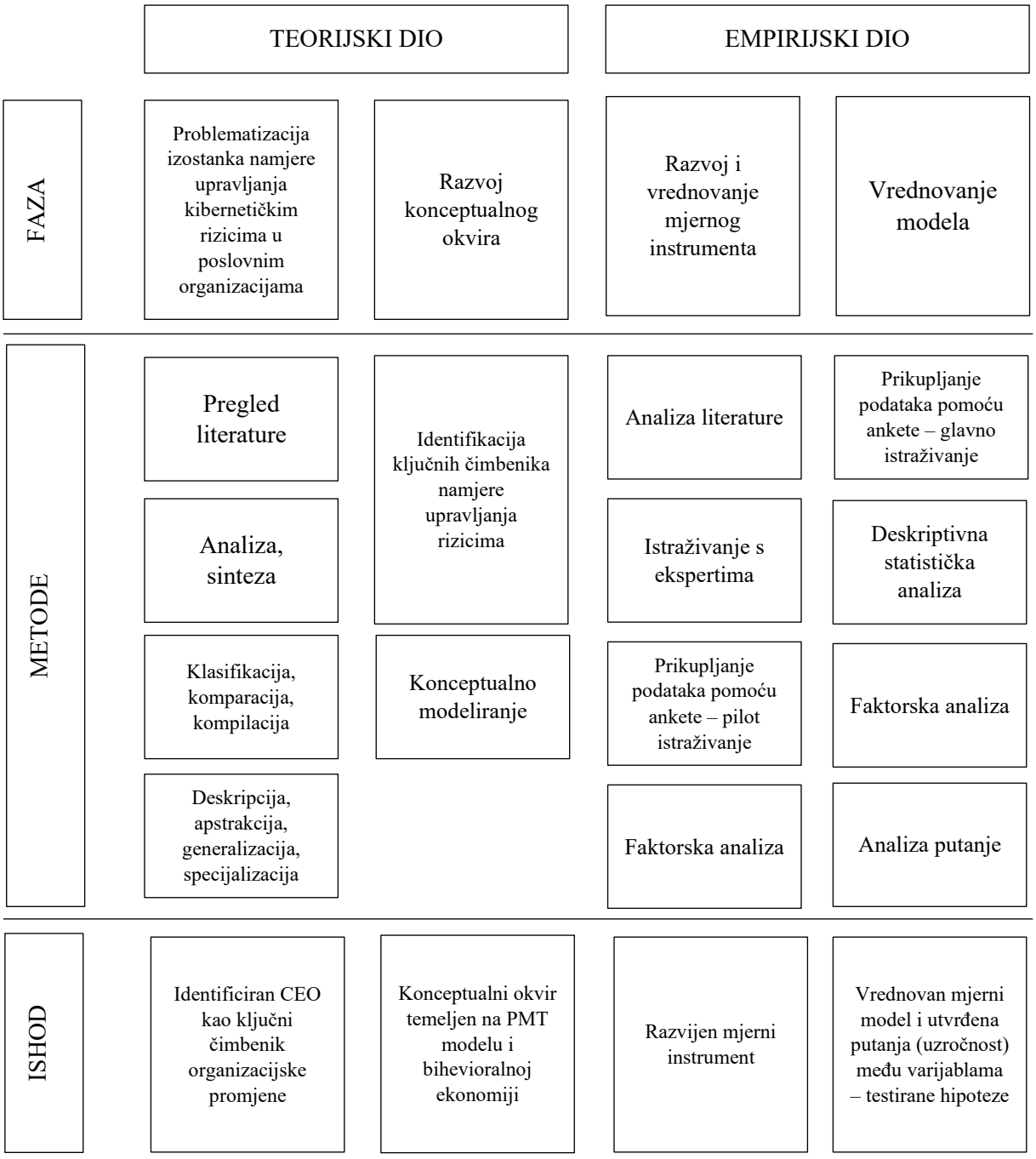
- Istaknuti ulogu koju pretpostavke bihevioralne ekonomije imaju u implementaciji procesa upravljanja kibernetičkim rizicima u organizacijama.
- Sugerirati unaprjeđenje i način implementacije procesa upravljanja kibernetičkim rizicima u organizacijama.

1.3. Metodologija istraživanja

Prilikom izrade doktorskog rada primijenjen je metodološki pristup sukladan obilježjima svakog dijela rada, pri čemu se razlikuje teorijski i empirijski segment. Sukladno svakom segmentu, primijenjena je znanstvena kvalitativna i kvantitativna metoda (*Slika 1*).

Prvi segment istraživanja obuhvaća pretragu relevantne znanstvene i stručne literature (*knjige, članci, izvještaji, propisi*) te ostalih publikacija koje su dostupne online ili putem knjižničnog

fonda te njihovo analiziranje u cilju donošenja zaključaka i osnovnog uporišta za provođenje drugog segmenta koji se odnosi na empirijsko istraživanje.



Slika 1. Nacrt istraživanja

Izvor: Izrada autora

U istraživanju se primjenjuje *metoda analize* koja pretpostavlja raščlanjivanje složenih cjelina na jednostavne dijelove, omogućavajući jasnije razumijevanje svakog dijela složene cjeline. S ciljem doprinosa kvaliteti teorijskog dijela rada, primjenjuje se *metoda sinteze* koja označava postupak povezivanja izdvojenih i manje složenih cjelina u složenije cjeline. Implementiranje

ranijih znanstvenih spoznaja bit će temeljeno na *metodi klasifikacije*, *metodi komparacije* te *metodi kompilacije*. Prilikom opisivanja procesa, pojava i činjenica koristi se *deskriptivna metoda* te *metoda apstrakcije, generalizacije* i *specijalizacije* koje doprinose razumijevanju razmatranih kategorija i njihove povezanosti. Konačno, primjenjuju se *metode indukcije* i *dedukcije* koje doprinose postizanju jasnije prosudbe u vezi problematike rada (Tkalac Verčić et al. 2010; Zelenika, 2000).

Drugi segment istraživanja obuhvaća testiranje konceptualnog modela odnosno istraživačkih pretpostavki (*hipoteza*) nad primarnim podacima temeljem **metode strukturalnog modeliranja** (*engl. Structural equation modeling – SEM*). Riječ je o multivarijatnoj metodi statističke analize utemeljenoj na faktorskoj analizi, analizi putanje te višestrukoj regresijskoj analizi (Hair et al., 2021; Sarstedt et al., 2021; Kline, 2015; Weston i Gore, 2006).

U cilju pripreme glavnog dijela istraživanja, provedeno je preliminarno istraživanje sa ekspertima što je omogućilo razvoj mjernog instrumenta te njegovo vrednovanje (sadržajna valjanost i razumljivost). Dodatno, s istom svrhom provedeno je preliminarno (pilot) istraživanje čime je testirana pouzdanost i valjanost mjernih čestica.

Podaci za potrebe istraživanja prikupljeni su putem upitnika odaslanog elektroničkim putem.

1.4. Opravdanost i znanstveni doprinos istraživanja

Pregledom literature potvrđuje se kako je relativno malo onih istraživanja koje kibernetičkim rizicima pristupaju iz ekonomske perspektive (Kovač, 2021, Ćurak, 2019; Eling, 2018; Marotta et al., 2017; Eling i Schnell, 2016). Nedovoljna istraženost područja upravljanja kibernetičkim rizicima iz ekonomske perspektive čimbenik je koji ograničava upravljanje kibernetičkim rizicima, a da je riječ o izazovu kojeg je potrebno u ozbiljnijoj mjeri razmatrati upućuju trendovi sve veće značajnosti i rasta kibernetičkih rizika.

Pregledom literature primjećuje se izostanak istraživanja problema upravljanja kibernetičkim rizicima unutar poslovnih organizacija te izostanak integracije kibernetičkih rizika unutar integriranog sustava upravljanja kibernetičkim rizicima (Ashby et al., 2018; Marotta i McShane, 2018, Price Waterhouse Coopers, 2018). U slučaju poslovnih organizacija, vidljivo je nedovoljno ulaganje u postizanje kibernetičke sigurnosti (Boehm et al., 2022; Ernst & Young, 2021; Deloitte, 2016). Najčešće je uočeno zanemarivanje kibernetičkih rizika kao prijetnje za poslovanje te nedovoljno upravljanje kibernetičkim rizicima što naglašava potrebu za

sveobuhvatnom promjenom. Nužnost promjene dodatno je naglašena dinamikom učestalosti i ozbiljnosti utjecaja kibernetičkih rizika na poslovanje (Allianz, 2023; Ponemon Institute, 2023; Deloitte, 2023; Verizon, 2022).

Slijedom navedenog, nužna je organizacijska promjena u pogledu kibernetičke sigurnosti (Gale et al., 2022). Istraživanja ukazuju kako je ulaganje isključivo u tehnička rješenja nedostatno (Nobles, 2018; Tu et al., 2018; Van Niekerk i Von Solms, 2010). Uloga čovjeka u postizanju kibernetičke sigurnosti je ključna, a nedovoljno se naglašava (Kannelønning i Katsikas, 2023; Ani et al., 2018; Biener et al., 2015), što je vidljivo u nedostatku istraživanja, u području kibernetičkih rizika, koja u fokus postavljaju čovjeka (Pollini et al., 2022; Corradini et al., 2020; Maalem Lahcen et al., 2020; Ratchford i Wang, 2019; Nobles, 2018; Alohali et al., 2017). Navedeno ukazuje na potrebu za holističkim pristupom koji, pored tehničkih rješenja, uključuje ljudski faktor u postizanju kibernetičke sigurnosti (Almansoori et al., 2023; Pretorius i Blaauw, 2022.).

Nužno je da organizacijska promjena pristupa upravljanju kibernetičkim rizicima nužno nastupa od vodstva organizacije (Arbanas, 2021; Soomro et al., 2016). Razumijevanje uloge vodstva organizacije u pokretanju promjena ključno je za učinkovito upravljanje kibernetičkim rizicima (Ahmed Shaikh i Siponen, 2023; Høiland, 2023; Soomro et al., 2016). Naime, stavovi, percepcije i odluke vodstva organizacije značajno utječu na kibernetičku sigurnost organizacije. S obzirom na nedostatak istraživanja o ulozi organizacijskog vodstva u kontekstu kibernetičke sigurnosti (Sharifi, 2023; Triplett et al., 2022; Hakami i Alshaikh 2022; Guhr et al., 2018), potrebno je fokusirati se na najviše izvršne menadžere.

Teorija motivacije za zaštitom sugerira da donošenje odluka u kontekstu upravljanja kibernetičkim rizicima uključuje procjenu prijetnje koju kibernetički rizici predstavljaju te procjenu sposobnosti suočavanja s prijetnjom. Stoga, smatra se opravdanim primijeniti PMT teoriju u propitivanju namjere glavnih izvršnih menadžera u pogledu upravljanja kibernetičkim rizicima s kojima se suočava poslovna organizacija. U prilog tome govori činjenica da je PMT teorija primjerena u istraživanju donošenja odluka u poslovnim organizacijama (Bode et al., 2022), a Connelly i Shi (2022) predlažu je za buduća istraživanja u kontekstu menadžerskog odlučivanja.

U dosadašnjim empirijskim istraživanjima izostaje konzistentnost rezultata utjecaja percepcije prijetnje na namjeru upravljanja kibernetičkim rizicima (Cram et al., 2019; Sommestad et al., 2014). Dodatno, temeljem pregleda recentne literature u okviru predstavljenog istraživanja,

potvrđuje se kako za razliku od percepcije sposobnosti suočavanja, u slučaju percepcije prijetnje izostaje jasna potvrda percepcije prijetnje koja bi utjecala na namjeru provođenja adaptivnog odgovora (upravljanje kibernetičkim rizicima). Rezultati sugeriraju da trenutni model ne obuhvaća u potpunosti složenost utjecaja percepcije prijetnje na namjeru upravljanja kibernetičkim rizicima, što rezultira nedostatkom sveobuhvatnog razumijevanja utjecaja percepcije prijetnje na namjeru upravljanja kibernetičkim rizicima.

Jedinstvene karakteristike kibernetičkih rizika, posebice njihova složenost i recentnost (Ćurak, 2019., Eling i Wirfs, 2016; Biener et al., 2016.), sugeriraju da donositelji odluka, u kontekstu istraživanja glavni izvršni menadžeri, mogu biti pod utjecajem kognitivnih pristranosti i emocija u procesu donošenja odluka. Navedeno je podržano postojećim istraživanjima. Naime, menadžeri pokazuju kognitivne pristranosti pri donošenju odluka (Kahneman et al., 2019; Powell et al., 2011; Hodgkinson i Clarke, 2007; Malmendier i Tate, 2005; Hammond et al., 1998; Samuelson i Zeckhauser, 1988; Kahneman et al., 1982; Schwenk, 1984), ali i emocije za koje je potvrđeno da imaju utjecaj na proces i ishode organizacijskog upravljanja (Brundin et al., 2022; Brundin i Liu, 2015). S obzirom na jedinstvene karakteristike kibernetičkih rizika, razmatranje utjecaja kognitivnih pristranosti i emocija na donositelje odluka zahtijeva daljnje istraživanje.

Slijedom navedenog, kako bi se postigao napredak u razumijevanju odluka u vezi upravljanja kibernetičkim rizicima, brojni autori (Kadena i Gupi, 2021; Patterson i Winston-Proctor, 2019; Hadlington, 2018; Biener et al., 2015; Chaudhry et al., 2012) zagovaraju uvažavanje psihologije te potrebu za interdisciplinarnim pristupom koji uvažava spoznaje iz područja bihevioralne ekonomije. Uključivanje kognitivnih pristranosti i emocija u PMT model predstavlja odmak od dosadašnjeg pristupa istraživanju tako što, temeljem spoznaja iz područja bihevioralne ekonomije, pruža objašnjenje utjecaja percepcije prijetnje na namjeru upravljanja kibernetičkim rizicima. Integracija spoznaja iz bihevioralne ekonomije i PMT-a nudi potencijalno objašnjenje za izostanak očekivane empirijske potvrde utjecaja procjene prijetnje na namjeru upravljanja kibernetičkim rizicima. Istraživanje sugerira da bihevioralni čimbenici igraju značajniju ulogu nego što se dosad smatralo.

Stoga se predloženim istraživanjem nastoji utvrditi na koji način percepcija o prijetnji i percepcija o sposobnosti suočavanja s prijetnjom te kognitivne pristranosti i emocije utječu na namjeru upravljanja kibernetičkim rizicima, poštujući dosad usvojene spoznaje i teorijske koncepte koji su potvrđeni u znanstvenim istraživanjima.

Doprinos se može razmotriti kroz sljedeće segmente:

- Prethodne studije u području kibernetičkih rizika koje koriste teoriju motivacije za zaštitom prepoznaju vrijednost teorije, ali također ukazuju na važnost proširenja izvornog modela koje bi poboljšalo razumijevanje namjera donositelja odluka (De Kimpe et al., 2021). Connelly i Shi (2022) i Haag et al. (2021) ističu važnost uvođenja osobnih varijabli. Stoga se u ovom istraživanju predlaže uvođenje varijabli iz skupine kognitivnih pristranosti i emocija. U cilju kvalitetnijeg uvida i potpunijeg razumijevanja odluka u vezi upravljanja kibernetičkim rizicima, osnovni PMT model se proširuje za varijable koje se odnose na obilježja donositelja odluka, a riječ je odabranim varijablama kognitivne pristranosti (*pristranost optimizma, pristranost dostupnosti*) i emocije (*strah i žaljenje*). Naime, navedene varijable nastavak su na istraživanje De Kimpe et al. (2021) koje ističe važnost uključivanja varijabli koje ukazuju na novu dimenziju koja osigurava uvažavanje činjenice da pojedinci ne donose savršeno racionalne odluke. Time se PMT model ne promatra isključivo kao opis kognitivnog procesa donošenja odluka.
- Primijenjena je teorija PMT u menadžerskom kontekstu u pogledu upravljanja kibernetičkim rizicima. Naime, Hoskisson et al. (2017) ističu kako je literatura o menadžerskom odlučivanju u uvjetima rizika odnosno neizvjesnosti oskudna, što pruža prostor za doprinos razumijevanju odluka menadžera u uvjetima rizika odnosno neizvjesnosti. Potonje se dodatno specificira isticanjem aktivnosti menadžera, tj. odlučivanja u vezi upravljanja kibernetičkim rizicima. Stoga se kao doprinos istraživanja ističe provođenje istraživanja na uzorku koji uključuje donositelje odluka u organizacijama, što je ranije zapostavljeno prilikom empirijskog testiranja. Navedeno uključuje pojedince koji preuzimaju ključnu odgovornost za uspostavu procesa upravljanja rizicima te kao izvršni menadžeri grade politiku i kulturu upravljanja rizicima u organizacijama. Na taj se način fokus istraživanja izdvaja iz heterogene kategorije *zaposlenici* (uključuje zaposlenike različitih hijerarhijskih razina u organizaciji), koji su u pravilu u dosadašnjim istraživanjima bili razmatrani kao individue koje ne postavljaju proces i ne upravljaju aktivnostima koje se odnose na s rizike, već u ulozi pojedinci-korisnici čije se ponašanje promatra u kontekstu usklađenosti s postavljenim politikama sigurnosti. Uzimajući u obzir važnost razumijevanja čimbenika menadžerske odluke, Connely i Shi (2022) naglašavaju važnost teorije motivacije za zaštitom. Sukladno Barlette et al. (2015), aktivnost izvršnog menadžera najvažniji je faktor u postizanju zaštite informacijskog sustava organizacije. Ponašanje izvršnog menadžera utječe na zaposlenike

te im omogućava snažan utjecaj na kibernetičku sigurnost organizacije (Barlette, 2015; Knapp et al., 2006). Opravdanost usmjerenja na menadžera pronalazi se u Arbanas (2021) koji navodi kako zaštita informacija temeljena na tehničkim mjerama zaštite više nije dovoljna, a informacijska sigurnost više ne predstavlja samo tehnički već i upravljački problem. Usmjeravanjem na populaciju menadžera postiže se korist istraživanja u vidu većeg stupnja identifikacije menadžera s organizacijom u odnosu na zaposlenike koji preuzimaju manji stupanj odgovornosti i koji su u manjoj mjeri izloženi rizicima poslovne organizacije od glavnih izvršnih menadžera. Naime, prema Menard et al. (2017), ukoliko je određena prijetnja izravno povezana s donositeljem odluke (zdravlje ili financijska korist) tada isti prijetnju doživljava kao više relevantnu. U istraživanju namjere upravljanja kibernetičkim rizicima s kojima se suočava organizacija dovodi se u pitanje relevantnost utjecaja *percepcije kibernetičkih rizika kao prijetnje* na *namjeru* i *stvarno upravljanje kibernetičkim rizicima*. Naime, uočene su nedosljednosti u rezultatima ranijih istraživanja pri čemu izostaje potvrda važnosti uloge percepcije prijetnje. Kao razlog nedosljednih rezultata, može se istaknuti uzorak istraživanja pri čemu je primarni fokus bio na nemenadžerskim ulogama unutar organizacije. Iako je moguće istaknuti kako je prethodno istraživanje, Barlette et al. (2015), uključilo glavne izvršne menadžere, važno je istaknuti bitne razlike u teorijskom okviru. Naime, prethodno istraživanje bilo je ograničeno osnovnim modelom teorije motivacije za zaštitom, bez uključivanja aspekata bihevioralne ekonomije poput kognitivnih pristranosti i emocija.

- Doprinos se ogleda u sveobuhvatnosti zavisne varijable koja sadržava ključne elemente procesa upravljanja kibernetičkim rizicima. Uključeni su aspekti poput ulaganja resursa, nadogradnje politika i pravila, primjene suvremenih standarda upravljanja kibernetičkim rizicima, razvoja sveobuhvatnog plana upravljanja identificiranim kibernetičkim rizicima, kao i jačanje svijesti zaposlenika o kibernetičkim rizicima te kako oni mogu doprinijeti promicanju sigurnosti organizacije. Svi ti elementi prepoznaju se kao neizostavni dijelovi sveobuhvatnog pristupa upravljanja rizicima, pri čemu su isti pažljivo prilagođeni proučavanoj populaciji glavnih izvršnih menadžera. Iako je moguće istaknuti kako je prethodno istraživanje, Barlette et al. (2015), također razmatralo namjeru upravljanja kibernetičkim rizicima kao zavisnu varijablu, istraživanje koje se provodi u nastavku pruža sveobuhvatniji uvid u upravljanje kibernetičkim rizicima kao dijela poslovnog procesa. U odnosu na prethodne pristupe, zavisna varijabla u predstavljenom istraživanju donosi napredniju konceptualizaciju koja upravljanje kibernetičkim rizicima razmatra kao

kompleksan proces te se ne zadržava isključivo na komponenti postavljanja sigurnosnih mjera.

Proučavanjem percepcije prijetnje i suočavanja te kognitivnih pristranosti i emocija u vezi rizika/prijetnje kod ključnih ljudi za uspostavu procesa upravljanja rizicima, ovo istraživanje doprinosi proširenju spoznaja o odlučivanju u uvjetima neizvjesnosti kada se očekuju odstupanja od savršeno racionalne odluke. Kognitivni proces predviđen teorijom PMT nadograđuje se za pristranosti i emocije te se smatra nužnom prilagodbom na kontekst u kojem se donositelj odluke nalazi (stanje neizvjesnosti i nedostupne potpune informacije) kao i nužnom nadogradnjom za razumijevanje razvoja prakse upravljanja rizicima.

Očekivani doprinos ovog istraživanja nalazi se u dubljem razumijevanju uloge menadžera kao pojedinca koji nije savršeno racionalan u kontekstu odlučivanja o kibernetičkim rizicima. S obzirom na složenost i specifičnost kibernetičkih rizika, ovo istraživanje osvjetljava izazove s kojima se menadžeri suočavaju pri donošenju odluka u području upravljanja kibernetičkim rizicima. Istraživanje ističe važnost bihevioralnih faktora u menadžerskim odlukama, pri čemu ukazuje na značajne implikacije kognitivnih pristranosti i emocija. Unatoč često povezanim pretpostavkama o njihovom potencijalnom negativnom utjecaju, one ne moraju nužno štetiti organizaciji, što otvara nove perspektive za razumijevanje menadžerskog odlučivanja u kontekstu kibernetičke sigurnosti. U konačnici, rezultati ovog istraživanja pružit će vrijedan izvor informacija za daljnja istraživanja, kao i za praktičnu primjenu u menadžerskim praksama vezanim uz kibernetičku sigurnost organizacija i javnim politikama.

1.5. Struktura rada

Uvodni dio pruža uvid u *područje i problem* istraživanja, *ciljeve istraživanja*, *korištenu metodologiju* te *znanstveni doprinos istraživanja*. Istim se nastoji pružiti pregled o važnosti upravljanja kibernetičkim rizicima u organizaciji, trenutnoj razini upravljanja kibernetičkim rizicima te važnosti glavnog izvršnog menadžera u postizanju organizacijske promjene kakvu zahtijeva poslovno okružje.

Drugo poglavlje usmjereno je na teorijsko definiranje kibernetičkih rizika, njihova obilježja i važnost, pri čemu se razmatra njihova implikacija na poslovanje organizacija. Pruža se uvid u zakonodavni okvir u vezi upravljanja kibernetičkim rizicima koji doprinosi razvoju procesa upravljanja kibernetičkim rizicima u poslovnim organizacijama. Razmatra se upravljanje

kibernetičkim rizicima u poslovnim organizacijama, pri čemu se opisuje integrirani pristup upravljanju rizicima (ERM). Iznose se organizacijski izazovi u upravljanju kibernetičkim rizicima, a u kontekstu njihovih karakteristika, pruža se uvid u bihevioralnu perspektivu te implikacije organizacijskih izazova u vezi procjena, odluka, namjera i ponašanja ključnih sudionika unutar organizacije.

Treće poglavlje pruža uvid u teorijsko uporište razvoja modela namjere upravljanja kibernetičkim rizicima, pri čemu se opisuju najvažnije teorije odlučivanja u kontekstu kibernetičkih rizika te izdvaja teorija motivacije za zaštitom (*engl. Protection motivation theory – PMT*) kao odabrano teorijsko uporište. Opisana je perspektiva bihevioralne ekonomije kao nadogradnja predstavljenih modela odlučivanja te se u tom smislu u ovom dijelu analiziraju kognitivne pristranosti i emocije koje utječu na namjere i odluke u vezi upravljanja kibernetičkim rizicima.

Četvrto poglavlje pruža detaljan uvid u predložen model namjere upravljanja kibernetičkim rizicima (teorija motivacije za zaštitom) u kojem se identificiraju čimbenici koji utječu na namjeru upravljanja kibernetičkim rizicima te pruža pregled rezultata ranijih istraživanja koji primjenjuju PMT model. U okviru ovog poglavlja detaljno se obrazlažu hipoteze istraživanja. Uvažavajući pretpostavke bihevioralne ekonomije, odnosno utjecaj kognitivnih pristranosti i emocija na oblikovanje namjere, kroz pregled konceptualnog modela daje se uvid u pretpostavljene veze između identificiranih čimbenika utjecaja na namjeru upravljanja kibernetičkim rizicima.

Peto poglavlje prezentira provedeno empirijsko istraživanje. Opisuje se metodološki okvir istraživanja, korištena metoda, populacija i uzorak istraživanja te korišteni instrument za prikupljanje podataka, nakon čega su prikazani rezultati analize mjernog modela i analize strukturnog modela za model prve i druge razine.

Konačno, **šesto poglavlje** donosi zaključna razmatranja na temelju provedenog pregleda istraživanja te rezultata empirijskog istraživanja. Raspravlja se o glavnim nalazima i važnosti istraživanja za razumijevanje namjera u vezi upravljanja kibernetičkim rizicima. Pruža se uvid u ograničenja istraživanja te iznose preporuke za buduća istraživanja. Konačno, iznosi se aplikativan doprinos istraživanja.

Na kraju istraživanja prezentira se *popis literature*, *popis kratica i oznaka*, *popis tablica slika i grafikona*, *prilozi* te *životopis autora*.

2. KIBERNETIČKI RIZICI I UPRAVLJANJE KIBERNETIČKIM RIZICIMA U POSLOVNIM ORGANIZACIJAMA

U ovome poglavlju pojašnjava se kategorija kibernetičkih rizika kao prijetnje za poslovanje organizacija. Opisuju se obilježja kibernetičkih rizika te njihov utjecaj na poslovanje organizacija. Pruža se uvid u zakonodavni okvir Europske unije i Republike Hrvatske u vezi kibernetičkih rizika i njihovog upravljanja. Raspravlja se o upravljanju kibernetičkim rizicima te integraciji istog u proces upravljanja poslovnim rizicima. Istaknuti su izazovi s kojima se organizacije suočavaju u implementaciji procesa upravljanja kibernetičkim rizicima, pri čemu se izdvaja ključna uloga čovjeka, a posebno uloga vodstva organizacije, u postizanju kibernetičke sigurnosti.

2.1. Kibernetički rizici

Zamjetni su različiti pristupi definiranju pojma kibernetički rizici, a jedinstvena definicija kibernetičkih rizika nije usvojena. Kibernetički rizici su interdisciplinarna kategorija, pri čemu se izdvajaju tehnička i ekonomska dimenzija (Böhme et al., 2019), zbog čega se mogu opravdati različiti pristupi u definiranju (vidjeti Tablicu 1). Složenost i kompleksnost su ključna svojstva zbog kojih izostaje jedinstvena i široko prihvaćena definicija (Zängerle i Schiereck, 2023; Strupczewski, 2021). Doprinos u razvijanju definicije kibernetičkih rizika, pored znanstvene zajednice, postoji i kod strukovnih tijela.

Tablica 1. Pregled definicija kibernetičkih rizika

Definicija	Izvor
Kibernetički rizik je rizik povezan s internetom.	Gordon et al. (2003)
Kršenje integriteta i kvar informacijsko-komunikacijske infrastrukture (ICT infrastrukture).	Böhme i Kataria (2006)
Kompromitacija triju osnovnih principa: povjerljivosti, cjelovitosti i dostupnosti podataka ili sustava, odražava negativne utjecaje na operativne aspekte organizacije (misiju, funkcije, javnu percepciju i ugled), imovinu, pojedince, druge organizacije te ima nepovoljan utjecaj na nacionalnoj razini.	National Institute of Standards and Technology (2006); International Organization for Standardization. (2009)

Definicija	Izvor
Operativni rizici informacijske i tehnološke imovine koji imaju posljedice na povjerljivost, cjelovitost i dostupnost informacija ili informacijskih sustava.	Cebula i Young (2010)
Rizici od financijskih, reputacijskih i tržišnih gubitaka u vezi s korištenjem ICT tehnologije.	Ögüt et al. (2011)
Kombinacija vjerojatnosti događaja u području umreženih informacijskih sustava i posljedica ovog događaja na imovinu i reputaciju pojedinca i organizacije.	World Economic Forum (2012)
Rizik povezan sa zlonamjernim elektroničkim događajima koji uzrokuju prekid poslovanja i financijski gubitak.	Mukhopadhyay et al. (2013)
Rizici povezani s aktivnostima na umreženim sustavima, internetskom trgovinom, elektroničkim sustavima i tehnološkim mrežama te pohranom osobnih podataka.	Willis (2013)
Rizici od financijskog gubitka, poremećaja u poslovanju ili štete ugledu organizacije zbog kvara ICT sustava. Realiziraju se zbog lošeg integriteta sustava, nenamjerne povrede sigurnosti te namjerne i neovlaštene povrede sigurnosti s ciljem pristupa ICT sustavima u svrhu špijunaže, iznude ili nanošenje štete ugledu.	Institute of Risk Management (2014)
Operativni rizici povezani s informacijama i tehnološkom imovinom koji imaju potencijalno negativan utjecaj na povjerljivost, cjelovitost i dostupnost informacija i informacijskih sustava.	Biener et al. (2015)
Prijetnja su pojedincu i organizacijama, a predstavljaju potencijalnu materijalnu štetu ili propuštene zarade zbog kvara digitalnih sustava ili oštećenih podataka.	Nieuwesteeg et al. (2015)
Uzrokovani su kibernetičkom prijetnjom koja se pojavljuje u kibernetičkom prostoru.	Refsdal et al. (2015)
Rizici poslovanja unutar kibernetičkog prostora. Obuhvaćaju: - sve vrste rizika koji nastupaju korištenjem i prijenosom elektroničkih podataka uključujući tehnologiju (primjerice internet, telekomunikacijska mreža) - materijalna šteta koja je uzrokovana kibernetičkim napadom - prijevara koja je rezultat zloupotrebe podataka - odgovornost koja proizlazi iz upotrebe, pohrane i prijenosa podataka - odgovornost koja proizlazi iz povjerljivosti, cjelovitosti i dostupnosti elektroničkih informacija bez obzira odnosi li se na pojedinca, organizaciju ili vladu (javno tijelo).	CRO Forum (2016)

Definicija	Izvor
Proizlaze iz upotrebe ICT-a, a koji ugrožavaju povjerljivost, cjelovitost i dostupnost podataka ili usluga. Dovode do prekida poslovanja, kvara (kritične) infrastrukture i materijalne štete za ljude i organizacije. Kibernetički rizici rezultat su djelovanja prirodnih sila ili čovjeka, a djelovanje čovjeka može proizaći iz ljudske pogreške, kibernetičkog kriminala, kibernetičkog rata ili terorizma.	Eling i Schnell (2016)
Imaju digitalni uzrok oštećenja digitalne imovine, digitalni uzrok oštećenja materijalne imovine ili materijalni uzrok oštećenja digitalne imovine.	Böhme et al. (2018)
Obuhvaćaju sve rizike povezane s online aktivnostima, poput pohrane osobnih podataka na internetu ili provođenje online transakcija koje mogu rezultirati povredom ugleda, financijskim gubitkom i poremećajem poslovanja.	National Association of Insurance Commissioners - (2018)
Operativni rizik povezan s aktivnostima unutar kibernetičkog prostora koji prijeti informacijskoj imovini, ICT infrastrukturi i tehnološkoj imovini te može uzrokovati štetu materijalne i nematerijalne imovine organizacije, prekid poslovanja ili štetu ugledu. Uključuje materijalnu štetu na ICT infrastrukturi.	Strupczewski (2021)
Odnose se na kombinaciju vjerojatnosti pojavljivanja kibernetičkih incidenata i njihovog utjecaja. Kibernetički incident označava svaku vidljivu pojavu u informacijskom sustavu koja: - ugrožava kibernetičku sigurnost informacijskog sustava ili informacija koje sustav obrađuje, pohranjuje ili prenosi, - ili krši sigurnosna pravila, sigurnosne procedure ili prihvatljiva pravila korištenja, bilo da je rezultat nenamjerne ili zlonamjerne aktivnosti.	Doerr et al. (2022); Financial Stability Board (2023)

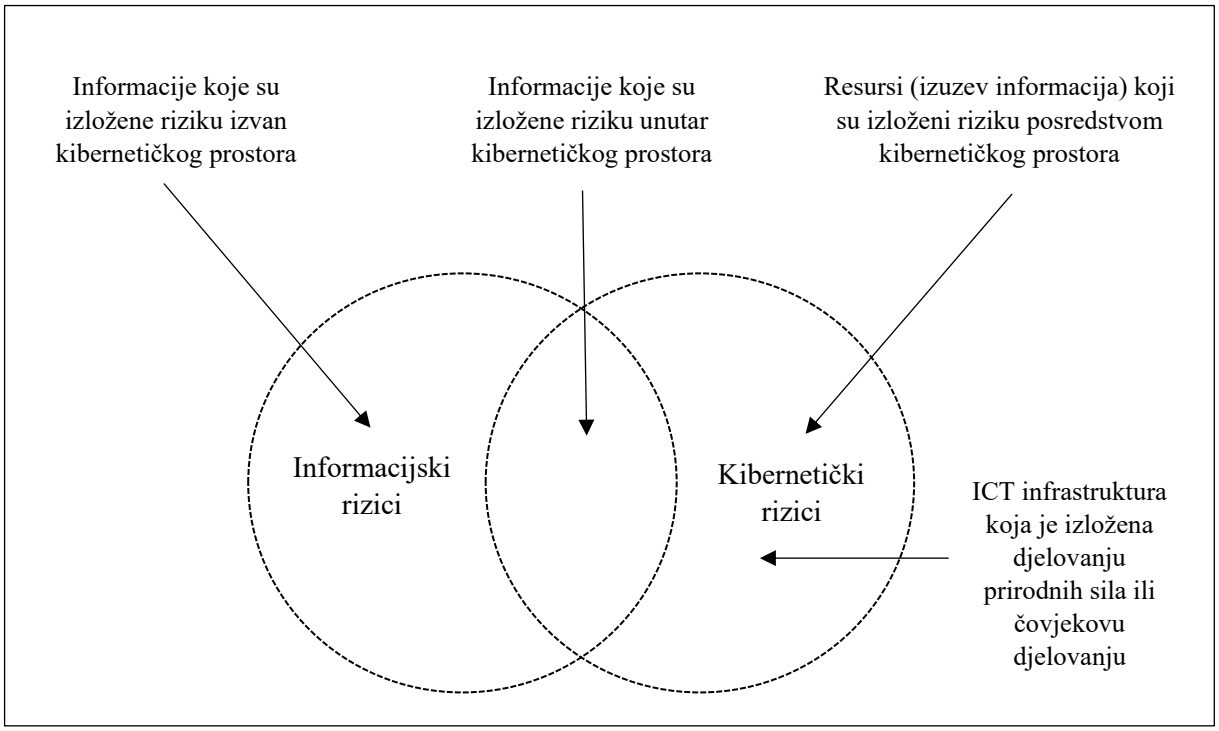
Izvor: Izrada autora

Dominantno prihvaćena definicija kibernetičkih rizika jest: *Kibernetički rizici jesu operativni rizici koji su povezani s informacijskom i tehnološkom imovinom koji imaju učinak na pouzdanost, cjelovitost i dostupnost informacija i informacijskih sustava*.[10] Međutim, uočava se da je definicija kibernetičkih rizika tijekom vremena razvijana, a u procesu razvoja izdvajaju se tri ključne dimenzije u definiranju kibernetičkih rizika, riječ je o *izvoru*, *objektu* te *utjecaju*

[10] **Povjerljivost** označava da je informacija zaštićena od neovlaštenog pristupa; **Cjelovitost** (*integritet*) označava da je informacija točna, potpuna i zaštićena od neovlaštene izmjene; **Dostupnost** označava da su informacije pravovremeno dostupne ovlaštenim korisnicima (ISO/IEC 27000:2018; Peters et al., 2018).

rizika (Strupczewski, 2021). Definicije koje se smatraju sveobuhvatnima razmatraju sve tri dimenzije koje su obuhvaćene i kod Strupczewski (2021) i Eling i Schnell (2016).

Naizmjenična upotreba termina *informacijski rizik* te *kibernetički rizik* česta je pojava u literaturi (Arbanas 2021; Von Solms i Van Niekerk, 2013; Öğüt et al., 2011). Wrede et al. (2019) razmatraju kibernetičke rizike kao podskup informacijskih rizika koji se odnose na rizike povezane s informacijama u digitalnom obliku i sustavima koji služe za njegovu pohranu i prijenos (Wrede et al., 2019). Iako su oba koncepta povezana s informacijama i tehnologijom te podrazumijevaju kršenje povjerljivosti, integriteta ili dostupnosti informacija, imaju različite opsege i fokuse (*Slika 2*). Informacijski rizici odnose se na rizike povezane sa svim vrstama informacija, bilo da je riječ o digitalnim ili nedigitalnim informacijama, kao što su, primjerice, informacije podijeljene u izravnoj komunikaciji ili putem tiskanog materijala (*vidljivo kako ne mora biti zastupljena informacijska i komunikacijska tehnologija*).



Slika 2. Odnos informacijskih i kibernetičkih rizika

Izvor: Izrada autora[11]

[11] Prema Von Solms i Van Niekerk (2013), dio koji razlikuje informacijsku i kibernetičku sigurnost u razmatranju rizika, jest činjenica da se u okviru informacijske sigurnosti razmatra informacijska imovina koja se pohranjuje ili prenosi bez ICT-a. S druge strane, u okviru kibernetičke sigurnosti razmatra se neinformacijska imovina koja je osjetljiva na prijetnje putem ICT-a.

Strupczewski (2021), ISO/IEC TS 27100:2020 (2020), Refsdal et al. (2015), CRO Forum (2016) u definiranju kibernetičkih rizika posebice izdvajaju kibernetički prostor (*engl. Cyberspace*) koji označava međusobno povezano digitalno okruženje *mreža*, *usluga*, *sustava*, *pojedinaca*, *procesa*, *organizacija*.[12] Biener et al. (2015) i Schmitt (2013) definiraju kibernetički prostor kao interaktivnu domenu sastavljenu od digitalnih mreža koje se koriste za pohranu i izmjenu informacija te komunikaciju. National Institute of Standards and Technology (2023) i Hogan i Newton (2015) navode kako kibernetički prostor predstavlja globalnu domenu unutar informacijskog okruženja sastavljenu od međuovisne mreže informacijskih sustava i informacijske infrastrukture, što primarno uključuje *internet*, *telekomunikacijske mreže* i *računalne sustave*. Prema Williams (2014), kibernetički prostor predstavlja informacijsko okruženje koje je rezultat povezivanja računalnih sustava s pripadajućom telekomunikacijskom opremom i drugim komponentama koje omogućuju brzi prijenos velike količine podataka.

Razmatrajući ranije opisan proces u kojem poslovne organizacije bilježe sve istaknutiju ovisnost poslovnih procesa o tehnološkim rješenjima te postizanje više razine digitalne zrelosti, informacijski i kibernetički rizici imaju sve izraženiju površinu presjeka (*Slika 2*) što sugerira kako termini postaju sve usklađeniji. U nastojanju da se razgraniče pojmovi informacijskih i kibernetičkih rizika, razmatrane su dvije dimenzije; objekt koji je izložen kibernetičkom riziku te kategorija prijetnje, pri čemu se u potonjoj dimenziji razlikuju informacijski i kibernetički rizici te je li prijetnja proizlazi izvan ili unutar kibernetičkog prostora.

Tablica 2. Razgraničenje pojma informacijski rizici i kibernetički rizici

	Kategorija prijetnje			
	Informacijski rizici		**Kibernetički rizici**	
Objekt koji je izložen rizicima	*Prijetnja unutar kibernetičkog prostora*	*Prijetnja izvan kibernetičkog prostora*	*Prijetnja unutar kibernetičkog prostora*	*Prijetnja izvan kibernetičkog prostora*
Materijalna imovina	(✓)	(✓)	✓	✓
Nematerijalna imovina	✓	✓	✓	/

Napomena: ✓- "primjenjuje se"; (✓) – „djelomično se primjenjuje“; / - “ne primjenjuje se”

Izvor: Izrada autora prema Zängerle i Schiereck (2023).

[12] Internet predstavlja najprepoznatljiviju mrežu unutar kibernetičkog prostora.

Temeljem *Tablice 2* pruža se jasniji uvid u složenost razgraničenja pojma između informacijskih i kibernetičkih rizika, a za detaljniju analizu razgraničenja sugestija je konzultirati istraživanje Zängerle i Schiereck (2023).

Na osnovu provedene analize, a za potrebe predstavljenog istraživanja, primijenjena je sljedeća definicija kibernetičkih rizika; *kibernetički rizici* predstavljaju **prijetnju** koja ugrožava *povjerljivost, cjelovitost* i *dostupnost* **informacija** koje se pohranjuju i prenose u digitalnom obliku, i **informacijsko-komunikacijskih sustava** koji su sredstvo pohrane i prijenosa. Kibernetički rizici **mogu biti uzrokovani faktorima:** *izvan organizacije* (uključuju hakerske napade i ucjene, utjecaj prirodnih sila) te *unutar organizacije* (uključuju zlonamjerno djelovanje, nemarnost ili slučajne propuste zaposlenika).

2.1.1. Obilježja kibernetičkih rizika

Kibernetički rizik određen je tehnologijom, a s obzirom na **neprekidan proces razvoja** tehnologije, kibernetički rizici pokazuju **evolucijsku prirodu**. Međutim, **ljudski faktor** ključni je **pokretač** kibernetičkih rizika (Boehm et al., 2022, Vrhovec i Mihelič, 2021; Siponen et al., 2014) koji doprinosi **kompleksnosti** proučavanoga koncepta. Ćurak (2019) izdvaja **obilježje promjenjivosti** kao rezultat napretka u informacijskoj tehnologiji te promjenjive prirode kibernetičkog kriminala. Imajući na umu **intenzivnu dinamiku** kibernetičkih rizika, **pouzdanost povijesnih podataka** u predviđanju budućih šteta dolazi u pitanje (Eling i Wirfs, 2016; Biener et al., 2016).

Nadalje, kada je riječ o kibernetičkim rizicima, neizostavno je osvrnuti se na **opsežnost utjecaja** i **lakoću širenja** kibernetičkih rizika. Međusobna povezanost elemenata unutar kibernetičkog prostora je okružje u kojem kibernetički incident unutar jedne poslovne organizacije može potencijalno utjecati na druge poslovne organizacije, što dovodi do domino efekta sigurnosnih incidenata (Aslam et al., 2022; Biener et al., 2015; Hofmann i Ramaj, 2011; Heal et al., 2006).[13]

Specifičnost kibernetičkih rizika očituje se kroz dimenzije *lokacije*, *utjecaja* i *vidljivosti* (Gordon et al., 2003). Kibernetički rizici su **sveprisutni**, a **geografske granice postaju manje**

[13] Primjerice, crv "*WannaCry*", vrsta zlonamjernog softvera, može zaraziti milijune računala širom svijeta u manje od 24 sata. Slično tome, jedna ranjivost u naširoko korištenom softveru, poput Windowsa, može potencijalno utjecati na milijune korisnika.

značajne (Wang i Kim, 2009). Kibernetičke prijetnje mogu biti inicirane s bilo koje lokacije u svijetu koja osigurava osnovnu infrastrukturu i pristup kibernetičkom prostoru, a mogu ciljati bilo koji povezani element sustava unutar kibernetičkog prostora. **Financijske posljedice** štete uzrokovane kibernetičkim incidentom mogu nadmašiti vrijednosti direktno povezane s podacima ili ICT infrastrukturom budući da mogu obuhvatiti i dodatne troškove vezane uz odgovornost i reputacijsku štetu (Ćurak, 2019). Kibernetički incidenti uglavnom generiraju nematerijalne gubitke, dok su materijalne štete (*primjerice štete na ICT infrastrukturi*) manje izražene.

Biener et al. (2015) naglašavaju **nedostatak podataka**, ali i **asimetriju informacija** o kibernetičkim incidentima, te izdvajaju kako je riječ o ključnom elementu za poticanje poboljšanja kibernetičke otpornosti. Dodatno, kibernetičkim rizicima pridaje se **obilježje jedinstvenosti**, ne samo na razini industrije, već i **na razini pojedinog poduzeća**. Posljedica je **otežana osigurljivost,** odnosno zahtjevno ugovaranje transfera rizika na društva za osiguranje (Aldasoro et al., 2022; Ćurak, 2019). Analizirajući obilježja kibernetičkih rizika s obzirom na učestalost pojavljivanja i intenzitet utjecaja, Eling i Wirfs (2016) ističu kako su istodobno prisutni rizici koji bilježe **visoku učestalost pojavljivanja i slab intenzitet** utjecaja te obrnuto. Eling i Schnell (2016) navode kako kibernetičke rizike karakterizira visok stupanj **međuovisnosti** kibernetičkih gubitaka, potencijalno ekstremni događaji, nedostupnost podataka i otežano modeliranje rizika.

U pogledu **odredivosti događaja** s aspekta vremena njegova nastanka, mjesta i uzroka, postoje određena ograničenja.[14] ENISA (2012) ističe kako je moguće odrediti vrijeme pojave događaja povezanih s kibernetičkim rizicima, no zbog specifičnosti kibernetičkih rizika, može se naići na poteškoće pri utvrđivanju lokacije i uzroka.

Zaključuje se kako je riječ o složenom fenomenu s potencijalno ozbiljnim posljedicama za poslovanje organizacija. Složenost kibernetičkih rizika proizlazi iz nekoliko dimenzija, uključujući evolucijsku prirodu tehnologije, postupanje pojedinca, sveprisutnost kibernetičkih rizika i međusobnu povezanost elemenata unutar kibernetičkog prostora. Nadalje, financijske i reputacijske implikacije mogu daleko nadmašiti izravne troškove povezane s podacima ili štetom na ICT infrastrukturi.

[14] Težnja počinitelja kibernetičkog incidenta je zaštiti vlastitu anonimnost, što otežava identifikaciju počinitelja. „*Stuxnet*“ iz 2010. godine, koji je prouzročio značajnu štetu iranskom nuklearnom programu, zloglasan je primjer sofisticiranog kibernetičkog napada čiji je izvor teško bilo utvrditi.

2.1.2. Klasifikacija izvora i vrsta kibernetičkih rizika u poslovnim organizacijama

Prema Biener et al. (2015) te Cebula i Young (2010) izvori kibernetičkih rizika svrstani su u **četiri kategorije**; *radnje ljudi, kvarovi sustava i tehnologije, neuspjeli organizacijski procesi i eksterni događaji*, što je sukladno okviru operativnog rizika prema Basel II i Solvency II. Međutim, kategorizaciju kibernetičkih rizika moguće je provoditi prema različitim kriterijima.

Tablica 3. Kategorizacija izvora kibernetičkih rizika

Kategorija	Potkategorija	Opis	Ključni elementi
Radnje ljudi	*Nesmotrenost*	Nenamjerne radnje poduzete bez štetne namjere	Pogreške, propusti, nepravilnosti
	Namjera	Radnje poduzete s namjerom nanošenja štete	Prijevara, krađa, vandalizam, sabotaža
	Zanemarivanje	Nedostatak aktivnosti i nedjelovanje	Nedostatak vještina, znanja, smjernica za djelovanje, dostupnosti
Kvarovi sustava i tehnologije	*Hardver*	Kvarovi na fizičkoj opremi	Problemi s kapacitetom, performansama, održavanjem, zastarjelošću
	Softver	Rizici povezani sa softverskom imovinom svih vrsta, poput programa, aplikacija i operativnih sustava	Problemi s kompatibilnošću, upravljanje konfiguracijom, kontrola promjena, sigurnosne postavke, testiranje
	Sustavi	Odstupanja u očekivanom funkcioniranju sustava	Problemi s dizajnom, specifikacijama, integracijom, složenošću
Neuspjeli interni procesi	*Dizajn ili izvedba procesa*	Neuspjeh u izvedbi definiranih procesa	Problemi s tokom procesa, dokumentacijom, ulogama i odgovornostima, obavijestima i upozorenjima, protokom informacija, eskalacijom problema,

Kategorija	Potkategorija	Opis	Ključni elementi
			dogovorima o razini usluge, prijenosom zadataka
	Kontrole procesa	Neadekvatne kontrole odvijanja procesa	Problemi s praćenjem statusa, ključnim pokazateljima rizika, ključnim pokazateljima učinka i kontrole
	Proces podrške	Neuspješni potporni procesi u isporuci odgovarajućih resursa	Problemi s osobljem, sustavom računovodstva, obukom i razvojem, nabavom
Vanjski događaji	*Katastrofe*	Događaji uzrokovani djelovanjem prirode i čovjeka te nad kojima organizacija nema kontrolu	Fizička oštećenja uzorkovana potresom, poplavom, požarom i sl.
	Pravna pitanja	Rizici izazvani pravnim sporovima	Problemi s regulatornom usklađenošću, zakonodavstvom, parnicama
	Poslovna pitanja	Rizici povezani s promjenama u poslovnom okruženju organizacije	Problemi s opskrbnim lancem, tržišnim i ekonomskim uvjetima
	Ovisnosti o uslugama	Rizici koji proizlazi iz ovisnosti tvrtke o vanjskim sudionicima	Problemi s javnim uslugama, opskrbom energijom, prijevozom i sl.

Izvor: Preuzeto iz Biener et al. (2015, str. 134) i Cebula i Young (2010, str. 3)

Kategorija *radnje ljudi* opisuje problem koji proizlazi iz poduzetih i propuštenih aktivnosti. Obuhvaća radnje unutarnjih i vanjskih aktera. Kvarovi sustava i tehnologije obuhvaćaju izazove proizašle iz nefunkcionalnosti tehnološke imovine, kao što su kvarovi hardvera, softvera te integriranih sustava. Neuspjeli interni procesi obuhvaćaju odstupanja od željenih rezultata integriranih procesa koji su posljedica lošeg dizajna ili njegove primjene. Kategorija vanjski događaji odnosi se na događaje koji su izvan kontrole organizacije.

Tablica 4. Kategorizacija kibernetičkih rizika prema CRO Forum-u

Kategorizacija kibernetičkih rizika	Definicija	Relevantne kategorije
Unutarnja prijevara	Rizik zbog namjerne zloupotrebe koja uključuje barem jednog zaposlenika organizacije	Neovlaštena aktivnost, interna krađa i prijevara, unutarnja sigurnost sustava
Vanjska prijevara	Događaji koji proizlaze iz prijevare i krađe koje inicira treća strana, uključujući sve oblike kibernetičkih rizika	Eksterna krađa i prijevara, eksterna sigurnost sustava
Sigurnost na radu	Namjerne aktivnosti i propusti koji su u suprotnosti s pravilima koji promiču sigurnost na radu	Odnosi među zaposlenicima, sigurnost radnog okruženja
Klijenti, proizvodi i poslovne prakse	Propust u ispunjavanju profesionalne obveze	Dijeljenje informacija, povjerljivost, poslovne prakse, karakteristike proizvoda, poslovna suradnja
Oštećenje fizičke imovine	Gubitci koji proizlaze iz uništenja ili oštećenja fizičke imovine	Prirodne katastrofe, nezgode, opća sigurnost
Prekid poslovanja i/ili kvarovi sustava	Gubitci povezani s prekidom poslovne aktivnosti	Interni kvarovi sustava, eksterni kvarovi sustava, nedostupnost mreže
Izvršenje, isporuka i upravljanje procesom	Gubitci zbog neuspjelog upravljanja procesom	Evidencija transakcija, izvršenje i održavanje, praćenje i izvještavanje, upravljanje računima klijenata i dobavljača

Izvor: Preuzeto iz CRO Forum (2016, str. 12)

Rea-Guaman et al. (2018) pružili su sustavan pregled radova usmjerenih na kategoriziranje kibernetičkih rizika.[15] Međutim, referirajući se na ključan rad u definiranju kibernetičkih rizika, a na kojem se temelji ovo istraživanje (Eling i Schnell, 2016), kibernetički rizici klasificiraju se prema **aktivnosti** (*kriminalni i nekriminalni*), **vrsti kibernetičkog napada** (primjerice *krađa*

[15] U cilju stvaranja uvida u različite pristupe kategorizacije kibernetičkih rizika preporuka je pogledati CERT (2021), Peters et al. (2018), Agrafiotis et al. (2018), OECD (2017).

identiteta, *prekid poslovanja*, *razotkrivanje povjerljivih informacija*), prema **izvoru** (*teroristi, kriminalci i vlade*) te prema **ciljevima napada** (*špijunaža, iznuđivanje, korištenje povjerljivih informacija, opstrukcija u radu*). Na tragu sugestija Zängerle i Schiereck, (2023), ovim istraživanjem se, također, ističe potreba za standardiziranim razumijevanjem i taksonomijom kibernetičkih rizika koja bi se koristila u budućim znanstvenim istraživanjima.

2.1.3. Utjecaj kibernetičkih rizika na poslovanje organizacija

Literatura koja je usmjerena na razmatranje utjecaja kibernetičkih rizika na poslovanje organizacija, odnosno na troškove poslovanja uzrokovane kibernetičkim rizicima, različito procjenjuje utjecaj kibernetičkih rizika na poslovanje organizacija. Naime, procjene troškova često su temeljene na anketama. Aldaroso et al. (2020) i Biener et al. (2015) ističu da je problem izostanak adekvatnog izvora informacija te visok stupanj nesigurnosti.[16] Stoga su cijeli proces i metodologija procjene troška kibernetičkih incidenata ograničeni, zbog čega je potrebno biti oprezan prilikom interpretacije učinka kibernetičkog incidenta. U cilju postizanja objektivnosti, istraživački se napori usmjeravaju na utvrđivanje promjene tržišne vrijednosti poduzeća koja su pretrpjela kibernetički incident. Mukhopadhyay et al. (2005) navode kako se neizravni učinci kibernetičkog incidenta pojavljuju u obliku gubitka reputacije, povjerenja, narušene privatnosti klijenata i smanjene tržišne kapitalizacije.

Cavusoglu et al. (2004) procjenjuju da se u razdoblju od dva dana nakon objave o pretrpljenom kibernetičkom napadu, tržišna vrijednost poslovnih organizacija smanjuje za 2,1 %, što u apsolutnim terminima u prosjeku iznosi 1,65 milijardi dolara gubitka tržišne vrijednosti. Yayla i Hu (2011) te Gordon et al. (2011) izvještavaju o značajnom smanjenju negativnog učinka kibernetičkog incidenta na vrijednost dionica tijekom vremena, pri čemu potonji rad navedenu pojavu objašnjava korekcijom procjene troškova koja je rezultat dobivanja većeg broja informacija o incidentu. Veći stupanj informiranosti investitora o kibernetičkim incidentima rezultira manjom osjetljivosti na objavu o pretrpljenom kibernetičkom incidentu (Pirounias et al., 2014). Mukhopadhyay et al. (2013) ističu kako kibernetički incidenti negativno utječu na profitnu maržu. Dodatno, ista studija potvrđuje da isti negativno utječu na reputaciju poslovne

[16] Veći dio javno dostupnih informacija o kibernetičkim incidentima te troškovima dolazi od konzultantskih tvrtki i tvrtki koje pružaju podršku u postizanju kibernetičke sigurnosti organizacijama. OECD (2017) ukazuje kako navedene podatke treba razmatrati s oprezom, budući da iste organizacije mogu imati financijsku korist od uveličavanja kibernetičkog rizika kao prijetnje.

organizacije te tržišnu kapitalizaciju. Ali et al. (2021a), Richardson et al. (2019) i Spanos i Angelis (2016) u opsežnom **pregledu literature, kojim obuhvaćaju radove u području utjecaja informacijskih i kibernetičkih rizika na tržišnu vrijednost dionica, zaključuju da rezultati većine radova upućuju na značajan negativan utjecaj incidenata na vrijednost dionica.**

McShane i Nguyen (2020), na tragu kritike Yayla i Hu (2011), razmatraju desetogodišnje razdoblje te opsežan broj kibernetičkih incidenata. Uočavaju da vrijednosnice u početku bilježe negativne prinose nakon čega se trend izmjenjuje. Kretanje krivulje prinosa najbolje je opisano U-oblikovanom funkcijom. Amir et al. (2018) ističu različite načine objave informacija o kibernetičkom incidentu, pri čemu razlikuju dobrovoljno objavljene informacije te inicijalno „skrivene“ informacije koje se objavljuju neovisno. U potonjem scenariju utjecaj objavljene informacije na vrijednost dionice je izraženije negativan. Ali et al. (2021b) potvrđuju da incidenti imaju negativne posljedice na prinose na ulaganja u dionice poslovnih organizacija tijekom razdoblja od godine dana nakon objave informacije o pretrpljenom incidentu. Dodatno, potvrđuje se povećanje rizika od nedostatne razine kapitala u razdoblju od pola godine nakon objave o pretrpljenoj povredi podataka, što sugerira da investitori percipiraju veći rizik investiranja u kompanije koje su bile izložene sigurnosnim propustima. Suprotno navedenom, Richardson et al. (2019) ukazuju da je negativan utjecaj u pravilu minimalan, posebice u slučaju izostanka ekstremnih povreda podataka, kada negativan utjecaj iščezava unutar nekoliko dana od javne objave.

Campbell et al. (2003) istražuju učinak pretrpljenog kibernetičkog napada (incident) na tržištu SAD-a te uočavaju kako reakcija tržišta ovisi o tipu napada. Uočena je značajna negativna tržišna reakcija na informaciju o neovlaštenom pristupu povjerljivim podacima, dok to nije slučaj kada je riječ o neovlaštenom pristupu podacima koji nemaju status povjerljivosti. Yayla i Hu (2011) izdvajaju uskraćivanje usluge kao oblik kibernetičkog incidenta koji uzrokuje snažniji negativni učinak na tržišnu vrijednost poduzeća u usporedbi s drugim oblicima incidenta. McShane i Nguyen (2020) tvrde da je negativni utjecaj na poslovnu organizaciju intenzivniji kada kibernetički incident uzrokuje prekid poslovanja nego kada uzrokuje povredu podataka klijenata.

Analiza utjecaja kibernetičkih rizika na poslovne organizacije može se proširiti uzimajući u obzir dodatna obilježja organizacije, poput njezine industrijske pripadnosti i veličine.

U pogledu utjecaja kibernetičkih napada na različite industrije, postizanje konsenzusa ostaje izazov s obzirom na nekonzistentne empirijske nalaze. Naime, Ali et al. (2021b), Arcuri et al. (2017), Bose i Leung (2014), Malhotra i Kubowicz Malhotra (2011) i Morse et al. (2011) ukazuju da tvrtke u financijskom sektoru doživljavaju negativnije reakcije tržišta na povrede podataka u usporedbi s drugim industrijama. Sasvim suprotno, Aldasoro et al. (2020) potvrđuju da banke i društva za osiguranje bilježe niže gubitke u usporedbi s poduzećima iz drugih sektora. Istodobno, McShaen i Nguyen (2020) potvrđuju kako se poslovne organizacije unutar maloprodajne i uslužne industrije suočavaju sa izraženijom negativnom reakcijom tržišta u odnosu na ostale industrije.

Recentno istraživanje Tayaksi et al. (2022) ukazuje da financijski i tehnološki sektori najviše trpe zbog negativnih posljedica kibernetičkih rizika. Ovi rezultati su u skladu s prethodnim studijama, poput Hovav i D'Arcy (2003) i Cavusoglu et al. (2004), koje naglašavaju da poduzeća koja maksimalno koriste prednosti internetskog poslovanja bilježe veću osjetljivost tržišne vrijednosti nakon kibernetičkog napada. Studija Yayla i Hu (2011) također potkrepljuje ovaj nalaz ukazujući na to da su tvrtke bazirane na elektroničkom poslovanju posebno izložene smanjenju tržišne vrijednosti. Hogan (2020) i Yayla i Hu (2011) ukazuju da je važan uzrok izostanka konsenzusa razmatranje uzoraka male veličine te obuhvat kratkog razdoblja.

Analizirajući različite studije, postaje jasno da je povezanost industrijske pripadnosti s ranjivošću organizacija na kibernetičke incidente složeno i neodređeno područje. U prilog navedenom govore Das et al. (2012) i Acquisiti et al. (2006) koji nisu utvrdili razlike između industrija u pogledu njihovih reakcija na kibernetičke incidente, što otežava formiranje zaključka o tome koja industrijska pripadnost povećava ranjivost organizacija na kibernetičke prijetnje.

Nakon razmatranja obilježja *industrijska pripadnost*, važno je osvrnuti se na obilježje *veličina poduzeća*. Vila et al. (2020) posebno ističu srednje i male organizacije koje zbog nedostatka znanja i sposobnosti upravljanja kibernetičkim rizicima postaju predmetom kibernetičkih napada. S druge strane, veće organizacije, iako imaju veći kapacitet za upravljanje kibernetičkim rizicima, privlačniji su cilj kibernetičkog napada. Uzimajući u obzir kako veće organizacije posluju na diversificiranim tržištima, ostvaruju prihode iz različitih izvora, imaju lakši pristup financiranju uz niže troškove, uspješnije preživljavaju nastup kibernetičkih rizika u usporedbi s manjim organizacijama (Cavusoglu et al., 2004). Empirijski nalazi Das et al. (2012), Telang i Wattal (2007) i Acquisti et al. (2006) ukazuju kako veće poslovne organizacije

bilježe veću otpornost na tržištu kapitala, u smislu manje volatilnosti u prinosu na ulaganje u dionice, nakon objave informacije o pretrpljenom kibernetičkom incidentu. Ove spoznaje naglašavaju potrebu za dubljim razumijevanjem i proučavanjem ponašanja manjih organizacija u kontekstu kibernetičkih rizika. Međutim, ne može se tvrditi kako je postignut konsenzus u vezi utjecaja kibernetičkih rizika s obzirom na veličinu. Naime, za razliku od istaknutih istraživanja, postoje istraživanja koja su polučila oprečne rezultate, pri čemu se tvrdi kako su veće organizacije izloženije negativnom djelovanju kibernetičkih rizika u odnosu na manje organizacije (Aldasoro et al., 2020; Malhotra i Kubowicz Malhotra, 2011; Gatzlaff i McCullough, 2010).

Dominantan broj radova upućuje na značajan i negativan utjecaj kibernetičkih rizika na tržišnu vrijednost poslovnih organizacija. Stoga bi **poslovne organizacije trebale usmjeriti znatno veću pažnju i uložiti veće napore u upravljanje kibernetičkim rizicima**. Na temelju analize dostupne literature, **nije moguće sa sigurnošću odrediti koja specifična obilježja poslovne organizacije izravno doprinose njihovoj osjetljivosti na kibernetičke rizike**. Stoga, pristup koji uključuje razmatranje nehomogene grupe organizacija može pružiti sveobuhvatniji uvid u ovu problematiku.

Sve izraženiji utjecaj kibernetičkih rizika na poslovanje iziskuje prilagodbe u zakonodavstvu. Propisi stalno evoluiraju i postaju važan pokretač promjena koje podupiru uspostavu prakse upravljanja kibernetičkim rizicima u poslovnim organizacijama. Stoga se u nastavku razmatra zakonodavni okvir upravljanja kibernetičkim rizicima.

2.2. Zakonodavni okvir upravljanja kibernetičkim rizicima

Zakonodavstvo u vezi kibernetičkih rizika čini temelj na koji se zemlje i poslovne organizacije oslanjaju prilikom definiranja, upravljanja te postupanja s kibernetičkim prijetnjama. U ovom dijelu rada predstavit će se zakonodavni okvir na prostoru Europske unije (EU) i Republike Hrvatske (RH) kojim se uređuje postupanje organizacija u vezi kibernetičkih rizika i promicanja kibernetičke sigurnosti. Međutim, prije no što se krene na razmatranje zakonodavstva u EU i RH, važno je istaknuti utjecaj Sjedinjenih Američkih Država (SAD) koje su bile pionir u postavljanju zakonodavnog okvira u području kibernetičke sigurnosti. Ključna promjena dogodila se 2002. godine donošenjem Zakona o domovinskoj sigurnosti (*engl. Homeland Security Act - HSA*) te uspostavom Ministarstva domovinske sigurnosti (*engl. U.S. Department*

of Homeland Security), što je osiguralo postavljanje fokusa na kibernetičke rizike i pitanje kibernetičke sigurnosti u SAD-u. Američko zakonodavstvo potaknulo je promjene na globalnoj razini, služeći kao model mnogim zemljama.

Unutar Europske unije, zakonodavstvo se prvenstveno usredotočilo na zaštitu podataka, privatnosti i kritične infrastrukture, pri čemu je potrebno izdvojiti: *Direktivu o mrežnoj i informacijskoj sigurnosti, Opću uredbu o zaštiti podataka i Akt o kibernetičkoj sigurnosti.*

Direktiva o mrežnoj i informacijskoj sigurnosti (NIS) značajna je prekretnica u području zakonodavstva o kibernetičkoj sigurnosti unutar EU. Primjenjuje se od 2016. godine te predstavlja prvi sveobuhvatan pokušaj EU da uspostavi standard kibernetičke sigurnosti među državama članicama. Direktivom su definirani **ključni sektori:** *energetika, transport, bankarstvo, infrastruktura financijskog tržišta, zdravstvo, opskrba i distribucija vodom te digitalna infrastruktura; odnosno* **operatori ključnih usluga - OKU** *(engl. Operators of Essential Services – OES)* te **davatelji digitalnih usluga - DDU** *(engl. Digital service providers – DSP, uključuje internetsko tržište, internetske tražilice, usluge računalstva u oblaku)* za koje se postavlja cilj postizanja visoke razine mrežne i informacijske sigurnosti. U okviru Direktive, predviđeno je **promicanje jedinstvenog digitalnog tržišta osnaživanjem** suradnje između država članica te **unaprjeđenje opće razine kibernetičke sigurnosti** kroz nametanje obveze pridržavanja mjera za postizanje visoke razine kibernetičke sigurnosti usluga koje pružaju (Direktiva (EU) 2016/1148).

Potrebno je istaknuti kako se primjena mjera **ograničava isključivo na ključne usluge** te da su iste uopćene na način da se primjenjuju termini „*tehničke i organizacijske mjere, mjere za sprječavanje i ublažavanje učinaka incidenta"*. Direktiva postavlja obvezujući cilj na razini Europske unije, a na pojedinačnim državama članicama je odgovornost da osmisle i usvoje odgovarajuće nacionalne propise (uredbe) kako bi se ti ciljevi postigli. Za implementaciju Direktive zadužena su nadležna tijela ili timovi za odgovor na računalne sigurnosne incidente (*engl. Computer Security Incident Response Teams – CSIRT*). Pored navedenog, organizacijama se nalaže prijavljivanje kibernetičkih incidenata nadležnim tijelima.

Sljedeća važna promjena u okviru zakonodavstva, a koja promiče ideju opće kibernetičke sigurnosti, jest **Opća uredba o zaštiti podataka** (*engl. General Data Protection Regulation – GDPR*). Primjenjuje se od 2018. godine, te je rezultat nastojanja EU da se zaštite osobni podaci

i podupre pravo na privatnost građana u svim državama članicama. Primarni cilj GDPR-a je zaštita individualnih prava na privatnost pružanjem kontrole građanima EU nad njihovim osobnim podacima (Uredba (EU) 2016/679). Prema GDPR-u, organizacije su dužne poduzeti adekvatne tehničke i organizacijske mjere za osiguranje zaštite podataka. Ove mjere uključuju pseudonimizaciju i šifriranje osobnih podataka, sposobnost osiguranja povjerljivosti, integriteta, dostupnosti i otpornosti sustava i usluga obrade te sposobnost pravovremenog obnavljanja dostupnosti podataka u slučaju fizičkog ili tehničkog incidenta (Uredba (EU) 2016/679, članak 32). Također, organizacijama se nalaže provođenje procjene učinka zaštite podataka prije pokretanja aktivnosti obrade podataka visokog rizika (Uredba (EU) 2016/679, članak 35). Nadalje, moraju obavijestiti nadzorno tijelo unutar 72 sata od dojave o povredi podataka, a u nekim slučajevima i obavijestiti oštećene strane o povredi podataka (Uredba (EU) 2016/679, članak 33-34). Ova regulatorna obveza ističe stratešku ulogu zaštite podataka te označava pomak prema većoj odgovornosti i transparentnosti u upravljanju osobnim podacima. Poslovne organizacije moraju dizajnirati svoje sustave za privatnost, minimizirati prikupljanje osobnih podataka i kontinuirano pregledavati i ažurirati mjere zaštite podataka. Ove se obveze proširuju na mala i srednja poduzeća (MSP) iako su za organizacije s manje od 250 zaposlenika, pod određenim okolnostima, predviđene iznimke (Uredba (EU) 2016/679, članak 13).

Potrebno je istaknuti kako GDPR igra ključnu ulogu u usmjeravanju postupanja s osobnim podacima, ali nije primarno usredotočena na implementaciju procesa upravljanja kibernetičkim rizicima. Iako se GDPR dotiče kibernetičke sigurnosti, fokus je prvenstveno na zaštiti prava pojedinaca na privatnost, a ne na sveobuhvatnom pristupu upravljanju kibernetičkim rizicima. Dakle, možemo zaključiti kako je riječ o zakonskom aktu koji je komplementaran s NIS Direktivom, ali u odnosu na NIS Direktivu nije obuhvatan u dijelu koji se odnosi na promicanje kibernetičke sigurnosti.

Konačno, na razini EU, potrebno je istaknuti **Akt o kibernetičkoj sigurnosti** (*engl. Cybersecurity Act*) koji je u primjeni od 2019. godine, a rezultat je nastojanja da se uspostavi europski program za certificiranje postignute kibernetičke sigurnosti za *ICT proizvode*, *usluge* i *procese*. Akt predviđa dodjelu ključne operativne uloge Agenciji Europske unije za kibernetičku sigurnost (*engl. The European Union Agency for Cybersecurity - ENISA*). Primarni cilj Akta je doprinijeti unaprijeđenu kibernetičke sigurnosti diljem EU te ojačati ulogu ENISA-e, što zajedno doprinosi jačanju povjerenja u digitalno gospodarstvo i funkcioniranje jedinstvenog digitalnog tržišta (Uredba (EU) 2019/88).

S obzirom na članstvo **Republike Hrvatske** u EU, njezino **zakonodavstvo u vezi kibernetičke sigurnosti** komplementarno je propisima na razini EU-a, a prethodno razmotreni ključni zakonodavni okviri u EU izravno određuju zakonodavni okvir u RH. Dodatno, Nacionalna strategija kibernetičke sigurnosti RH i Nacionalni okvir za razvoj i implementaciju informacijske sigurnosti u RH usklađeni su sa strategijom kibernetičke sigurnosti EU. Navedene činjenice potvrda su konvergencije nacionalnih i europskih ciljeva kibernetičke sigurnosti. U nastavku su razmotreni ključni zakonski akti u Republici Hrvatskoj.

Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/2018) ključni je dio hrvatske nacionalne strategije kibernetičke sigurnosti. Primjenjuje se od 2018. godine i predstavlja implementaciju Direktive EU o sigurnosti mrežnih i informacijskih sustava (NIS Direktiva) u nacionalno zakonodavstvo. Primarni je cilj Zakona osigurati visoku razinu sigurnosti mrežnih i informacijskih sustava diljem zemlje, pri čemu je primjena predviđena za **operatore ključnih usluga (OKU)** i **davatelje digitalnih usluga (DDU)**. Republika Hrvatska je identificirala osam ključnih sektora: *energetiku, transport, bankarstvo, infrastrukture financijskog tržišta, zdravstvo, opskrbu i distribuciju vode*, *digitalnu infrastrukturu* te *poslovne usluge za državna tijela*. Potonji je dodatni sektoru u odnosu na NIS direktivu.

Sukladno Zakonu, OKU je javni ili privatni subjekt koji pruža ključnu uslugu prikazanu u okviru priloga (*Prilog A - Pregled sektora, podsektora te ključnih usluga za koje su identificirani operatori dužni provoditi aktivnosti održavanja visokog stupanja kibernetičke sigurnosti*), pri čemu ključna usluga ovisi o mrežnim i informacijskim sustavima, a eventualni incident bi imao znatni negativan učinak na pružanje ključne usluge. S druge strane, DDU su privatni subjekti koji pružaju digitalnu uslugu pri čemu Zakon identificira tri digitalne usluge: *internetsko tržište, internetsku tražilicu* i *usluge računalstva u oblaku*. Postupak identifikacije OKU i DDU provodi Nadležno sektorsko tijelo, a detaljni prikaz vidljiv je u okviru priloga (*Prilog B - Pregled nadležnih sektorskih tijela, CSIRT-ova i tehničkog tijela za ocjenu sukladnosti prema sektorima ključnih usluga*). Prema Zakonu (NN 64/2018, članak 14.), operatori ključnih usluga i davatelji digitalnih usluga obvezni su, u cilju održavanja kontinuiteta, poduzimati mjere za postizanje visoke razine kibernetičke sigurnosti. Navedeno uključuje tehničke i organizacijske mjere za upravljanje rizicima te mjere za sprječavanje i ublažavanje učinka kibernetičkog incidenta na sigurnost mrežnih i informacijskih sustava ili

njegovog dijela koji je identificiran kao dio o kojem ovisi pružanje ključne usluge ili digitalne usluge.

Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 68/2018) donesena 2018. godine nadopunjuje Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/2018) te je usklađena s Direktivom EU-a o sigurnosti mrežnih i informacijskih sustava (NIS Direktiva). Primarni cilj Uredbe je pružiti detaljne kriterije i postupke za identifikaciju OKU-a i DDU-a, a pridonosi širem cilju NIS Direktive da se poboljša kibernetička sigurnost u EU-u uspostavljanjem jasnih odgovornosti za subjekte koji igraju ključne uloge u održavanju važnih društvenih i ekonomskih aktivnosti.

Uredbom se **utvrđuju mjere** za postizanje visoke razine kibernetičke sigurnosti operatora ključnih usluga, **način njihove provedbe**, kriteriji za određivanje incidenata koji imaju znatan učinak na pružanje ključnih usluga, sadržaj obavijesti i druga bitna pitanja koja se odnose na obavještavanje o incidentima.

Operatori ključnih usluga i davatelji digitalnih usluga dužni su: *uspostaviti sustav upravljanja sigurnošću mrežnih i informacijskih sustava te dokumentirati politiku koja mora biti odobrena na najvišoj upravljačkoj razini*; *uspostaviti organizacijsku strukturu s formalnom raspodjelom zadaća, ovlasti i odgovornosti, pri čemu je potrebno dodijeliti odgovornost za uspostavu i upravljanje sigurnostšću ključnih sustava (Prilog C) osobi s najvišim rukovodnim ovlastima; uspostaviti sustav internog nadzora provedbe mjera kibernetičke sigurnosti određenih politikom upravljanja sigurnošću ključnih sustava, o čemu je nužno izvještavati jednom godišnje u pisanoj formi; uspostaviti sustav upravljanja rizicima kojima je izložen ključni sustav, pri čemu se pretpostavlja korištenje mjera za sprječavanje i ublažavanje učinaka incidenata* (NN 68/2018).

Zakon o provedbi Opće uredbe o zaštiti podataka - GDPR (NN 42/2018) ključni je dio hrvatskog zakonodavnog okvira u pogledu zaštite osobnih podataka. Donesen je 2018. godine i predstavlja nacionalnu prilagodbu Republike Hrvatske Općoj uredbi o zaštiti podataka (GDPR) na razini EU, ciljajući na jedinstveno zakonodavstvo o zaštiti podataka na području Europske unije. Zakonom se propisuje novčana kazna za kršenje odredbi vezanih za zaštitu osobnih podataka te kao nadležno tijelo definira Agenciju za zaštitu osobnih podataka (AZOP).

Zakon o provedbi kibernetičke sigurnosne certifikacije (NN 63/2022) kao primarnu namjenu ima jačanje jedinstvenog digitalnog tržišta Europske unije s ciljem ostvarivanja digitalne suverenosti. Zakon teži tome da EU postane značajniji čimbenik na globalnoj sceni te da se poboljša otpornost tržišta na potencijalno disruptivna djelovanja konkurentskih globalnih gospodarstava. Zakon stvara temelj za trajno unaprjeđenje kibernetičke sigurnosne certifikacije kako bi se adekvatno odgovorilo na izazove digitalne transformacije. Također, definira nadležna tijela na nacionalnoj razini za provedbu certifikacije, postavlja pravila o sankcijama i pravnoj zaštiti te objašnjava postupak certificiranja za subjekte koji žele plasirati svoje informacijsko-komunikacijske proizvode, usluge ili procese na jedinstveno tržište Europske unije. Dodatno, Zavod za sigurnost informacijskih sustava određen je kao ključna institucija za nadzor i provedbu ovoga Zakona na nacionalnoj razini.

Postavljanjem zakonodavnog okvira na razini Europske unije i Republike Hrvatske stvorena je osnova za promicanje opće razine kibernetičke sigurnosti na prostoru Republike Hrvatske. Međutim, potrebno je istaknuti elemente zakonodavnog okvira koji otežavaju promicanje opće razine kibernetičke sigurnosti, pri čemu izdvajamo usmjerenost Zakona i Uredbe na operatore ključnih usluga u identificiranim sektorima te davatelje digitalnih usluga, zbog čega **izostaje obuhvatan pristup kojim se unutar zakonodavnog okvira obuhvaćaju one djelatnosti i usluge koje imaju značajan potencijal postati predmetom kibernetičkih rizika** (*primjerice za djelatnosti: sektor M – stručne, znanstvene i tehničke djelatnosti i sektor P – obrazovanje / primjerice za ključne usluge; sve osnovne i dodatne financijske usluge kreditnih institucija, a ne isključivo platne usluge*)**.** Dodatno, **izostaje razumijevanje poslovnih organizacija što definira ključnu uslugu, a isto nije moguće iščitati iz zakonskih akata čime se ostavlja prostor za interpretaciju.** Angažman Nadležnog sektorskog tijela, koje je odgovorno za identifikaciju poslovnih subjekata obuhvaćenih propisima, smanjuje mogućnost slobodne interpretacije i to na način da u izravnoj komunikaciji razjasni ključne aspekte zakona i usmjeri poslovne subjekte na ispunjenje obveza prema zahtjevima zakonodavnog okvira.[17] U prilog

[17] Međutim, pored isticanja primjene mjera visoke razine sigurnosti za ključne usluge, ističe se problem prilagodbe na zahtjeve koje postavlja Zakon, što u velikoj mjeri ovisi i o radu nadležnih sektorskih tijela koja, nakon identifikacije operatora ključnih usluga ili pružatelja digitalnih usluga i provedbe nadzora, izdaju rješenje kojim, u slučaju nepravilnosti, predviđa prilagodbu u razdoblju od godine dana. Kako bi se dobio jasan uvid u kojoj mjeri je zaživjela primjena Zakona i kako navedeno utječe na identificirane operatore ključnih usluga i davatelje digitalnih usluga, na stranicama Hrvatske agencije za nadzor financijskih usluga (HANFA), koja je nadležno tijelo za sektor infrastrukture financijskog tržišta prema Zakonu, objavljen je interesantan podatak. Naime, sukladno primjeni Direktive i Zakona, HANFA je tek u travnju 2021. godine izdala Rješenje Zagrebačkoj burzi d.d. u kojem se otkriva veći broj nesukladnosti sa Zakonom (primjerice; nerevidirani i

navedenim tvrdnjama govori Europska komisija (2023) koja izdvaja nedostatke NIS direktive, a kao glavne točke navodi: *nedovoljnu razinu kibernetičke otpornosti poduzeća koja posluju u EU, nedosljednu otpornost u državama članicama i sektorima, nedovoljno zajedničko razumijevanje glavnih prijetnji i izazova među državama članicama*. Kako bi se odgovorilo na sve nedostatke, ali i sve veće prijetnje uzrokovane digitalizacijom i međusobnom povezanošću, Komisija je revidirala skup pravila za budućnost s ciljem jačanja razine kibernetičke otpornosti unutar EU, na temelju čega je usvojena **NIS2 Direktiva**[18]**.** Ona je stupila na snagu u siječnju 2023. godine, a obvezuje države članice EU-a da do listopada 2024. godine usvoje i objave mjere potrebne za prilagodbu na NIS2 Direktivu. Na tragu recentnih zakonodavnih promjena, vrijedno je istaknuti Europski akt o upravljanju podacima (Regulativa (EU) 2022/868 2022/868)[19] čiji je glavni cilj uspostaviti usklađena pravila za pravedan pristup i upotrebu podataka.

Standardi i mjere koje zakonodavstvo predviđa moraju se shvatiti kao minimalni te ne isključuju potrebu za dodatnim, naprednijim mjerama kibernetičke sigurnosti koje poslovnim organizacijama stoje na raspolaganju. Stoga, na organizacijama ostaje da prepoznaju potrebu

neažurirani interni akti upravljanja rizicima, ugovorima, incidentima, pravilnici u vezi organizacijskog ustroja Odjela informacijske tehnologije itd.), a prilagodba se predviđa u roku od godine dana (do travnja 2022. godine). Dodatno, primjer spore prilagodbe na obvezujuću Direktivu, Zakon i Uredbu su i zastarjele Odluke Hrvatske narodne banke (HNB), Zakonom definiranog ključnog regulatornog tijela za sektor bankarstva. Naime, Odluka o primjerenom upravljanju informacijskim sustavom (NN 37/2010) najkonkretnije obrađuje pitanje kibernetičke sigurnosti, a donesena je 2010. godine, značajno prije Direktive, Zakona i Uredbe. Odluka iz 2010. godine bila je na snazi sve do travnja 2023. godine, nakon čega je na snagu stupio novi Zakon (NN 110/2022).

[18] NIS2 direktiva obuhvaća širi spektar sektora i aktivnosti, pri čemu se uklanja razlika između operatora ključnih usluga i davatelja digitalnih usluga. Subjekti se klasificiraju prema važnosti i podijeljeni su u dvije kategorije: bitni i važni subjekti, a shodno tome predviđen je različit režim nadzora. Pretpostavlja se da će sve srednje i velike poslovne organizacije u identificiranim sektorima bit obuhvaćene NIS2 Direktivom. Istodobno, državama članicama ostavlja se diskrecijsko pravo identificiranja manjih subjekata s profilom visokog sigurnosnog rizika koji bi također trebali biti obuhvaćeni obvezama NIS2 Direktive. Propisuju se ključni elementi na koje tvrtke trebaju obratiti pažnju u svojim politikama upravljanja kibernetičkim rizikom. Nastoji se uravnotežiti brzo izvješćivanje kako bi se spriječilo širenje incidenata s dubinskim izvješćivanjem kako bi se dobili vrijedni uvidi iz svakog slučaja. Uvodi se stroži nadzor te se predviđaju poboljšana pravila o postupanju i odgovoru na kibernetičke incidente.

[19] Cilj Akta o upravljanju podacima jest osigurati širu dostupnost podataka te potaknuti njihovu razmjenu između različitih sektora i država članica EU-a. Ova namjera proizlazi iz prepoznate važnosti podataka kao ključnog resursa za unaprjeđenje europske ekonomije i dobrobiti njenih građana. Stoga se kroz ovu inicijativu teži maksimalnom iskorištavanju potencijala podataka, s ciljem generiranja konkretnih koristi kako za europske građane, tako i za poslovne subjekte unutar Unije. Akt promiče veću pravnu jasnoću, sprječava zlouporabu prilikom dijeljenja podataka, omogućava pristup podacima javnog sektora privatnom sektoru u svrhu javnog interesa i otvara put za učinkovitiju interoperabilnost podataka (Europska komisija, 2023b).

za stalnim poboljšanjem svoje kibernetičke sigurnosti, prilagođavajući se brzom razvoju tehnologija i kibernetičkim prijetnjama. Primjena zakona i njihova učinkovitost u praksi ovisit će o nizu čimbenika kao što su kapacitet država za provedbu i nadzor te inicijativa i sposobnost organizacija.

2.3. Upravljanje kibernetičkim rizicima u poslovnim organizacijama

U kontekstu tehnološke evolucije, upravljanje kibernetičkim rizicima postaje ključni aspekt zaštite informacija, informacijskih sustava i komunikacijske infrastrukture u poslovnim organizacijama, pri čemu se upravljanje kibernetičkim rizicima opisuje kao proces koji obuhvaća analiziranje prijetnji, ranjivosti i utjecaja kibernetičkih napada na ciljeve organizacije te pruža način postizanja ravnoteže između sigurnosti i funkcionalnosti angažiranih informacijskih sustava (Wallner, 2014). Potonje naglašava važnost strateškog promišljanja o sigurnosti i funkcionalnosti kao suprotstavljenim, ali jednako važnim, aspektima u dizajnu i održavanju informacijskih sustava. IBM (2023) *upravljanje kibernetičkim rizicima* izjednačava s terminom *upravljanje rizicima kibernetičke sigurnosti* koji opisuje kao proces prepoznavanja i određivanja prioriteta te upravljanja i praćenja rizika za informacijske sustave. Hoppe et al. (2021), oslanjajući se na ISO/IEC standard, *upravljanje kibernetičkim rizicima* opisuju kao skup aktivnosti koje se mogu podijeliti u tri glavna područja: identifikaciju rizika, procjenu rizika te tretman rizika, pri čemu ističu da su standardi neizostavni element u nastojanju istraživača da definiraju upravljanje kibernetičkim rizicima. Potonje se potvrđuje u Romanosky i Sayers (2023), Eling et al. (2021), Elling i Schnell (2016) i Kosub (2015).

Eling et al. (2021) raspravljaju o pojmu *upravljanje kibernetičkim rizicima*, referirajući se na nekoliko ključnih termina kao što su *računalna sigurnost*, *informacijska sigurnost* i *kibernetička sigurnost*, a svaki odražava različite faze i aspekte područja. Raznolikost terminologije, kako ističu Eling et al. (2021), bila je predmetom mnogih znanstvenih radova (Schatz et al., 2017; Alshaikh et al., 2014; Craigen et al., 2014; Finne, 2000; Stubley, 2013; Von Solms i Van Niekerk, 2013) koji su za cilj imali razjašnjavanje ovih pojmova. Eling et al. (2021) naglašavaju da ova evolucija termina povezanih s upravljanjem kibernetičkim rizicima i dalje stvara konfuziju, što predstavlja izazov za uspostavu ujedinjenog pristupa u upravljanju korporativnim kibernetičkim rizicima i provođenju interdisciplinarnih istraživanja.

Upravljanje kibernetičkim rizicima i kibernetička sigurnost usko su povezani. Kako bi se postigla kibernetička sigurnost, ključno je adekvatno upravljati kibernetičkim rizicima. Schatz et al. (2017) kibernetičku sigurnost povezuju sa skupom aktivnosti i mjera čija je svrha doprinijeti očuvanju povjerljivosti, cjelovitosti i dostupnosti informacija i sustava u kibernetičkom prostoru.[20] Potonji pristup je sukladan CERT (2021) i ISO/IEC 270032:2023 (2023). Obuhvatnu definiciju ponudili su Von Solms i Van Niekerk (2013), pri čemu se kibernetička sigurnost definira kao zaštita kibernetičkog prostora, elektroničkih informacija, ICT infrastrukture i korisnika kibernetičkog prostora, uključujući sve njihove interese čija ranjivost proizlazi iz kibernetičkog prostora.

Prema International Communication Union (2008) sigurnost u kibernetičkom prostoru predstavlja skup alata, politika, sigurnosnih koncepta, sigurnosnih mjera, smjernica, pristupa upravljanju rizikom, akcija, obuke, najboljih praksi, jamstava i tehnologija koje se mogu koristiti za zaštitu kibernetičkog prostora. Craigen et al. (2014) definiraju kibernetičku sigurnost kao promišljeno kombiniranje resursa, procesa i struktura, kojima se štiti kibernetički prostor te sustavi povezani s kibernetičkim prostorom. Kibernetička sigurnost uključuje složenu interakciju između ljudi, između sustava te između ljudi i sustava, a usmjerena je na obranu od namjernih, slučajnih i prirodnih prijetnji. Temeljem pregleda literature, zaključuje se da je kibernetička sigurnost primarno usmjerena na zaštitu i očuvanje povjerljivosti, cjelovitosti i dostupnosti informacija unutar kibernetičkog prostora, pri čemu zaštita obuhvaća širok skup elemenata koji uključuju *elektroničke informacije*, *ICT infrastrukturu* i *korisnike*. Primarno pretpostavlja kombinaciju alata, mjera i tehnologija s ciljem zaštite od različitih prijetnji, bilo da su rezultat namjere, slučaja ili prirodne sile.

Nužno je ukazati na to da kibernetička sigurnost ne bi smjela biti ograničena na tehničke mjere[21] koje predstavljaju mehanizam zaštite od kibernetičkih rizika. Naime, tehničke mjere predstavljaju neizostavni dio dobro osmišljenoga procesa upravljanja kibernetičkim rizicima (Arbanas, 2021), a u interesu organizacije je da postanu integrirani dio procesa upravljanja poslovnim rizicima organizacije (*engl. Enterprise risk management - ERM*).

[20] Eling et al. (2020) ukazuju kako se termin upravljanje kibernetičkim rizicima pojavljuje u varijacijama te izdvaja termine računalna sigurnost, informacijska sigurnost, upravljanje rizikom informacijske sigurnosti, i kibernetička sigurnost (Von Solms i Van Niekerk, 2013).

[21] Primjerice, tehničke mjere zaštite odnosile bi se na enkripciju, vatrozid, antivirusni program, alat za otkrivanje i sprječavanje neautoriziranog pristupa i sl. (Arbanas, 2021).

Naime, poslovne organizacije se ne suočavaju isključivo s jednom kategorijom rizika, stoga je potrebno uspostaviti integrirano upravljanje kibernetičkim rizicima. ERM se znatno razlikuje od tradicionalnih koncepata upravljanja rizicima te kombinira cjelokupne korporativne aktivnosti upravljanja rizicima u jedan integrirani, holistički okvir (Romanosky i Sayers, 2023; Gatzert i Martin, 2015). Definira se kao proces koji objedinjuje *identifikaciju, kvantifikaciju* (procjenu potencijalnih utjecaja na poslovanje), *integraciju* (izradu agregiranog profila rizika za poslovnu organizaciju), *prioritizaciju*, potom *izbor* i *primjenu* određene *metode upravljanja rizikom* prema relevantnom kriteriju te *nadzor* (Harrington i Niehaus, 2004; Stine et al., 2020). Tradicionalni pristupi, nasuprot tome, općenito se temelje na razmatranju rizika u „silosima" odnosno u izoliranoj perspektivi, pri čemu se aktivnosti upravljanja razmatraju pojedinačno, od rizika do rizika (Harrington i Niehaus, 2004; Kleffner et al., 2003).

Zbog toga što ERM agregira sve rizike na razini poslovne organizacije i uzima u obzir međuovisnosti između rizika, time omogućava bolju procjenu izloženosti riziku cjelokupne poslovne organizacije te dodatno poboljšava proces odlučivanja (Pagach i Warr, 2011; Hoyt i Liebenberg, 2011; Nocco i Stulz, 2006). COSO (2009) ističe ERM kao dio korporativne strategije, stoga su odluke definirane odozgo prema dolje, pri čemu viši menadžment preuzima ključnu odgovornost.

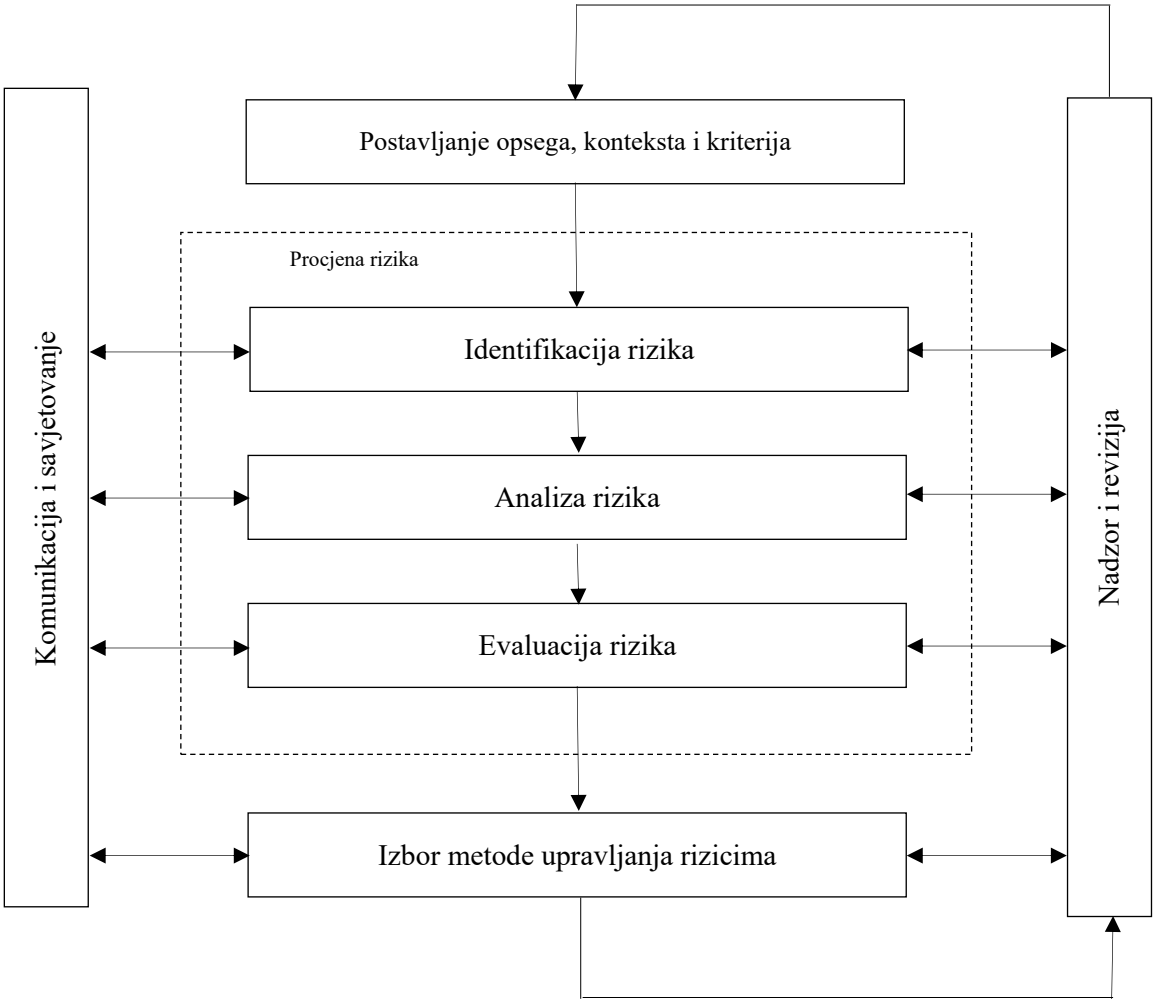
ERM, upravljanje kibernetičkim rizicima i kibernetička sigurnost su komplementarni, a njihov zajednički cilj je zaštita organizacije te stvaranje otpornosti prema sve složenijem i neizvjesnijem okruženju. Uspješno uspostavljen ERM uvažava činjenicu da u današnje vrijeme kibernetički rizici postaju kritična stavka u postizanju neometanog odvijanja poslovnih procesa te da je nužno koristiti načela kibernetičke sigurnosti. Kada je upravljanje kibernetičkim rizicima usklađeno s pristupom organizacije upravljanju poslovnim rizicima (ERM), osigurava se zaštita najvažnijih i najosjetljivijih resursa, a organizacija postiže kibernetičku sigurnost.

S ciljem sveobuhvatnijeg razumijevanja ERM-a kao procesa, u nastavku se pruža uvid u njegove neizostavne komponente. U razradi procesa primjenjuje se međunarodni standard ISO/IEC 3100:2018 (2018) koji obuhvaća ključne aspekte potrebne za uspješno upravljanje rizicima poslovne organizacije.

2.3.1. Elementi procesa upravljanja rizicima

Proces upravljanja rizikom uključuje „*sustavnu primjenu politika, postupaka i praksi na aktivnosti komuniciranja i savjetovanja, uspostavljanja konteksta i procjene, tretiranja, praćenja, pregleda, bilježenja i izvješćivanja o riziku*“ (ISO/IEC 3100:2018).

Razmatranjem **koncepta upravljanja rizicima** kao poslovnog procesa pruža se koncepcijska osnova za analizu, procjenu i obradu rizika, pri čemu je primjena adekvatna za različita područja.



Slika 3. Integrirani pristup upravljanja rizicima

Izvor: Izrada autora prema ISO/IEC 3100:2018 (2018)

Nakon što su istaknuti osnovni elementi procesa upravljanja rizicima prema ISO/IEC standardu (*Slika 3*), važno je detaljno razmotriti svaku pojedinu komponentu procesa kako bi se stekao potpuni uvid u njegov sadržaj i funkcionalnost.

Komunikacija i savjetovanje

Svrha komunikacije i savjetovanja je pomoći relevantnim dionicima u poslovnoj organizaciji da svoje odluke temelje na riziku koji razumiju i da poduzmu potrebne korake koje proces upravljanja rizicima predviđa. Komunikacija osigurava jačanje svijesti i razumijevanje rizika, dok savjetovanje jamči podršku u odlučivanju, a oboje bi trebalo biti zastupljeno kroz cjelokupni proces upravljanja rizicima. Komunikacija i savjetovanje, kao element procesa upravljanja rizicima, predviđa različita područja stručnosti unutarnjih i vanjskih dionika te osigurava da se rizik razmotri iz različitih perspektiva i pruži dovoljno informacija kako bi se olakšalo donošenje odluka u vezi rizika (ISO/IEC 31000:2018).

Komunikacija u kontekstu upravljanja kibernetičkim rizicima uključuje redovito dijeljenje informacija o kibernetičkim rizicima unutar poslovne organizacije koje za ključni cilj ima jačanje svijesti o kibernetičkim rizicima i doprinos njegovom razumijevanju. Savjetovanje, s druge strane, obuhvaća aktivno angažiranje sudionika i stručnjaka u proces upravljanja rizicima te stvara podršku u odlučivanju. Prilikom definiranja relevantnih izvora informacija i identifikacije tko bi mogao biti pogođen kibernetičkim rizicima, važno je uzeti u obzir sve dionike. S obzirom na globalnu prirodu kibernetičkog prostora, potencijalni dionici mogu biti prisutni na različitim lokacijama. Stoga su potrebni dobro osmišljeni planovi i procedure za prikupljanje, dijeljenje, zaprimanje i korištenje relevantnih informacija (Refsdal et al., 2015). Nadalje, potencijalni izvori rizika su višestruki, a nastup kibernetičkog rizika može imati značajan utjecaj na poslovanje organizacije. S obzirom na činjenicu da su kibernetički rizici kompleksni, a posljedice kibernetičkih incidenata mogu biti ozbiljne, važno je da svi ključni dionici poslovne organizacije imaju točne i ažurne informacije o rizicima te da su aktivno uključeni u proces upravljanja rizicima.

Postavljanje opsega, konteksta i kriterija

Opseg se odnosi na aktivnosti upravljanja rizicima koje poslovna organizacija planira provoditi, a može se primijeniti na različite razine unutar organizacije uključujući strateške, operativne, programske, projektne aktivnosti. Prilikom određivanja opsega aktivnosti ključno je definirati

aktivnosti sukladne općim ciljevima organizacije. U okviru predstavljene faze, potrebno je razumjeti unutarnje i vanjsko okruženje u kojem poslovna organizacija djeluje. Riječ je o razumijevanju konteksta u kojemu se poslovne aktivnosti odvijaju, a na koje je potrebno primijeniti proces upravljanja rizicima. Definiranje kriterija rizika počinje određivanjem razine sklonosti organizacije prema riziku. Nakon toga, odlučuje se o strategijama upravljanja za svaku vrstu rizika, bilo da se radi o *izbjegavanju, umanjivanju, transferu* ili *zadržavanju* određenih rizika. Također, organizacija treba odrediti kriterije za procjenu značajnosti rizika i donošenje odluka koji trebaju biti usklađeni s politikama upravljanja rizicima organizacije, prilagođeni specifičnim ciljevima i opsegu aktivnosti te odražavati vrijednosti, ciljeve i resurse organizacije (ISO/IEC 3100:2018).

Planirane aktivnosti poslovne organizacije mogu uključivati upravljanje specifičnim oblicima kibernetičkog rizika kao što je rizik od zlonamjernog softvera (*engl. Malware*), ucjenjivačkog softvera (*engl. Ransomware*), rizik od napada s ciljem krađe identiteta (*engl. Phishing*), i rizik od neovlaštenog pristupa i sl., ali i provođenje općih mjera zaštite osjetljivih podataka i sprječavanje neovlaštenog pristupa, pri čemu se razmatra širi spektar oblika kibernetičkog rizika. Kada se razmatra kontekst, vanjski čimbenici mogu se odnositi na promjenu regulative u pogledu zaštite podataka, očekivanja kupaca u vezi sigurnosti podataka te različite oblike utjecaja u domeni administracije, politike, ekonomije te društvenog okružja. Unutarnji čimbenici mogu se odnositi na unutarnje politike i procedure, postupanje zaposlenika, implementirana tehnološka rješenja, ali i ono što je u domeni organizacijske misije, vizije, strategije, upravljanja i kulture (Hoppe et al., 2021).

Procjena rizika

Procjena rizika je cjelokupni proces *identifikacije rizika*, *analize rizika* i *evaluacije rizika*, a treba se provoditi sustavno, iterativno i koordinirano, koristeći napredna znanja i suvremenu praksu (ISO/IEC 3100:2018).

Identifikacija rizika

Svrha identifikacije rizika je prepoznati i opisati rizike koji bi poslovnoj organizaciji onemogućili postizanje ciljeva. Prilikom identifikacije rizika ključno je raspolagati relevantnim te ažuriranim informacijama (ISO/IEC 3100:2018). Poslovne organizacija bi trebale identificirati rizike, bez obzira koliko je iste moguće kontrolirati. Rafsdale et al. (2015) segmentiraju proces identifikacije na nenamjerne i zlonamjerne izvore kibernetičkih rizika.

Kako bi se olakšala identifikacija, korisno je konzultirati relevantne izvore, poput međunarodnih standarda, godišnjih i polugodišnjih izvještaja o kibernetičkim rizicima i sigurnosti, ali i korisnih kataloga rizika[22]. Prilikom provođenja aktivnosti identifikacije rizika, korisno je uključiti pojedince čija stručnost i znanje doprinose kvaliteti provedbe identifikacije rizika. Informacije se nerijetko prikupljaju putem upitnika, intervjua i radionica (*delphi metode, brainstroming sesija*) (Harrington i Niehaus, 2004). Kako bi se identificirali relevantni zlonamjerni izvori prijetnje, potrebno je razumjeti tko može pokrenuti napade, što ih motivira, kakve su njihove sposobnosti i namjere te kako se napadi mogu pokrenuti (Rafsdale et al., 2015). Osim navedenoga, u okviru ove faze procesa upravljanja rizicima, istražuju se postojeći mehanizmi obrane kako bi se definirala njihova adekvatnost u odnosu na identificirane prijetnje. Za specifične prijetnje ili ranjivosti također se provode razne vrste sigurnosnih testiranja, poput penetracijskog testiranja i skeniranja ranjivosti. Nastavljajući se na identifikaciju kibernetičkih rizika koji nisu uzrokovani s namjerom, važno je razmotriti tko je uključen u proces koji se nadzire, a čiji sudionici mogu uzrokovati nastup incidenta. Potrebno je razmotriti i kibernetičke rizike čiji izvor nije čovjek već tehnologija, poput kvara hardvera, djelovanja prirodne sile i sl. Sustavno prikupljanje podataka o takvim incidentima doprinosi identifikaciji izvora prijetnji. ISO standard te NIST vodič također mogu biti od pomoći (Rafsdale et al., 2015).

Analiza rizika

Svrha analize rizika je razumijevanje prirode rizika i njegovih karakteristika. U ovoj fazi primarno se razmatra učestalost pojavljivanja i intenzitet utjecaja. Također, predviđena je izrada scenarija pri čemu je nužno poštovati činjenicu kako potencijalni incident može uzrokovati različite posljedice i može utjecati na različite organizacijske ciljeve (ISO/IEC 3100:2018). Ovisno o dostupnosti i pouzdanosti podataka te raspoloživim resursima, analiza rizika se može provesti s različitim stupnjem složenosti pa razlikujemo kvalitativnu, kvantitativnu te kombiniranu analiza. ISO/IEC 3100:2018 (2018) ističe kako je analiza rizika podložna pristranostima i percepciji rizika, stoga je ključno analizu dokumentirati, a donositelje odluka obavijestiti o ograničenjima. S obzirom na obilježja kibernetičkih rizika (*opisano pod točkom 2.1.2.*), procjena vjerojatnosti nastupa i razmjera utjecaja kibernetičkih rizika na poslovanje

[22] Korisno je istaknuti katalog rizika (informacija) koji pomaže u identifikaciji rizika, a kojega pružaju međunarodno prepoznate neprofitne organizacije Mitre i Open Web Application Security Project (OWASP). Katalozi pružaju pomoć u identifikaciji i upravljanju kibernetičkim rizicima te pomažu organizacijama u identifikaciji ranjivosti koje treba otkloniti i odabiru najboljeg načina kako to napraviti..

organizacije iznimno je zahtjevna, pri čemu se posebno izdvajaju kibernetički rizici čiji izvor je ljudska namjera.

Evaluacija rizika

Cilj evaluacije rizika jest pružanje podrške u donošenju odluka. Evaluacija rizika u skladu s ISO standardima podrazumijeva usporedbu rezultata dobivenih analizom rizika s prethodno utvrđenim kriterijima rizika, a s ciljem identifikacije područja koja zahtijevaju dodatne aktivnosti. U tom kontekstu, moguće su različite odluke: *ne poduzimati dodatne korake*, *razmatrati opcije za tretman rizika*, *provesti detaljniju analizu za bolje razumijevanje rizika*, *zadržati postojeće kontrole* ili *ponovno preispitati ciljeve*. Sve donesene odluke trebaju uzeti u obzir širi kontekst te stvarne i percipirane posljedice za sve vanjske i unutarnje dionike (ISO/IEC 3100:2018).

Izbor metode upravljanja rizicima

Izbor metode upravljanja rizicima ogleda se u odabiru i implementaciji odgovarajućih opcija za njegovo rješavanje. Prema ISO standardu, obuhvaća niz iterativnih koraka: *formuliranje i odabir najboljih opcija za upravljanje rizicima*, *planiranje i provedba*, *procjena učinkovitosti implementiranih mjera*, *evaluacija prihvatljivosti preostalog rizika*. Odabir najprikladnije kombinacije metoda upravljanja rizicima, pri čemu razlikujemo *izbjegavanje rizika*, *smanjivanje rizika*, *prijenos rizika* i *zadržavanje rizika* (Eling et al., 2020), podrazumijeva balansiranje između potencijalnih koristi koje proizlaze iz smanjenja negativnog utjecaja rizika na poslovanje te troškova koji se javljaju prilikom implementacije procesa upravljanja rizicima (Harrington i Niehaus, 2004). Metode upravljanja rizicima nisu međusobno isključive, niti su uvijek prikladne u svim okolnostima, međutim, odluka o tretiranju rizika temelji se na širem skupu čimbenika. Pored ekonomskih čimbenika, važno je uključiti stavove, vrijednosti i percepcije dionika procesa upravljanja rizicima.

Upravljanje rizicima predviđa izradu plana djelovanja kojeg je nužno integrirati s općim planovima i procesima u poslovnoj organizaciji. Izrađuju se kako bi bili razumljivi svima koji su uključeni u njihovu provedbu. Plan upravljanja rizicima trebao bi sadržavati sljedeće informacije: *obrazloženje za odabir određenih opcija tretiranja, uključujući očekivane koristi koje se namjeravaju ostvariti; imenovanje osoba odgovornih za odobravanje i implementaciju plana; predložene radnje koje treba poduzeti; potrebne resurse, pokazatelje učinkovitosti; eventualna ograničenja; zahtjeve za izvještavanje i praćenje; te rokove za provođenje i*

dovršetak određenih radnji. Time se osigurava transparentnost i jasnoća procesa, što olakšava provedbu upravljanja rizicima (ISO/IEC 3100:2018).

Tehnička priroda kibernetičkih rizika određuje mogućnosti tretiranja rizika, ali ne smije se zanemariti ljudski faktor koji utječe na koristi primijenjene metode upravljanja kibernetičkim rizicima (Rafsdale et al., 2015). Kada se identificirani rizici smatraju prevelikima ili izostaje korist od drugih metoda upravljanja rizicima, adekvatno je donijeti odluku o potpunom izbjegavanju rizika (ISO/IEC 27005/2022). Izraženija integracija digitalnih rješenja u poslovne procese čini metodu izbjegavanja rizika teže provedivom i manje racionalnom (Eling et al., 2020). Primjenjivanje metode *smanjenje rizika* podrazumijeva smanjivanje intenziteta i učestalosti pojavljivanja kibernetičkih rizika. Upravo ova metoda predstavlja ključni pristup u upravljanju kibernetičkim rizicima. Alati i kontrole korisni za smanjenje kibernetičkih rizika uključuju *korekciju, eliminaciju, prevenciju, minimiziranje utjecaja, odvraćanje, otkrivanje, oporavak, nadzor i podizanje svijesti među zaposlenicima* (ISO/IEC 27005/2022).[23] Poslovne organizacije moraju pažljivo odabrati alate i kontrole kako bi se postigla ravnoteža između performansi sustava i učinkovitosti sigurnosti (Arbanas, 2021). Uvođenje kontrola i primjena alata kojima se kontrolira izloženost riziku ne jamči potpuno sprječavanje negativnog djelovanja kibernetičkih rizika, stoga je korisno kibernetičke rizike prenijeti na društvo za osiguranje (Mukhopadhyay et al., 2005). Riječ je o primjeni financijske kontrole rizika pri čemu *prijenos rizika* kao metoda upravljanja rizicima podrazumijeva odluku poslovne organizacije da ugovori policu osiguranja od kibernetičkih rizika te tim postupkom transferira rizik na društvo za osiguranje (ENISA, 2012). Snižavanje premije osiguranja zbog poduzetih preventivnih mjera potiče poslovne organizacije na investiranje u mjere sigurnosti (Shetty et al., 2018; Marotta et al., 2017; Baer i Parkinson, 2007), a metodu transfera rizika čini komplementarnim metodama smanjivanja rizika kroz uvođenje tehničkih rješenja i kontrola. Prijenos rizika može se postići prijenosom odgovornosti na organizacije koje preuzimaju ulogu pružanja podrške u kibernetičkoj sigurnosti, a time kontroliraju izloženost organizacije kibernetičkom prostoru (ISO/IEC 27005/2022). Ukoliko razina kibernetičkih rizika s kojima se suočava organizacija ne prelazi kritičnu razinu te vodstvo organizacije smatra kibernetički rizik prihvatljivim, adekvatno je primijeniti metodu *zadržavanje rizika,* pri čemu se u slučaju nastupa kibernetičkih rizika sve negativne posljedice pokrivaju iz vlastitih izvora, bez mogućnosti

[23] Detaljniji uvid o kontrolama koje su korisne za kontroliranje informacijskih i kibernetičkih rizika razmatran je u okviru ISO/IEC 27002:2022 (2022).

sudjelovanja vanjskog subjekta kao što je slučaj s ugovorenom policom osiguranja od kibernetičkih rizika.

Nadzor i revizija

Svrha nadzora i revizije je osigurati i poboljšati kvalitetu i učinkovitost procesa upravljanja rizicima. Kontinuirani nadzor i periodična revizija procesa upravljanja rizicima i njegovih rezultata trebali bi biti planirani dio procesa upravljanja rizicima. Nadzor i revizija trebali bi se odvijati u svim fazama procesa te uključivati *planiranje, prikupljanje i analizu informacija, bilježenje rezultata i pružanje povratnih informacija*. Rezultati nadzora i revizije trebaju biti dio redovnih izvještavanja organizacije (ISO/IEC 3100:2018). Koristi izvještavanja se ogledaju u pružanju informacija koje podržavaju donošenje odluka, poboljšanje aktivnosti upravljanja rizikom te olakšanu interakciju sa svim relevantnim dionicima. Faktori koje je potrebno uzeti u obzir prilikom izvještavanja uključuju: različite dionike i njihove specifične potrebe za informacijama, trošak, učestalost i pravovremenost izvještavanja, metodu izvještavanja, te relevantnost informacija za organizacijske ciljeve i donošenje odluka što u konačnici za rezultat ima bolje, transparentnije i učinkovitije postavljen proces upravljanja rizicima (ISO/IEC 3100:2018).

S obzirom na obilježja kibernetičkih rizika, proces upravljanja kibernetičkim rizicima mora biti fleksibilniji i dinamičniji od tradicionalnih procesa upravljanja rizicima. Takvo dinamično okruženje zahtijeva oslanjanje na suvremenu tehnologiju te provođenje procesa u realnom vremenu, kako bi se moglo adekvatno odgovoriti na izazove koji se stalno mijenjaju. Stoga bi se svi opisani koraci procesa upravljanja rizicima trebali u većoj mjeri automatizirati, kako bi se postigla korist uspostave procesa upravljanja kibernetičkim rizicima i njihove integracije u okvir procesa upravljanja poslovnim rizicima.

Nakon razmatranja elemenata procesa upravljanja rizicima, u nastavku se pruža uvid u koristi upravljanja kibernetičkim rizicima, pri čemu implementacija prilagođenoga procesa upravljanja ne samo da štiti resurse i reputaciju organizacije, već može doprinijeti ostvarivanju strateških ciljeva, poboljšanju konkurentske prednosti i u konačnici, osiguravanju održivog rasta. U ovom dijelu ćemo istražiti konkretne primjere koristi koje organizacije ostvaruju kroz sofisticirano upravljanje kibernetičkim rizicima, dokazujući time važnost integracije ovog procesa u opće upravljanje rizicima.

2.3.2. Koristi i izazovi integriranog upravljanja kibernetičkim rizicima

Implementacija ERM-a pozitivno doprinosi poslovanju organizacije te bogatstvu dioničara (Romanosky i Sayers 2023; Gatzert i Martin, 2015). Primjena ERM-a doprinosi smanjenju ukupnog rizika organizacije (McShane, 2018; Grace et al., 2015), a značajan pozitivan utjecaj implementacije ERM-a i vrijednosti za dioničare potvrđuju studije Lechner i Gatzert (2018), McShane et al. (2011), Pagach i Warr (2011) te Hoyt i Liebenberg (2011; 2008). Utjecaj ERM-a na operativnu efikasnost tvrtke potvrđuje se u istraživanju Grace et al. (2013; 2015). Potvrđuje se da uspješno implementiran proces upravljanja rizikom stvara dodanu vrijednost za organizaciju (Hoyt i Liebenberg, 2015). Naime, tvrtke s ERM-om mogu profitirati od holističkog pristupa razmatranju rizika i poboljšane koordinacije odjela na način da poboljša alokacija resursa i poveća povrat na kapital. ERM doprinosi smanjenju volatilnosti prihoda i novčanog toka, čime se smanjuje vjerojatnost financijskih poteškoća, a financiranje se ostvaruje prema povoljnijim uvjetima. Sax i Anderson (2019) potvrđuju kako ERM utječe na povećanje profitabilnosti. Međutim, iako je sveobuhvatni utjecaj ERM-a na tvrtke pozitivan, pojedinačni utjecaj može varirati ovisno o specifičnim karakteristikama tvrtke, ciljevima i metodama implementacije ERM-a (Gatzert i Martin, 2015).

Poštujući činjenicu da kibernetička sigurnost često zauzima usmjereniji pristup i koncentrirajući se na rizike vezane uz informacije, mreže i sustave povezane s kibernetičkim prostorom, potrebno je istaknuti kako integracija upravljanja kibernetičkim rizicima unutar okvira ERM-a može donijeti značajne koristi, uključujući konsolidaciju, optimizaciju kapitala i bolje korištenje resursa (Kure et al., 2018). ERM, koji uključuje kibernetičke rizike kao dio portfelja, pruža poduzećima alat za identifikaciju i praćenje potencijalnih prijetnji kroz sveobuhvatan pristup te reducira troškove obrane od različitih izvora prijetnji (McShane, 2018; Krause i Tse, 2016).

Istraživanje Ashby et al. (2018) ističe da sustavi upravljanja rizicima u poslovnim organizacijama ne pridaju dovoljno pažnje kibernetičkim rizicima. Ističu problem izostanka integracije kibernetičkih rizika u okvir ERM-a, što rezultira zanemarivanjem kibernetičkih rizika. U prilog tome ističe se istraživanje Marotta i McShane (2018) koje ukazuje na izostanak analize i strateškog pristupa u suočavanju s kibernetičkim rizicima. Potonje je vidljivo iz rezultata istraživanja Price Waterhouse Coopers (2018) u kojem se potvrđuje da se upravljanje kibernetičkim rizicima često svodi na niže razine organizacije, što je posljedica nedostatka

razumijevanja i spremnosti uprave da se bavi ovim izazovima, kao što je istaknuto i u radu Eling et al. (2020). Stine et al. (2020) potvrđuju važnost komunikacije u postizanju integracije kibernetičkih rizika u okviru ERM-a, međutim, komunikacija između voditelja informacijske sigurnosti (*engl. Chief information security officer - CISO*) i voditelja IT odjela (*engl. Chief information officer - CIO*) s ostalim odjelima nije na optimalnoj razini. RiskOptics (2023) u svom izvješću otkrila je da mnoge organizacije u SAD-u, posebno na razini glavnih izvršnih menadžera, ne razumiju u potpunosti kibernetičke rizike, što rezultira nedovoljnim ulaganjima u kibernetičku sigurnost. Marsh (2019) dodatno naglašava da većina članova uprave ne posvećuje dovoljno vremena razmatranju kibernetičkih rizika. Istaknute činjenice upućuju na zaključak da ne postoji dovoljna integracija procesa upravljanja kibernetičkim rizicima unutar ERM-a (Ernst & Young, 2018).

Na tragu Gale et al. (2022) koji naglašavaju važnost uključivanja kibernetičke sigurnosti kao integralnog dijela ERM-a te Lanz (2018), ističe se nužnost napuštanja prakse izoliranog upravljanja kibernetičkim rizicima unutar IT odjela. Potreban je integrirani pristup upravljanju rizicima koji, uvažavajući međuovisnost svih poslovnih rizika, uzima u obzir utjecaj kibernetičkih rizika na poslovanje organizacije.

Na tragu uočenog nedovoljnog upravljanja kibernetičkim rizicima i njegove integracije unutar upravljanja poslovnim rizicima, u nastavku se izdvajaju izazovi upravljanja kibernetičkim rizicima, koji doprinose uspostavi prakse upravljanja rizicima i njezine integraciji u poslovne procese.

Organizacija koja se odluči na upravljanje kibernetičkim rizicima suočena je s nizom izazova, a koristan pregled izazova u kontekstu upravljanja informacijskim rizicima, primjenjiv na kibernetičke rizike, ponudilo je istraživanje Bergström i Ericson (2019) po uzoru na Feng et al. (2014). Identificirano je šest skupina izazova kako slijedi: *problem utvrđivanja vrijedne imovine koju treba zaštititi i koje bi se potencijalne protumjere mogle upotrijebiti za zaštitu imovine, procjena vrijednosti imovine koju treba zaštiti od rizika*; *neuspješna procjena rizika*; *podcjenjivanje rizika*, *nedostatak razmjene znanja i informacija* te *nedostatak tehnika procjene troškova i koristi povezanih s aktivnostima upravljanja kibernetičkim rizicima*. Pregledom literature identificirane su dodatne prepreke razvoju prakse upravljanja kibernetičkim rizicima u poslovnim organizacijama. Sukladno Deloitte (2016), izdvajaju se *neravnoteža između trenutnih ranjivosti i budućih sigurnosnih zahtjeva, neadekvatan budžet te izostanak*

promišljenih ulaganja, manjak stručnog kadra u području kibernetičke sigurnosti, izostanak standarda i zahtjeva za izvještavanjem, izostanak dijeljenja informacija o kibernetičkim rizicima te *poteškoće u integraciji i inovaciji sigurnosnih rješenja.*

Upravljanje kibernetičkim rizicima zahtijeva investicije u tehnička rješenja i tehnologiju, ali i adekvatno prenošenje znanja i provedbe obuke na zaposlenike. Izazov s kojim se poslovne organizacije suočavaju je **nedostatak resursa**, a ključno je izdvojiti **nedostatak stručnjaka** u području upravljanja kibernetičkim rizicima koji bi imali kapacitet doprinijeti jačanju kibernetičke otpornosti poslovne organizacije kojoj pripadaju. Drugim riječima, koji bi bili sposobni pratiti izloženost organizacije kibernetičkim rizicima i nuditi korisna rješenja prilagođena za dinamično okružje, što u konačnici pruža dodanu vrijednost organizaciji. Uočen je **nedostatak komunikacije** između IT podrške, podrške koja se brine o kibernetičkoj sigurnosti i nositelja drugih organizacijskih funkcija (menadžera i rukovoditelja). Korištena terminologija, nerazumljiva za ostale poslovne funkcije, zasigurno ne doprinosi razumijevanju važnosti upravljanja kibernetičkim rizicima.

Svi izvori prepreka proizlaze iz obilježja kibernetičkih rizika, pri čemu izdvajamo **inherentnu promjenjivost**. Naime, nove se prijetnje konstantno pojavljuju, a kontekst, s obzirom na promjene u tehnologiji, stalno izmjenjuje. Riječ je o **složenom području** koje zahtijeva razumijevanje tehnologije. S obzirom na široku implementaciju tehnologije u poslovne procese, kibernetički rizici utječu na gotovo svaki aspekt organizacije odnosno procesa, a upravo **sveprisutnost** čini kibernetičke rizike izazovnima za upravljanje. Nastavno na ovaj segment, nužno je ukazati na obilježje **nepredvidivosti,** jer se pojavljuju s bilo kojeg mjesta, u bilo kojem trenutku.

Bone (2017) i Kosub et al. (2015), među izazovima u postizanju učinkovitog upravljanja kibernetičkim rizicima, izdvajaju **ljudski faktor,** primarno usmjeravajući se na njihovu svijest o kibernetičkim rizicima kao prijetnji za poslovanje. Svijest odražava razumijevanje, prihvaćanje i prakticiranje sigurnosti u cijeloj organizaciji (Furnell i Thomson, 2009). Koliko je uloga čovjeka i njegova svijest o rizicima važna, upućuju Ma et al. (2009) i Hagen et al. (2008) koji podizanje svijesti izdvajaju kao najučinkovitiju mjeru sigurnosti. Takva promjena svijesti može se postići kada organizacija razvija pozitivnu kulturu prema upravljanju kibernetičkim rizicima (Li et al., 2019; Hwang et al., 2017), a promjena kulture polazi od vrha organizacije (Kannelønning i Katsikas, 2023; Chaudhry et al., 2012; Hu et al. 2012). Stoga će razvoj i kontinuirano unapređenje kulture biti zadatak menadžmenta organizacije (Reeves et

al., 2020; Li et al., 2019). Potvrđuje se utjecaj vodstva organizacije na namjeravano ponašanje zaposlenika u pogledu informacijske sigurnosti (Guhr et al., 2018), poticanje osjećaja predanosti organizacijskim politikama (Liu et al., 2020), razumijevanje usklađenosti zaposlenika sa sigurnosnim politikama (Chen et al., 2021), a određivanje svijesti zaposlenika (Parsons et al., 2014) pokazalo se ključnim za postizanje kibernetičke sigurnosti u organizacijama. Ono što se pokazuje aktualnim izazovom jest činjenica da menadžeri pokazuju nižu razinu svijesti o informacijskoj sigurnosti, stvarajući paradoks jer su obično oni ti koji imaju zadatak izgraditi i poboljšati organizacijsku kulturu (Reeves et al., 2020).

Nakon razmatranja izazova upravljanja kibernetičkim rizicima, nužno je osvrnuti se na ključnu ulogu vodstva. Kako je prethodno istaknuto, vodstvo organizacije igra središnju ulogu u oblikovanju kulture suočavanja s kibernetičkim rizicima, a njihova svijest i angažman presudni su za uspješno upravljanje tim rizicima. Zbog toga, ako vodstvo nije dovoljno informirano ili ne pokazuje odgovarajuću razinu svijesti, može doći do paradoksa u kojemu upravo oni koji bi trebali biti nositelji promjena, koče napredak.

Kao posljedica svih gore navedenih prepreka, dolazimo do točke u kojoj se ističe nedostatak razumijevanja kibernetičkih rizika odnosno izostanak svijesti o kibernetičkim rizicima kao prijetnji za poslovanje. Navedeno se u okviru ovog istraživanja, kroz prizmu vodstva organizacije posebno problematizira. Svijest na razini organizacije polazi od vodstva organizacije.

2.4. Središnja uloga čovjeka u upravljanju kibernetičkim rizicima

Rasprave o kibernetičkim rizicima u pravilu su usredotočene na tehnički aspekt. Međutim, efikasnost tehničkih rješenja određena je ulogom čovjeka kojoj je u dosadašnjim istraživanjima posvećeno manje pažnje (Pollini et al., 2022; Corradini et al., 2020; Ratchford i Wang, 2019; Nobles, 2018; Alohali et al., 2017; Anwar et al., 2017; Crossler i Belanger, 2014; Maalem Lahcen et al., 2020). Razloge za navedeno nudi Nobles (2018), koji pojašnjava kako davanje na važnosti čovjeku u okviru upravljanja informacijskim i kibernetičkim rizicima još uvijek predstavlja nekonvencionalan pristup. Slijedom navedenog, sugerira se detaljnije razmatranje uloge čovjeka u upravljanju kibernetičkim rizicima (Almansoori et al., 2023; Pretorius i Blaauw, 2022).

No, kako bi se postiglo efikasno upravljanje kibernetičkim rizicima, potrebno je razumijevanje psihologije ljudskog ponašanja, posebno u kontekstu rizika i neizvjesnosti. Čimbenici poput pristranosti, percepcije rizika i motivacije imaju značajnu ulogu u donošenju odluka koje izravno utječu na sigurnost (Badie i Lashkari, 2012). Nepredvidiva priroda ljudskog ponašanja i djelovanja čini čovjeka važnom odrednicom kibernetičke sigurnosti, a jedini način proaktivnog djelovanja u postizanju kibernetičke sigurnosti jest uzeti u razmatranje pojedinca i njegovo ponašanje (Greitzer i Hohimer, 2011). Kannelønning i Katsikas (2023), Ani et al. (2019) i Biener et al. (2015) smatraju da je čovjek najkritičnija točka u postizanju kibernetičke sigurnosti. Posljedično, brojni autori (Kadena i Gupi, 2021; Patterson i Winston-Proctor, 2019; Hadlington, 2017; Biener et al., 2015; Chaudhry et al., 2012) zagovaraju uvažavanje psihologije te potrebu za interdisciplinarnim pristupom. Takav pristup uvažava spoznaje iz područja bihevioralne ekonomije s ciljem postizanja napretka u ostvarivanju više razine kibernetičke sigurnosti. Naime, spoznaje iz bihevioralne ekonomije omogućavaju razumijevanje ljudskih odluka i pružaju alate za sistematizaciju ponašanja. Na temelju takvoga pristupa, opravdano je tražiti rješenje u nastojanju da se postigne uspješnije upravljanje kibernetičkim rizicima poslovnih organizacija (Nobles, 2018; Pfleegera i Caputa, 2012).

Stoga, u ovome se istraživanju zauzima stav da je potrebna promjena u pristupu istraživanju te davanje veće važnosti čovjeku, sukladno bihevioralnom aspektu upravljanja kibernetičkim rizicima. Takav pristup podržan je i rezultatima istraživanja Kendrick (2010) u kojemu se navodi da je ljudska pogreška doprinijela u 70 % nastalih incidenata. Dodatno, temeljem IBM-ovog izvješća iz 2014. godine, proizlazi da je ljudska pogreška bila faktor u više od 95 % svih kibernetičkih incidenata. Najučestalija pogreška bila je interakcija s kontaminiranim privitcima ili web stranicama, dok su drugi uobičajeni problemi uključivali loše odabrane lozinke, izgubljena računala te nereguliranu komunikaciju putem elektroničke pošte. Biener et al. (2015) pokazali su da su ljudske radnje, uključujući hakerske napade, pogreške i manipulacije od strane zaposlenika, bile uzrokom približno 90 % svih kibernetičkih incidenata. Verizonovo izvješće o istrazi povreda podataka za 2022. godinu pokazalo je da 82 % povreda podataka uključuje ljudski element.

Temeljem iznesenih podataka o učestalosti kibernetičkih incidenata u kojima je primarni razlog ljudski faktor, njegovu važnost u kontekstu kibernetičke sigurnosti potrebno je naglasiti. Posljedice kibernetičkog incidenta su dalekosežne, što je potvrđeno mnogim primjerima. Jedan od najpoznatijih dogodio se 2014. godine kada je Sony Pictures Entertainment bio žrtva

složenog napada putem lažnog predstavljanja ranjivoj grupi zaposlenika (*engl. Spear-phishing*) s ciljem stjecanja povjerljivih informacija. Napadači su ciljali specifične zaposlenike unutar organizacije, koristeći sofisticirane metode socijalnog inženjeringa kako bi ih naveli na otvaranje zlonamjernih e-mailova. Ova taktika bila je uspješna upravo zbog ljudskih pogrešaka. Zaposlenici kojima su poruke ciljano odaslane nisu imali potrebno znanje ili svijest da bi prepoznali pokušaj napada, a kao rezultat, napadači su ostvarili pristup mreži i izveli jedan od najvećih hakerskih napada u povijesti. Slučaj "WannaCry" iz 2017. godine primjer je napada putem ucjenjivačkog softvera (*engl. Ransomware*) koji je paralizirao računalne sustave diljem svijeta, uzrokujući milijarde dolara štete. Iako je Microsoft mjesecima prije napada izdao sigurnosnu zakrpu koja bi otklonila slabosti sustava, mnoge organizacije i osobni korisnici nisu ažurirali svoje operativne sustave što je omogućilo nastanak negativnih implikacija kibernetičkog incidenta. U nastavku je dan pregled najznačajnijih kibernetičkih incidenata čijem nastanku je doprinijelo ljudsko djelovanje.

Tablica 5. Odabrani primjeri kibernetičkih incidenata

Naziv incidenta	Opis incidenta	Troškovi o kojima je podnesen izvještaj
Equifax	Equifax, vodeća američka kreditna agencija, u 2017. godini izvijestila je o kompromitaciji osobnih podataka 143 milijuna ljudi, uključujući imena, adrese i brojeve socijalnog osiguranja. Dodatno, dogodio se neovlašteni pristup brojevima kreditnih kartica za oko 200.000 osoba.	Poslovna organizacija je pretrpjela značajne financijske gubitke, uključujući pad tržišne vrijednosti u visini 3,5 milijarde USD (smanjenje cijene dionica za 30%). Brojne istrage pokrenule su sudske sporove, čiji se trošak procjenjuju na 200 milijuna USD. Otkazi i podnesene ostavke više izvršnih direktora.
Yahoo	Tijekom 2013. i 2014. godine, Yahoo je doživio dva kibernetička incidenta, što je rezultiralo s 1,5 milijardi oštećenih korisnika. Incidenti su rezultirali kompromitacijom osobnih podataka, uključujući imena, e-mailove, telefonske brojeve, datume rođenja, te djelomične informacije o pristupnim podacima. Istraga je potvrdila da je do listopada 2017. godine	Poslovna organizacija doživjela je pad vrijednosti od 350 milijuna USD i izravne troškove od 16 milijuna USD u procesu akvizicije za. Pokrenute tužbe dovele su do troškova u visini od 37,5 milijuna USD. Posljedice je osjetio i glavni izvršni menadžer tvrtke čije se zarade u obliku bonusa nisu realizirale.

Naziv incidenta	Opis incidenta	Troškovi o kojima je podnesen izvještaj
	Yahoo revidirao svoju procjenu broja pogođenih korisnika do 3 milijarde.	
Anthem	U veljači 2015. godine, pružatelj zdravstvenog osiguranja u SAD-u Anthem suočio se s hakerskim napadom, rezultat čega je bio neovlašten pristup osobnim podacima korisnika, uključujući identifikacijske brojeve, adrese, telefonske brojeve i podatke o zaposlenju. Iako financijske i zdravstvene informacije nisu bile kompromitirane, incident je utjecao na ukupno 78,8 milijuna osiguranika i zaposlenika.	Poslovna organizacija uložila je ukupno 142 milijuna USD za forenzičko istraživanje, sanaciju i unapređenje svoje sigurnosne infrastrukture. Tvrtka je 2017. godine pristala na nagodbu od 115 milijuna USD namijenjenih podmirivanju potraživanja korisnika usluge.
eBay	U 2014. godini, eBay je objavio sigurnosni propust koji je utjecao na svih 145 milijuna korisnika. Kibernetički incident rezultirao je neovlaštenim pristupom mreži tvrtke, što je dovelo do kršenja povjerljivosti korisničkih imena i pristupnih podataka korisnika i zaposlenika.	Nakon otkrivanja sigurnosnog propusta, eBay je prijavio smanjenu aktivnost korisnika i smanjio projekcije prihoda za 2014. godinu za 200 milijuna USD. U izvješću za investitore za drugi kvartal, prijavljen je pad operativne marže za 1,9 % zbog troškova povezanih s incidentom i ulaganjima u poboljšanje mrežne sigurnosti.

Izvor: Izrada autora prema OECD (2017).

Uvažavajući navedene primjere, zaključuje se da je razumijevanjem odluka pojedinaca odnosno identificiranjem i ispravljanjem ljudskih slabosti i pogrešaka (Pollini et al., 2022), primarno kroz podizanje svijesti i edukaciju (Hu et al., 2007), moguće unaprijediti kibernetičku sigurnost organizacije.

Nedvojbeno je da svaki pojedinac unutar organizacije snosi odgovornost za postizanje kibernetičke sigurnosti. No, važno je razlikovati uloge i razinu odgovornosti između zaposlenika. Naime, iako svi zaposlenici igraju važnu ulogu u održavanju kibernetičke sigurnosti, glavni izvršni menadžeri, kao lideri, u jedinstvenom su položaju oblikovati

sigurnosnu kulturu i aktivno promicati promjene koje će osnažiti kibernetičku otpornost na svim razinama organizacije (Ahmed Shaikh i Siponen, 2023; Høiland, 2023).

Uloga menadžera postaje presudna u stvaranju okruženja u kojem se bihevioralni aspekti sigurnosti smatraju jednako važnim kao i tehnički aspekti. Kad menadžeri uspješno utječu na promjene u ponašanju zaposlenika, cijela organizacija postaje snažnija u suočavanju s kibernetičkim prijetnjama, stoga, stavljanje menadžmenta u središte istraživanja kibernetičke sigurnosti nije samo logičan korak, već i nužnost. S obzirom na izostanak istraživanja uloge vodstva organizacije u kontekstu kibernetičke sigurnosti (Sharifi, 2023; Triplett et al., 2022; Hakami i Alshaikh 2022; Guhr et al., 2018), stavljanje glavnih izvršnih menadžera u fokus smatra se opravdanim i važnim.

3. TEORIJSKI OKVIR MODELA NAMJERE UPRAVLJANJA KIBERNETIČKIM RIZICIMA

U nastavku se pruža uvid u teorijsko uporište razvoja modela namjere upravljanja kibernetičkim rizicima, pri čemu se opisuju najvažnije teorije odlučivanja u kontekstu kibernetičkih rizika te izdvaja teorija motivacije za zaštitom (*engl. Protection motivation theory – PMT*) kao odabrano teorijsko uporište. Opisana je perspektiva bihevioralne ekonomije kao nadogradnja tradicionalnih teorija odlučivanja te se, u tom smislu, u ovom dijelu govori o kognitivnim pristranostima i emocionalnim faktorima koji utječu na namjere i odluke u vezi upravljanja kibernetičkim rizicima.

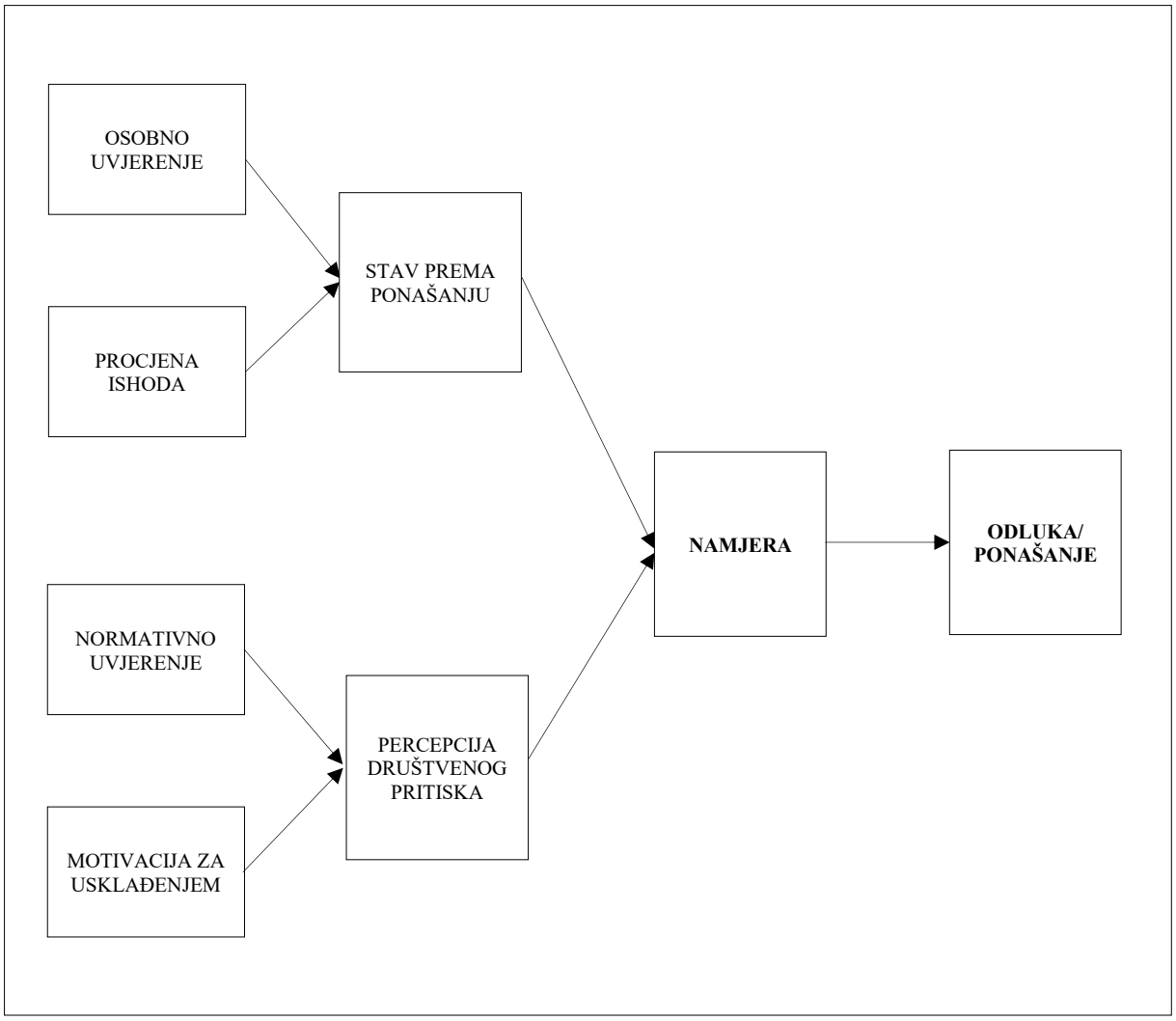
3.1. Teorije odlučivanja u kontekstu kibernetičkih rizika

Kako bi se dobio potpuni uvid u ključne čimbenike koji određuju namjeru odnosno objašnjavanju postupke u vezi upravljanja kibernetičkim rizicima, ključno je razumjeti temeljne teorije koje su osnova razumijevanja postupaka pojedinca, a time i odluka koje se tiču kibernetičkih rizika. Temeljem uvida u pregledne radove Almansoori et al. (2023), Hong i Furnell (2021), Alassaf i Alkhalifah (2021), Lu (2018) i Lebek et al. (2014), uočava se da se odluke u vezi kibernetičkih rizika mogu razmatrati pomoću različitih teorija (identificirano je preko 50 teorija), međutim, najčešći korišteni teorijski okviri u kontekstu kibernetičkih rizika i kibernetičke sigurnosti su teorije prezentirane u nastavku; t*eorija razložite akcije*, *teorija planiranog ponašanja, model prihvaćanja tehnologije* i *teorija motivacije za zaštitom*.

Teorija razložite akcije (engl. *Theory of reasoned action – TRA)*

Ključna pretpostavka **TRA** jest da su ljudska bića racionalna te da je ponašanje pojedinca primarno određeno namjerama. Sukladno Ajzen i Fishbein (1975), namjera je funkcija dvaju primarnih čimbenika: *stava prema ponašanju* (*engl. Attitude*) i percipiranog društvenog pritiska poznatog pod terminom *subjektivna norma* (*engl. Subjective norm*).

Ukoliko donositelj odluke procijeni razmatrani način ponašanja kao pozitivan (stav) te ukoliko procjenjuje da je razmatrani način ponašanja društveno poželjan, navedeno rezultira izraženijom namjerom (motivacijom) da se takav način ponašanja provede i povećanom vjerojatnosti da će se donositelj odluke (pojedinac) na razmatrani način ponašati.



Slika 4. Model temeljen na teoriji razložite akcije

Izvor: Izrada autora

Prošireni oblik TRA teorije specificira odrednice stava prema ponašanju i percepciju o društvenom pritisku. Smatra se da stav odražava uvjerenje osobe o mogućim osobnim posljedicama postupka i procjenu vjerojatnosti ishoda. S druge strane, percepcija o društvenom pritisku je funkcija uvjerenja donositelja odluke o tome kako se treba ponašati te motiviranosti donositelja odluka da se pridržava normi koje nameće okolina (Sutton, 2001). Model temeljen na *teoriji razložite akcije* prezentiran je u okviru *Slike 4*. U kontekstu istraživanja izdvajamo slikovit primjer u kojemu će donositelj odluke imati povoljan stav prema prihvaćanju upravljanja kibernetičkih rizika ukoliko vjeruje da će implementacija prakse upravljanja kibernetičkim rizicima dovesti do pozitivnih osobnih posljedica. Paralelno, ukoliko donositelj odluka smatra kako je stav okoline, u kojoj djeluje, pozitivan glede implementacije procesa upravljanja kibernetičkim rizicima, osjetit će društveni pritisak da to učini. Teorija je dobila

široku empirijsku primjenu (Moody et al., 2018; Floyd et al., 2000; Sheppard et al., 1988) te se primjenjuje u razumijevanju odluka i ponašanja u kontekstu informacijskih i kibernetičkih rizika (Siponen et al., 2014; Bulgurcu et al., 2010).

Ajzen (2020) i Fishbein i Ajzen (2011) ističu da pojedinac ne postupa uvijek sukladno vlastitim namjerama te da promjena namjere neće nužno biti popraćena promjenom ponašanja. Ključni razlog navedenoga je stupanj kontrole koju pojedinac ima nad ponašanjem. Stoga, pojedinci uspješno provode namjere ukoliko imaju potrebnu kontrolu nad ponašanjem (Fishbein i Ajzen, 2011). Sugerirana je nadogradnja TRA teorije, koja je predložena u vidu *teorije planiranog ponašanja* (Ajzen, 1991).

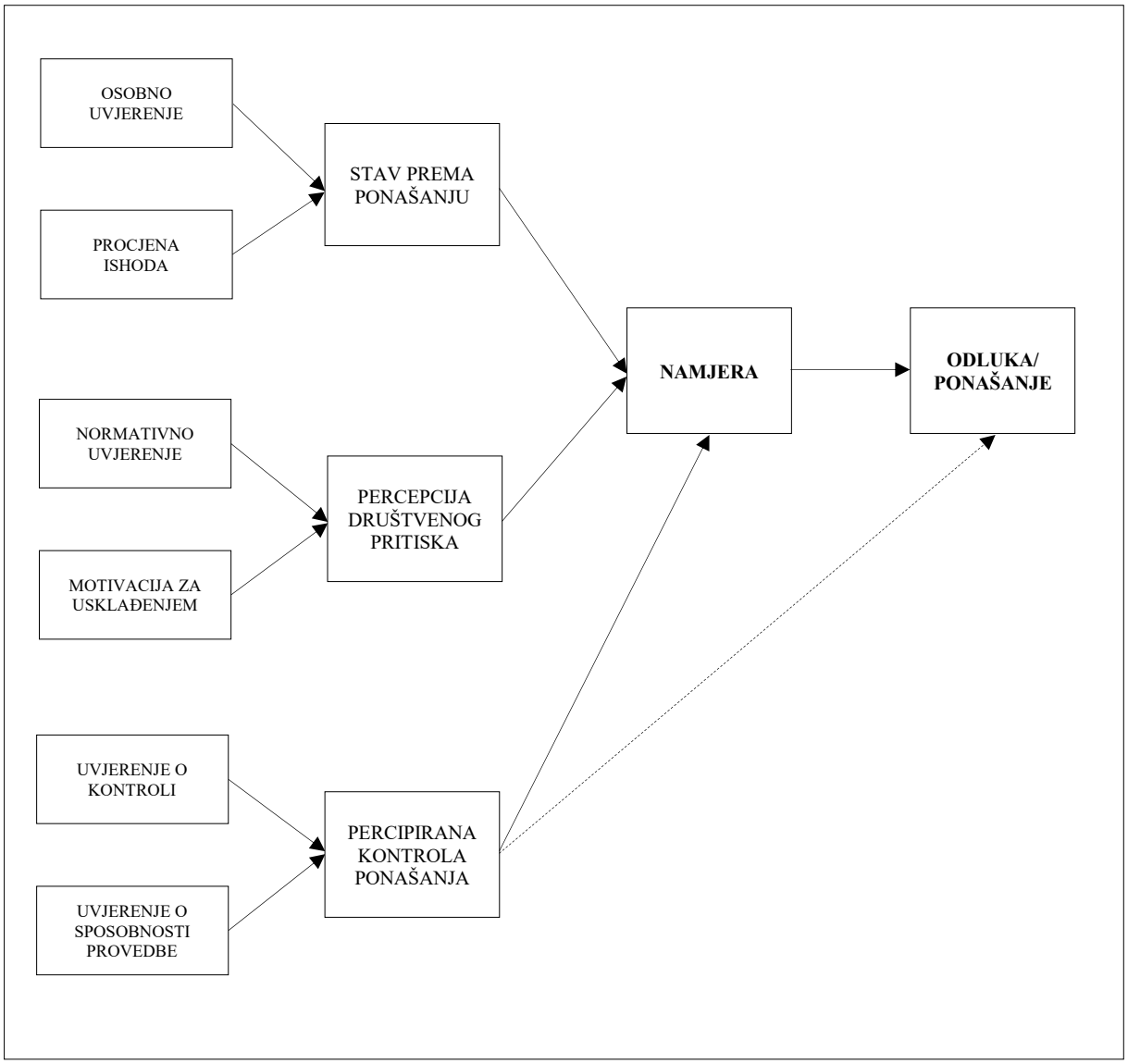
Teorija planiranog ponašanja (*engl. Theory of planned behavior – TPB*)

Iako je TRA pružila teorijski okvir u mnogim kontekstima i u više disciplina, istraživači su otkrili da bi dodatni konstrukt povećao sposobnost predviđanja ponašanja kada pojedinci percipiraju da postoje čimbenici izvan njihove kontrole (Ajzen, 1985). Naime, mnoga ponašanja ne mogu se jednostavno izvoditi po volji, za njihovu uspješnu provedbu potrebne su vještine i resursi. Da bi se prilagodio takvim ponašanjima, Ajzen (1991) je TRA-i dodao varijablu koju je nazvao **percipirana kontrola ponašanja**.

Varijabla *percipirana kontrola ponašanja* pretpostavlja percepciju o samoučinkovitosti te potrebnom angažmanu resursa, koji doprinose odnosno otežavaju konkretni oblik ponašanja - upravljanje kibernetičkim rizicima. Ajzen i Madden (1986), ovu varijablu opisuju kao percepciju pojedinca o raspoloživosti potrebnih resursa i postojanju mogućnosti za provedbu adekvatnog oblika ponašanja. Percipirana kontrola ponašanja funkcija je uvjerenja o kontroli na isti način kao što je subjektivna norma funkcija normativnih uvjerenja. Model temeljen na teoriji planiranog ponašanja prezentiran je u okviru *Slike 5*.

Ukoliko je donositelj odluka stava daje korisno uspostaviti proces upravljanja kibernetičkim rizicima, tada je njegov stav pozitivan te se posredstvom namjere povećava vjerojatnost poduzimanja aktivnosti potrebnih za implementaciju sustava upravljanja rizicima. Paralelno, ukoliko donositelj odluka percipira da okolina smatra kako je važno implementirati proces upravljanja rizicima, vjerojatnije je da će poduzeti potrebne aktivnosti uspostave sustava upravljanja rizicima.

Sve navedeno opisano je TRA teorijom, međutim, uvođenjem TPB-a uvažava se utjecaj uvjerenja donositelja odluka u pogledu sposobnosti uspostave procesa upravljanja kibernetičkim rizicima.



Slika 5. Model temeljen na teoriji planiranog ponašanja

Izvor: Izrada autora

Stoga, ukoliko donositelj odluka iskazuje uvjerenje u sposobnosti upravljanja kibernetičkim rizicima, navedeno će pozitivno utjecati na namjeru upravljanja kibernetičkim rizicima. Teorija je dobila široku empirijsku primjenu (Sommestad et al., 2015b; Sommestad et al., 2014; Ifinedo, 2014).

Tablica 6. Pregled empirijskih istraživanja značajnosti faktora utjecaja na namjere i odluke u okviru TRA i TPB teorije

Varijabla	Teorija	Očekivani smjer veze na stvarno poduzimanje aktivnosti	Članak	Značajnost	Ispitivana grupa
Stav prema ponašanju	Teorija planiranog ponašanja, Teorija razložite akcije, Teorija motivacije za zaštitom	**Pozitivan** Prilagođeno prema Ajzen (1991), pozitivan stav donositelja odluke o aktivnostima upravljanja kibernetičkim rizicima pozitivno utječe na stvarno upravljanje kibernetičkim rizicima.	Dinev et al. (2006)	Nije značajno	Studenti / IS stručnjaci
			Hu i Dinev (2007)	Značajno	Studenti / IS stručnjaci
			Herath i Rao (2009)	Nije značajno	Zaposlenici
			Zhang et al. (2009)	Značajno	Zaposlenici
			Bulgurcu et al. (2010)	Značajno	Zaposlenici
			Hu et al. (2012)	Značajno	Zaposlenici
			Ifinedo (2012)	Značajno	Manageri / IS stručnjaci
			Ifinedo (2014)	Značajno	Manageri / IS stručnjaci
			Sommestad et al. (2015a)	Značajno	Zaposlenici
Subjektivna norma	Teorija planiranog ponašanja, Teorija razložite akcije	**Pozitivan** Prilagođeno prema Ajzen (1991), subjektivna norma odnosi se na percepciju donositelja odluke u pogledu pritiska okoline da se upravlja kibernetičkim rizicima.	Dinev et al. (2006)	Značajno	Studenti / IS stručnjaci
			Hu i Dinev (2007)	Nije značajno	Studenti / IS stručnjaci
			Herath i Rao (2009)	Značajno	Zaposlenici
			Zhang et al. (2009)	Nije značajno	Zaposlenici
			Bulgurcu et al. (2010)	Značajno	Zaposlenici
			Hu et al. (2012)	Značajno	Zaposlenici
			Hovav i D'Arcy (2012)	Značajno	Zaposlenici
			Ifinedo (2012)	Značajno	Manageri / IS stručnjaci
			Ifinedo (2014)	Značajno	Manageri / IS stručnjaci
			Sommestad et al. (2015a)	Značajno	Zaposlenici
		Pozitivan Prilagođeno prema	Dinev et al. (2006)	Značajno	Studenti / IS stručnjaci

Varijabla	Teorija	Očekivani smjer veze na stvarno poduzimanje aktivnosti	Članak	Značajnost	Ispitivana grupa
Percipirana kontrola ponašanja	Teorija planiranog ponašanja	Ajzen (1991), percipirana kontrola ponašanja odnosi se na očekivanja donositelja odluke u pogledu upravljanja rizicima po stupnju spremnosti (potrebna sredstva i resursi) i sposobnosti poslovne organizacije u provedbi aktivnosti upravljanja kibernetičkim rizicima.	Hu i Dinev (2007)	Značajno	Studenti / IS stručnjaci
			Herath i Rao (2009)	Značajno	Zaposlenici
			Zhang et al. (2009)	Značajno	Zaposlenici
			Bulgurcu et al. (2010)	Značajno	Zaposlenici
			Hu et al. (2012)	Značajno	Zaposlenici
			Ifinedo (2012)	Značajno	IS stručnjaci
			Sommestad et al. (2015a)	Značajno	Zaposlenici

Izvor: Izrada autora

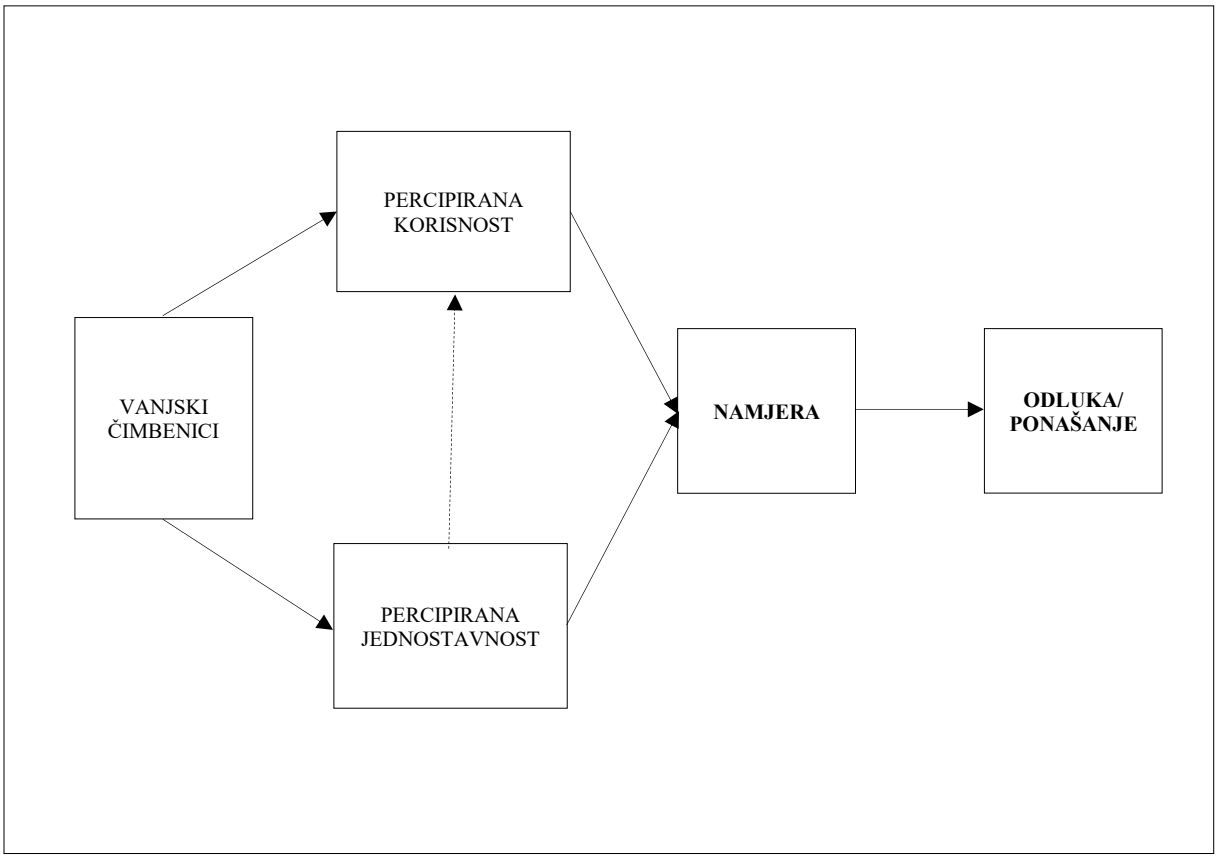
Model prihvaćanja tehnologije (*engl. Technology Acceptance Model - TAM*)

Model prihvaćanja tehnologije jedna je od vodećih paradigmi u istraživanju prihvaćanja tehnologije (Davis, 1989; Davis et al., 1989). Središnji element TAM-a je pretpostavka o snažnoj povezanosti uspjeha implementacije nove tehnologije s prihvaćanjem i korištenjem tehnologije od strane korisnika. Prema modelu, kada se suoče s novom tehnologijom, korisnici će racionalno procijeniti korisnosti i lakoću upotrebe tehnologije prije donošenja informirane odluke o njezinom prihvaćanju (Davis et al., 1989; Venkatesh, 1999).

Dok je originalni TAM pružio dubinske uvide u prihvaćanje tehnologije, kasnija istraživanja proširila su njegovu osnovu, tako je nastao model TAM2 koji nastavlja prepoznavati percepciju lakoće upotrebe kao izravan utjecaj na percepciju korisnosti (Davis et al., 1989). Postoji značajan empirijski dokaz koji sugerira da percepcija lakoće upotrebe utječe na namjere prihvaćanja tehnologije, kako izravno, tako i putem njenog utjecaja na percepciju korisnosti (Davis et al., 1989; Venkatesh, 1999). Model temeljen na teoriji prihvaćanja tehnologije prezentiran je u okviru *Slike 6*.

Teorija je dobila široku empirijsku primjenu u razumijevanju odluka i ponašanja u kontekstu informacijskih i kibernetičkih rizika (Siponen et al., 2014; Bulgurcu et al., 2010). Brojna empirijska istraživanja dokazala su da TAM dosljedno opisuje i objašnjava veliki dio ponašanja

vezanih uz kontekst informacijske i kibernetičke sigurnosti (Lu, 2018). Time se potvrđuje njegova robusnost i parasimonija (Venkatesh i Davis, 2000).



Slika 6. Model temeljen na teoriji prihvaćanja tehnologije

Izvor: Izrada autora

U kontekstu odluka vezanih za upravljanje kibernetičkim rizicima, TAM model pretpostavlja da će namjera upravljanja kibernetičkim rizicima biti usko povezana s percipiranom koristi i lakoćom provođenja aktivnosti upravljanja kibernetičkim rizicima. Ukoliko glavni izvršni menadžeri upravljanje kibernetičkim rizicima percipiraju korisnim, na način da doprinosi sigurnosti poslovne organizacije, postoji veća vjerojatnost da će ga prihvatiti i koristiti.

Ukoliko glavni izvršni menadžeri smatraju da je upravljanje kibernetičkim rizicima jednostavno primjenjivati, postoji veća vjerojatnost primjene aktivnosti upravljanja kibernetičkim rizicima. Sukladno TAM2 modelu koji predviđa kako percepcija lakoće upotrebe ima izravni utjecaj na percepciju korisnosti, u kontekstu kibernetičkih rizika, zaključuje se da će glavni izvršni menadžeri koji smatraju da je upravljanje kibernetičkim rizicima jednostavno za provođenje, vjerojatnije smatrati upravljanje kibernetičkim rizicima korisnijim.

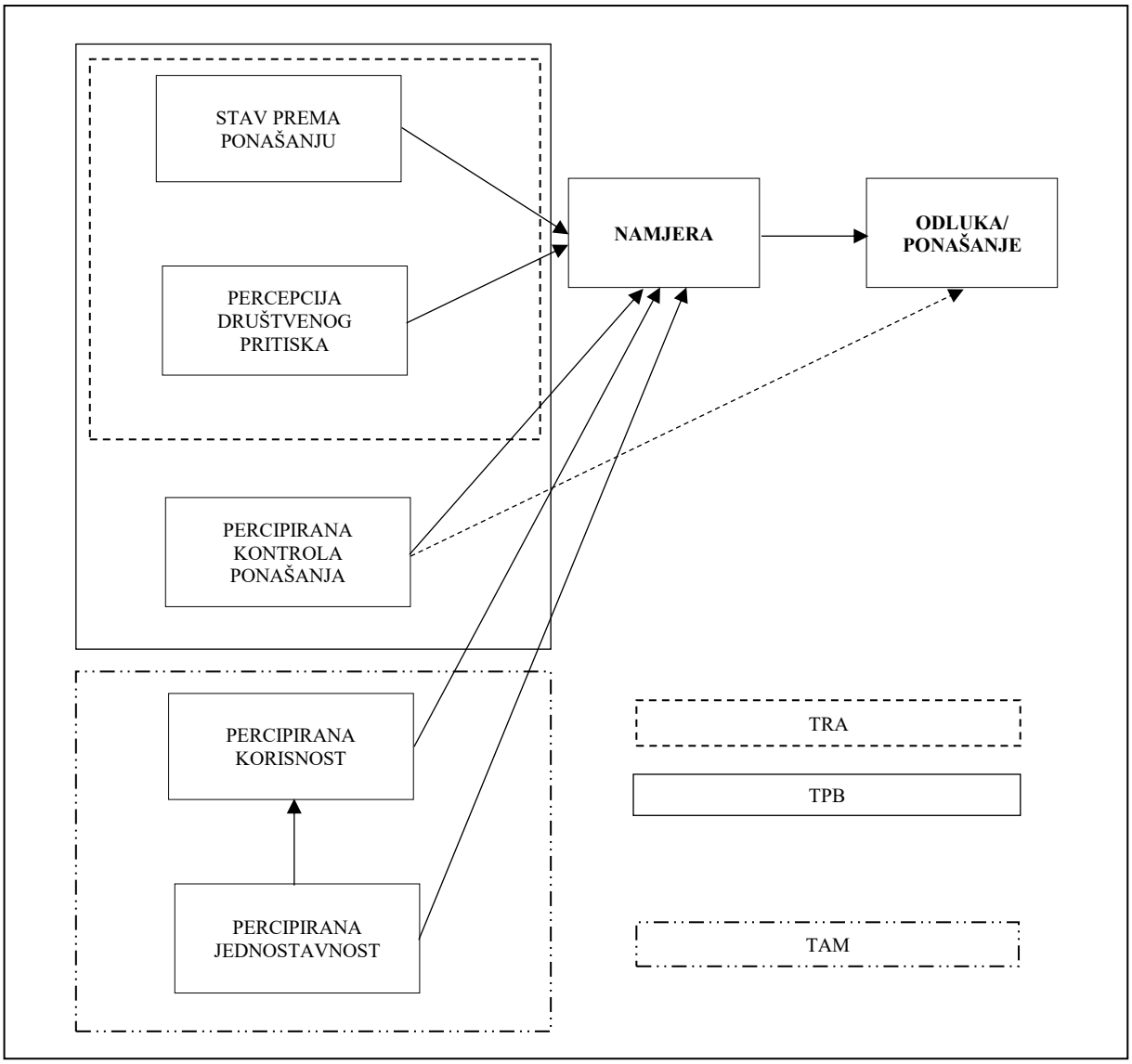
Tablica 7. Pregled empirijskih istraživanja značajnosti faktora utjecaja na namjere i odluke u okviru TAM teorije

Varijabla	Teorija	Očekivani smjer veze na stvarno poduzimanje aktivnosti	Članak	Značajnost	Ispitivana grupa
Percipirana korisnost	Teorija prihvaćanja tehnologije	**Pozitivan**	Davis et al. (1989)	Značajno	Studenti
			Igbaria et al. 1997	Značajno	Zaposlenici
			Jones (2010)	Nije značajno	Zaposlenici
			Xue et al. (2011)	Značajno	Zaposlenici
			Alharbi i Drew (2014)	Značajno	Zaposlenici
			Addae et al. (2019)	Značajno	Studenti i zaposlenici
			Abdalla et al. (2021)	Značajno	Zaposlenici
Percipirana jednostavnost	Teorija prihvaćanja tehnologije	**Pozitivan**	Davis et al. (1989)	Značajno	Studenti
			Igbaria et al. (1997)	Značajno	Zaposlenici
			Jones (2010)	Nije značajno	Zaposlenici
			Xue et al. (2011)	Značajno*	Zaposlenici
			Alharbi i Drew (2014)	Značajno	Zaposlenici
			Addae et al. (2019)	Značajno	Studenti i zaposlenici
			Abdalla et al. (2021)	Značajno	Zaposlenici

Napomena: *testiran je neizravni utjecaj

Izvor: Izrada autora

Analizom vodećih teorijskih pristupa prikazanih na *Slici 7* identificirani su ključni indikatori koji su usklađeni s **teorijom motivacije za zaštitom** kao ključnim teorijskom okvirom na koji se istraživanje naslanja.



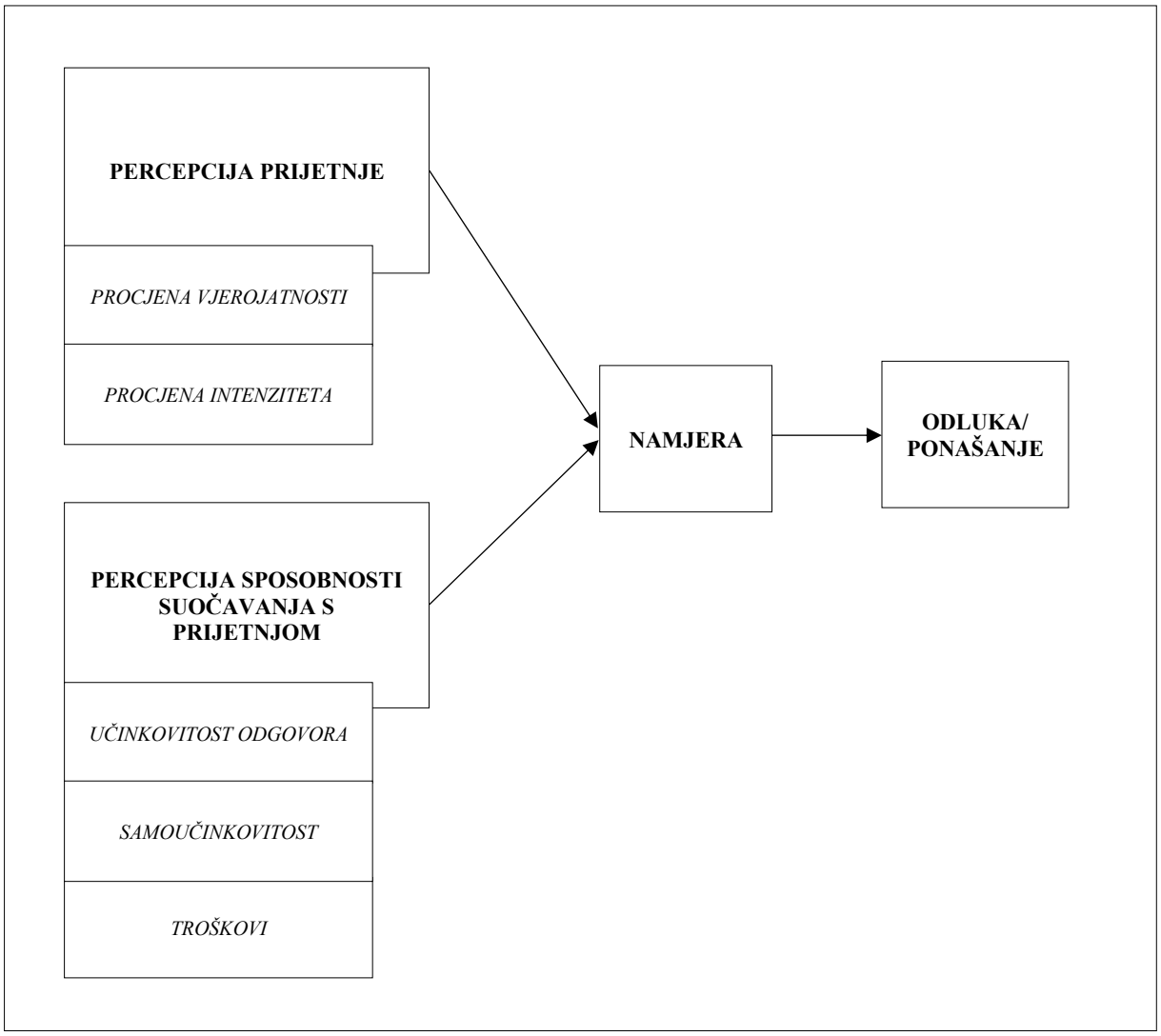
Slika 7. Kombinirani prikaz identificiranih ključnih teorija u kontekstu kibernetičkih rizika

Izvor: Izrada autora

U nastavku istraživanja ključnih teorijskih okvira kojima se objašnjavaju namjere i postupanje donositelja odluka, izdvaja se teorija motivacije za zaštitom (PMT) koja se prema zaključku Almansoori et al. (2023), Haag et al. (2021), Kianpour et al. (2019), Li et al. (2019), Boss et al. (2015), potvrđuje kao vodeći teorijski okvir u istraživanju odluka u vezi informacijske i kibernetičke sigurnosti. Riječ je o teoriji koja je primjerena donošenju odluka u organizacijama (Bode et al., 2022), a njezina primjena u kontekstu menadžerskog odlučivanja sugerira se u radu Connelly i Shi (2022).

3.2.Teorija motivacije za zaštitom

PMT objašnjava kognitivni proces kroz koji donositelj odluka prolazi kada je suočen s prijetnjom (Rogers 1983), a koji rezultira namjerom donositelja odluka da provede aktivnosti zaštite.[24]



Slika 8. Model temeljen na teoriji motivacije za zaštitom

Izvor: Izrada autora

Namjera provođenja mjera zaštite od rizika/prijetnje (adaptivan odgovor) određena je percepcijom prijetnje, u kontekstu istraživanja riječ je o **percepciji kibernetičkih rizika**, i

[24] Teorija motivacije za zaštitom (PMT) izvorno je razvijena za razumijevanje odgovora pojedinaca na prijetnje zdravlju, ali je od tada proširena i primijenjena na širok raspon konteksta, uključujući poslovne uvjete i uvjete koji se ne odnose na poslovanje.

percepcijom suočavanja, u kontekstu istraživanja riječ je o **percepciji sposobnosti organizacije u upravljanju kibernetičkim rizicima**.[25]

Percepcija prijetnje odnosi se na *percepciju učestalosti*[26] i *percepciju intenziteta* utjecaja kibernetičkih rizika na organizaciju koju donositelj odluka predstavlja. Percepcija suočavanja odnosi se na *percepciju korisnosti upravljanja* kibernetičkim rizicima (učinkovitost upravljanja), *percepciju o sposobnostima organizacije u upravljanju* kibernetičkim rizicima (samoučinkovitost primjene aktivnosti upravljanja kibernetičkim rizicima) i *percepciju troškova upravljanja* kibernetičkim rizicima (novčana sredstva, vrijeme) (Posey et al., 2011).

Pretpostavka teorije motivacije za zaštitom jest da učestalija izloženost i intenzivniji utjecaj prijetnje, drugim riječima **izraženija percepcija kibernetičkih rizika kao prijetnje,** imaju pozitivne učinke na namjeru upravljanja kibernetičkim rizicima. Nadalje, pretpostavka teorije jest da korisnost (učinkovitost) upravljanja kibernetičkim rizicima i samoučinkovitost primjene aktivnosti upravljanja kibernetičkim rizicima, suprotno od percepcije troškova, pozitivno utječu na namjeru upravljanja rizicima (Menard et al., 2017; Siponen et al., 2014; McMath i Prentice-Dunn, 2005).

Prema Johnston i Warkentin (2010), teorija motivacije za zaštitom je pouzdan i učinkovit (robustan) teorijski model u razumijevanju donošenja odluka, a prikladan je u istraživanju odluka čiji je motiv izbjeći prijetnju, odnosno njezine posljedice. Koliko je teorija motivacije za zaštitom dosad primjenjivana u području informacijske sigurnosti potvrđuju pregledni radovi Haag et al. (2021) i Boss et al. (2015). U kontekstu navedenih radova posebno se izdvaja zaključak istraživanja Haag et al. (2021) u kojem se navodi da teorija motivacije za zaštitom, primijenjena u području psihologije, može inspirirati nove i važne ideje koje mogu pomoći u stvaranju novih spoznaja u području informacijske, a time i kibernetičke, sigurnosti. Sukladno navedenom, odluke u vezi upravljanja kibernetičkim prijetnjama (rizicima) opravdano je razmatrati unutar okvira teorije motivacije za zaštitom.

[25] Boss et al. (2015) razmatra obuhvatniju nomologiju, odnosno model, koja pored navedenih varijabli, sadržava varijablu koristi od nepoduzimanja aktivnosti zaštite. Međutim, navedena varijabla iskazuje povezanost s procjenom suočavanja. Stoga se u ovom istraživanju, sukladno Cram et al. (2019), zauzima stav kako potpuna PMT nomologija nije ključna za proučavanje informacijske sigurnosti.

[26] Premda se operacionalizira kao vjerojatnost nastupa prijetnje, u literaturi se često primjenjuje termin *ranjivost*. S druge strane, strogo tehnički gledano, ranjivost jest produkt učestalosti i intenziteta razmatrane prijetnje. Iz navedenih razloga, ispravnije je koristiti termin *učestalost*.

Dok su studije temeljene na TRA i TPB i TAM naglašavale usvajanje tehnologija ili procesa, studije s PMT-om kao temeljnom teorijom uključivale su koncept zaštite od prijetnji povezanih s tehnologijama.

U sklopu analize ključnih teorijskih okvira koji se bave donošenjem odluka unutar područja kibernetičkih rizika, PMT je istaknut zbog svoje široko prihvaćene primjene i obuhvatnosti ključnih čimbenika koji pružaju uvid u motivacijske procese koji potiču pojedinca i organizacije da usvoje mjere kibernetičke sigurnosti. Primjena PMT-a u poslovnim okruženjima postala je sve relevantnija s povećanjem rasprostranjenosti i važnosti kibernetičkih i informacijskih rizika, osobito u posljednjih nekoliko desetljeća (Lu, 2018). Zaključujući raspravu o teorijskim pristupima odlučivanja u kontekstu kibernetičkih rizika, u sljedećem segmentu će se pružiti uvid u empirijske studije koje su implementirale PMT u poslovnom okruženju, što će omogućit dublji uvid u primjenu PMT-a kao teorijskog okvira koji doprinosi razumijevanju odluka/namjera upravljanju kibernetičkim rizicima u poslovnim organizacijama (*Tablica 8*).

Tablica 8. Pregled empirijskih istraživanja koja su primijenila PMT kao teorijski okvir u razumijevanju namjera i odluka u vezi kibernetičkih i informacijskih rizika u organizacijskom kontekstu

Istraživački rad	Godina	Područje istraživanja	Zemlja	Populacija	Tko je izložen riziku?
Barlette et al.	2015.	Odluke u području informacijske sigurnosti	Francuska	CEO	Organizacija
Tu et al.	2015.	Odluke u području informacijske sigurnosti	SAD	Zaposlenici	Organizacija
Burns et al.	2017.	Informacijska sigurnost u organizaciji	SAD	Zaposlenici	Organizacija
Hanus et al.	2018.	Usklađenost s politikom informacijske sigurnosti	SAD	Zaposlenici	Organizacija
Blythe i Coventry	2018.	Odluke u području informacijske sigurnosti – Program za suzbijanje zlonamjernog softvera	UK	Zaposlenici	Organizacija
Hooper i Blunt	2019.	Odluke u području informacijske sigurnosti – online	Novi Zeland	Zaposlenici	Organizacija
Li et al	2019.	Ponašanje u vezi s kibernetičkom sigurnošću	SAD	Zaposlenici	Organizacija
Rajab i Eydgahi	2019.	Usklađenost s politikom informacijske sigurnosti	SAD	Zaposlenici	Organizacija
Heidt et al	2019.	Odluke u području informacijske sigurnosti – zaštita putem lozinke	Njemačka	Zaposlenici	Organizacija
Hina et al	2019.	Usklađenost s politikom informacijske sigurnosti	Malezija	Zaposlenici	Organizacija

Istraživački rad	Godina	Područje istraživanja	Zemlja	Populacija	Tko je izložen riziku?
Aurigemma i Mattson -Studija 1	2019.	Usklađenost s politikom informacijske sigurnosti	SAD	Zaposlenici	Organizacija
Aurigemma i Mattson - Studija 2	2019.	Odluke u području informacijske sigurnosti	SAD	Zaposlenici	Organizacija
Ameen et al. - Uzorak 1	2020.	Odluke u području informacijske sigurnosti – Sigurnost pametnih telefona	SAD	Zaposlenici	Organizacija
Ameen et al. - Uzorak 2	2020.	Odluke u području informacijske sigurnosti – Sigurnost pametnih telefona	UAE	Zaposlenici	Organizacija
Vrhovec i Mihelič	2021.	Odluke u području kibernetičke sigurnosti	Slovenija	Zaposlenici	Organizacija
Ma	2022.	Odluke u području informacijske sigurnosti	Kina	Zaposlenici	Organizacija

Izvor: Izrada autora

Brojne studije pokazale su da je PMT korisna u razumijevanju adaptivnog odgovora odnosno primjenjiva u smislu razumijevanja aktivnosti zaštite (odgovor na prijetnju u poslovnom kontekstu). Percepcija o ozbiljnosti prijetnje, percepcija o ranjivosti, učinkovitosti, samoučinkovitosti i troškovima odgovora na prijetnju mogu se razmatrati u kontekstu organizacije. Stoga PMT pruža primjenjivi okvir za razumijevanje i predviđanje odgovora na kibernetičke rizike u poslovnom kontekstu te nudi temelj za tvrtke kako potaknuti zaštitno ponašanje i ublažiti potencijalne učinke ovih rizika.

3.3. Perspektiva bihevioralne ekonomije u nadogradnji tradicionalnih teorija odlučivanja

Prethodno razmotrene teorije, kojima se objašnjavaju namjere i postupanje pojedinca, uvažavaju pretpostavku da je pojedinac racionalan u svom djelovanju. Racionalnost, u klasičnom ekonomskom smislu, pretpostavlja da su pojedinci sposobni donositi optimalne odluke temeljene na potpunim informacijama. U skladu s von Neumann i Morgenstern (1944), ovakva percepcija pojedinca sugerira njegovu sposobnost racionalnog procesuiranja informacija i donošenja odluka koje imaju za cilj povećanje njegove korisnosti. Tradicionalna ekonomija bazirana je na pretpostavci da donositelji odluka posjeduju neograničeno znanje, vrijeme i sposobnosti obrade informacija (Grewal et al., 2016). Unatoč dugotrajnoj dominaciji tradicionalnih ekonomskih pretpostavki, kritike nisu izostale, a sukladno Ross (2012), tradicionalne ekonomske teorije i modeli pojednostavljuju sliku čovjeka, često zanemarujući

važne razlike između čovjeka u stvarnom okruženju i idealiziranog racionalnog agenta. Simon (1955) dovodi u pitanje pretpostavke tradicionalne ekonomske škole, s obzirom da je ljudska racionalnost određena *kognitivnim ograničenjima*, *količinom informacija* i *vremenom* koji stoji na raspolaganju za potrebe donošenja odluka. Potonje se može interpretirati kao kontekstualni utjecaj koji ima značajan utjecaj na racionalnost u procesu donošenja odluka (Dane i Pratt, 2007). Stoga, suština kritike tradicionalne ekonomske teorije proizlazi iz činjenice da tradicionalni ekonomski modeli ne uvažavaju kontekst i složenost procesa donošenja odluka.

U okviru ove rasprave, ključno je istaknuti **bihevioralnu ekonomiju koja se odmiče od modela „*homo-economicus*“[27] te razmatra kako kognitivne pristranosti, emocije, kontekst i društveno okruženje određuju ekonomske odluke (**Kahneman, 2011). Kada je riječ o bihevioralnoj ekonomiji, važno je ukazati na spoznaje **teorije dualnog procesa** (*engl. Dual Process Theory*) koja uvažava dva različita sustava za obradu informacija; prvi sustav (sustav 1) je intuitivan, vođen automatizmom i emocijama te drugi sustav (sustav 2) koji je promišljen, spor i logičan (Kahneman, 2011; Kahneman i Frederick, 2002). Dok je potonji sustav bliži tradicionalnom konceptu racionalnosti, prema Evans (2003) ograničen je kapacitetom radne memorije i povezan s općom inteligencijom, stoga je njegova primjena ograničena. Posljedično, prvi sustav često ima važnu ulogu u donošenju odluka.

Bihevioralna ekonomija integrira spoznaje iz područja psihologije u nastojanju da protumači proces donošenja odluka (Grewal et al., 2016; Dhami i al-Nowaihi, 2012). Sukladno Angner i Loewenstein (2012), ekonomske odluke su neprekidno vezane uz psihološke procese. Stoga, umjesto da se bazira isključivo na klasičnom ekonomskom načelu da pojedinci uvijek djeluju racionalno, bihevioralna ekonomija priznaje da je proces odlučivanja podložan mnoštvu kognitivnih pristranosti, emocija, društvenih utjecaja i drugih kontekstualnih obilježja koje dovode do odstupanja od racionalnog donošenja odluka (DellaVigna, 2009; Camerer i Loewenstein, 2004). Time su nalazi iz psihologije opovrgli ključnu pretpostavku tradicionalne ekonomije, ističući kako kognitivni, emocionalni i društveni čimbenici igraju ključnu ulogu u procesima ekonomskog donošenja odluka (Ariely, 2008, Loewenstein, 2004, Thaler 1999), a u tom smislu, psihologija integrirana kroz bihevioralnu teoriju postala je ključno uporište kritike tradicionalne ekonomske škole (Dhami i al-Nowaihi, 2012).

[27] Idealizirani pojedinac koji djeluje racionalno, s potpunim znanjem i u potpunosti usmjeren na maksimizaciju osobne koristi.

Bihevioralna ekonomija se od samih početaka isticala zbog cilja da bude interdisciplinarna (Mullainathan i Thaler, 2001). Naime, dok tradicionalna ekonomija ostaje unutar discipline ekonomije kako bi analizirala ponašanje i donošenje odluka, bihevioralna ekonomija koristi se spoznajama iz različitih područja društvenih znanosti, kako bi potpunije razumjela način donošenja odluka i ponašanja (Mullainathan i Thaler, 2001). Rehman (2017) prepoznaje doprinos psihologije i područja sociologije i antropologije u nadogradnji bihevioralne ekonomije. Stavljanjem naglaska na bihevioralnu osnovu, koja je je neodvojiva od psihologije, bihevioralna ekonomija nastoji objasniti pojave koje su ostale nedovoljno objašnjene u tradicionalnim ekonomskim teorijama. Bihevioralna ekonomija pruža realniji pogled na individualno i organizacijsko donošenje odluka, nego što to čini tradicionalna ekonomija (Mullainathan i Thaler, 2001).

Evolucija ekonomske misli utjelovljena kroz bihevioralnu ekonomiju ne implicira potpuno odbacivanje tradicionalne ekonomske teorije. Premda su tijekom razvoja bihevioralne ekonomije bili prisutni zagovornici revolucionarne retorike kao što su Fullbrook (2003) Heilbroner i Milburg (1995) te Ormerod (1994), koji su isticali kako bihevioralna ekonomija zamjenjuje tradicionalnu ekonomiju, veći dio autora suvremene literature o bihevioralnoj ekonomiji nastoji usavršiti, a ne potpuno revidirati, tradicionalnu ekonomsku teoriju (Rehman, 2017). S obzirom da je vrijednost tradicionalne ekonomske škole i dalje očigledna (Ross, 2012), slijedom razvoja, bihevioralna ekonomija postavljena je u ulogu komplementa tradicionalnoj ekonomskoj teoriji (Angner i Loewenstein, 2012; Camerer i Loewenstein, 2004). Takav pristup zauzet je i u kontekstu predstavljenog istraživanja.

S obzirom na stalni razvoj bihevioralne ekonomije, ovo polje ima potencijal pružiti još detaljniji uvid o kompleksnost ekonomskih odluka, a preporuka za buduće istraživanje u području razumijevanja odluka pojedinca ili organizacije jest da se u većoj mjeri koriste saznanja iz psihologije.

S obzirom na racionalnost na kojoj su utemeljeni, tradicionalni ekonomski modeli suočavaju se s izazovom prilikom tumačenja donošenja odluka pojedinca ili organizacije u uvjetima rizika i neizvjesnosti. Naime, donošenje odluka u rizičnim situacijama i neizvjesnosti nije samo vezano uz kognitivnu procjenu, već je potrebno uvažiti pojavu emocionalne reakcije (Gradinaru, 2014). Prepoznavanjem važnosti integracije spoznaja iz šireg područja društvenih znanosti, a primarno iz područja psihologije, omogućava se predviđanje sustavnih pogrešaka u procesu donošenja ekonomskih odluka (Shefrin, 2002; Rabin, 1998). Ovaj integrirani pristup nastavlja dobivati na

važnosti a analiziranje odluka u vezi upravljanja kibernetičkim rizicima moglo bi imati iznimne koristi od spoznaja koje pruža bihevioralna ekonomija.

Uzimajući u obzir spoznaje o obilježjima kibernetičkih rizika, koje narušavaju pretpostavke tradicionalne ekonomske škole, naglašavanje važnosti bihevioralne ekonomije u ovom kontekstu postaje opravdan pristup. U nastavku se, sukladno Simon (1955), izdvajaju činjenice koje prepoznaje bihevioralna ekonomija, poput kognitivnog ograničenja, količine informacija i vremena, a ovim istraživanjem u fokus postavljamo kognitivne pristranost i emocije, koje su u konačnici, između ostalog, određene i obilježjima kibernetičkih rizika.

Vremenska ograničenja često dovode do ishitrene odluke, povećane upotrebe heuristika i niže kvalitete odluke (Maule el al., 2000). Uz navedeno, vremenski pritisak može pojačati učinak kognitivnih pristranosti, dodatno smanjujući kvalitetu odluke (Ordonez i Benson, 1997). Složenost odluke, definirana brojem alternativa i neizvjesnosti, značajna je odrednica ponašanja pri donošenju odluke. Payne et al. (1993) sugeriraju da je veća vjerojatnost da će pojedinci pribjeći mentalnim prečacima (heuristikama) što su odluke složenije i što se njihov broj povećava. U poslovnom svijetu koji progresivno ovisi o digitalnim sustavima, učinkovito donošenje odluka o kibernetičkom riziku je ključno. Proces je, međutim, složen i podložan brojnim utjecajima, uključujući određene jedinstvene karakteristike kibernetičkih rizika. U odnosu na većinu tradicionalnih rizika, kibernetičke prijetnje teško se identificiraju, a još teže ih je kvantificirati. Potonje je razlog pojave kognitivnih pristranosti, pri čemu donositelji odluka mogu podcijeniti rizike (Egelman et al., 2013; Maule et al., 2000). Stoga, uvažavanje konteksta donošenja odluke doprinosi u izgradnji adekvatnog modela kojim se oslikava proces donošenja odluke u području kibernetičkih rizika, povećavajući učinkovitost u upravljanju kibernetičkim rizicima.

Istraživanja u području bihevioralne ekonomije ukazuju na to da su kognitivne pristranosti i emocije značajni čimbenici u ljudskom odlučivanju, uključujući menadžerske odluke. Naime, menadžeri prilikom odlučivanja iskazuju kognitivne pristranosti (Kahneman et al., 2019; Powell et al., 2011; Hodgkinson i Clarke, 2007; Malmendier i Tate, 2005; Hammond et al., 1998; Samuelson i Zeckhauser, 1988; Schwenk, 1984; Kahneman et al., 1982), ali i emocije za koje se potvrđuje da imaju utjecaj na proces i ishode upravljanja organizacijom (Brundin et al., 2022; Brundin i Liu, 2015).

Odstupanje od racionalnosti u donošenju odluka, posebno unutar menadžerskog konteksta, ima značajne implikacije koje se protežu kroz različite dimenzije organizacije te utječu na stratešku

određenost (Lovallo i Sibony, 2010; Malmendier i Tate, 2005), operativnu učinkovitost i, u konačnici, na ukupni organizacijski učinak. Uvid u psihološku perspektivu donositelja odluka opravdano nameće pitanje je li klasični ekonomski koncept racionalnosti adekvatan u razumijevanju namjera, odluka i ponašanja pojedinca, a istodobno se postavlja temelj za nadogradnju tradicionalnih modela odlučivanja, predstavljenih u okviru točke 3.1. Zaključuje se kako racionalno donošenje odluka ostaje aspiracijsko mjerilo, a uvažavanje pretpostavki i produkata iracionalnog te razumijevanje njihovih implikacija, bitan korak prema razumijevanju prakse donošenja odluka u poslovnom kontekstu.

3.3.1. Kognitivne pristranosti

Kognitivne pristranosti definirane su kao obrazac odstupanja koji dovodi do netočne prosudbe, nelogične interpretacije, a rezultat je postupanje koje opisujemo iracionalnim (Das i Teng, 1999; Kahneman et al., 1982; Tversky i Kahneman, 1974). Kognitivne pristranosti definiraju se kao sustavne pogreške u promišljanju koje nastaju prilikom interpretacije podataka iz okoline i utječu na zaključke, percepciju, namjere i odluke (Pohl, 2017; Kahneman i Tversky, 1972). Prema Johnson et al. (2013), mogu unaprijediti proces donošenja odluka, a prema Marshall et al. (2013), način su postizanja optimalnih odluka uzimajući u obzir ograničenja s kojima se donositelj odluka suočava.

Kognitivne pristranosti rezultat su pokušaja pojedinca da pojednostavi složenu stvarnost i olakša donošenje odluka te time očuva mentalnu energiju (Kahneman, 2011). Dodatno, proizlaze iz zablude u spoznaji, odnosno pogrešnog uvjerenja (Rhee et al., 2005). U okviru bihevioralne ekonomije, izdvaja se lista 90 najrelevantnijih kognitivnih pristranosti (Decision Lab, 2023). Prema Pryor (2023), lista broji 219 kognitivnih pristranosti. Wilke i Mata (2012) pružaju listu 11 uobičajenih kognitivnih pristranosti, a Eppler i Muntwiler (2021) dokumentiraju više od 180 kognitivnih pristranosti koje imaju utjecaj na menadžersko donošenje odluka. Bez obzira na koju se listu kognitivnih pristranosti referiramo, vrijedi daje lista kognitivnih pristranosti dinamična, tj. da se redovno proširuje (Suomala i Kauttonen, 2023; Baron, 2023). Navedeno je snažan indikator da pojedinac u svom djelovanju odstupa od potpuno racionalnog postupanja. Istraživanja Acciarini et al. (2020), Deligonul et. al. (2008), Hodgkinson et al. (1999), Busenitz i Barney (1997), Schwenk (1986) i James i Barnes (1984) potvrđuju da je riječ o važnom aspektu kojeg je potrebno razmotriti u strateškom odlučivanju čiji je nositelj glavni izvršni menadžer.

Iako mnoge kognitivne pristranosti mogu biti nadogradnja teorijskog okvira PMT-a, postoji teorijski razlog za integraciju pristranosti optimizma i pristranost dostupnosti unutar PMT-a. Naime, kognitivne pristranosti utječu na racionalnost ljudi koji djeluju u uvjetima rizika (Kahneman i Tversky, 1979). Isto proizlazi iz obilježja kibernetičkih rizika pri čemu se sukladno Simon (1972) izdvaja *neizvjesnost, nepotpune informacije i kompleksnost* te *izostanak istraživanja* navedenih pristranosti u kontekstu menadžerskih odluka u vezi kibernetičkih rizika.

Stoga, bez umanjivanja važnosti drugih pristranosti u proširenju PMT modela, nužno se ograničiti na odabrane kognitivne pristranosti koje izraženije povezujemo s percepcijom prijetnje, a koje su istodobno uvjetovane obilježjima kibernetičkih rizika. Riječ je o **pristranosti optimizma i pristranosti dostupnosti** kao središnjim pristranostima kojima se nastoji razumjeti percepcija kibernetičkih rizika kao prijetnja za poslovnu organizaciju te istodobno nadograditi tradicionalni PMT model. Pored pristranosti, ograničena racionalnost u odlučivanju može proizaći i iz emocija, stoga se uloga emocija razmatra u nastavku.

3.3.2. Emocije

Neurobiološki model donošenja odluka pojašnjava da donošenje odluka nije regulirano jednom regijom mozga, već opsežnom mrežom koja uključuje prefrontalni korteks i amigdalu, odnosno obradu emocija (Rangel et al., 2008). Psihologija potvrđuje kako emocije doprinose razumijevanju donošenja odluka (Lerner et al., 2015). Strah i anksioznost, koji su uobičajena pojava u kontekstu izloženosti prijetnji, mogu dovesti do opreznijih odluka koje navode na izbjegavanje rizika. Nasuprot tome, pozitivne emocije poput sreće često navode na donošenja odluka koje podrazumijevaju izlaganje riziku (Isen, 2001). Ljutnja se potvrđuje kao emocija koja potiče donositelja odluka na preuzimanje rizika, dok tuga, ovisno o kontekstu, različito utječe na odluke o izlaganju riziku (Lerner i Keltner, 2001).

Pojava emocija među donositeljima odluka rezultat je složene interakcije različitih čimbenika. Istraživanja iz psihologije i neuroznanosti ističu ključne uzroke koji uključuju *percipiranu razinu rizika*, *percipirani utjecaj odluke*, *osobnu izloženost* te *informacije iz okoline* (Bechara i Damasio, 2005; Loewenstein, 2000). **Percipirana razina rizika** okidač je za pojavu emocija, posebice straha. Kada donositelji odluka percipiraju visoku razinu rizika, isto uvjetuje pojavu straha i rezultira opreznijim postupanjem i donošenjem odluka koje navode na izbjegavanje rizika (Lerner i Keltner, 2001). **Percipirani utjecaj odluke** utječe na emocionalno stanje

donositelja odluka, pri čemu odluke koje nose značajne posljedice izazivaju snažne emocije, poput tjeskobe i stresa (Starcke i Brand, 2012). **Osobna izloženost** potiče pojavu emocija, donositelji odluka često doživljavaju pojačana emocionalna stanja kada rezultati njihovih odluka izravno utječu na njihov osobni ili profesionalni život (Mellers et al., 1997). **Informacije iz okoline** nesvjesno utječu na emocije, čime određuju odluke. Pozitivne informacije iz okoline dovode do odluka koje su tolerantnije na rizik (Isen, 2001). Emocije nisu izolirane pojave, već su duboko povezane s kontekstualnim čimbenicima. Navedeno posebice vrijedi za odluke povezane s kibernetičkim rizicima koje su određene unutarnjim organizacijskim i vanjskim čimbenicima.

Razumijevanje uzroka koji uvjetuju različita emocionalna stanja kod donositelja odluka neizbježno je razmotriti kod odlučivanja u kontekstu kibernetičkih rizika, a razlog je temeljen na obilježjima kibernetičkih rizika. Dodatno, odluke mogu značajno utjecati na budućnost poslovne organizacije i karijeru glavnih izvršnih menadžera.

Uvjeti pod kojima se upravlja kibernetičkim rizicima, obilježeni kompleksnošću i čestim nedostatkom informacija, prožeti su visokom razinom neizvjesnosti i utječu na odluke u upravljanju. Neizvjesnost, kombinirana s visokim ulozima povezanim sa zaštitom osjetljivih informacija i sustava, stvara okruženje pogodno za generiranje emocija (Pfleeger i Caputo, 2012).

Kada se uvaži da je fokus istraživanja na glavnom izvršnom menadžeru, koji je nositelj strateških odluka visokog uloga, a uvjeti u kojima se donose odluke i ishodi neizvjesni, navedene složene karakteristike dodatno uvjetuju pojavu emocija. Prema Loewenstein i Lerner (2003) i Huy (1999), suočavanje menadžera s odlukama koje nose ozbiljne posljedice i nepredvidljive rezultate može potaknuti emocije koje oblikuju njihov proces odlučivanja.

Sustavna analiza literature koju su proveli Alshammari et al. (2023) potvrđuje da emocije igraju ključnu ulogu prilikom donošenja odluka i ponašanja u vezi kibernetičkih rizika u organizacijskom kontekstu. Među negativnim emocijama, sram i krivicu istražili su Farshadkhah et al. (2021), dok je frustracija bila predmet istraživanja D'Arcy i Teh (2019). Emocije gubitka, koje obuhvaćaju ljutnju, emocije odvraćanja i anksioznost, bile su u fokusu studije Beaudry i Pinsonneaulta (2010). Empatiju i ljutnju istražio je Gulenko (2014), dok su Zhen et al. (2021) obuhvatili širok spektar negativnih emocija, kao što su obeshrabrenost, nelagoda i ljutnja. Chen et al. (2022b) i Burns et al. (2019) također zauzimaju pristup razmatranja šireg skupa negativnih emocije, dok su Xu et al. (2020) proučavali ljutnju i strah.

Ogbanufe i Pavur (2022) fokus su stavili na žaljenje i strah. S druge strane, postoji i niz pozitivnih emocija koje su identificirane u literaturi u kontekstu donošenja odluka. Zhen et al. (2020) opisali su sreću, uzbuđenje i zadovoljstvo. Beaudry i Pinsonneault (2010) identificirali su sreću kao emociju postignuća i uzbuđenje kao emociju izazova. Pozitivne emocije istražuju Burns et al. (2019), fokusirajući se na sreću, te Gulenko (2014) koji se koncentrira na radost.

Stoga se zaključuje da emocije mogu igrati značajnu ulogu u oblikovanju odluka, a bolje razumijevanje uloge emocije može dovesti do boljeg razumijevanja odluka u vezi upravljanja kibernetičkim rizicima (Alshammari et al., 2023). S obzirom da je riječ o nedovoljno istraženom području (Brundin et al., 2022), u nastavku će se tradicionalni PMT model proširiti za faktor kognitivnih pristranosti i emocija.

4. MODEL NAMJERE UPRAVLJANJA KIBERNETIČKIM RIZICIMA

Četvrto poglavlje pruža detaljan uvid u predloženi model namjere upravljanja kibernetičkim rizicima (teorija motivacije za zaštitom) gdje se identificiraju čimbenici koji utječu na namjeru upravljanja kibernetičkim rizicima te se daje uvid u rezultate ranijih istraživanja koji primjenjuju PMT model. Poglavlje pruža detaljniji uvid u specifične veze između varijabli koje su predviđene modelom istraživanja, što će omogućiti bolje razumijevanje načina na koji PMT može biti primijenjen u analizi kibernetičkih rizika u organizacijskom okruženju. U okviru ovog poglavlja, detaljno se obrazlažu hipoteze istraživanja. Uvažavajući pretpostavke bihevioralne ekonomije, odnosno utjecaj kognitivnih pristranosti i emocija na oblikovanje namjere, kroz pregled konceptualnog modela daje se uvid u pretpostavljene veze između identificiranih čimbenika utjecaja na namjeru upravljanja kibernetičkim rizicima.

4.1. Integracija teorije motivacije za zaštitom i bihevioralnih čimbenika u modeliranju namjere upravljanja kibernetičkim rizicima

Integracija teorije motivacije za zaštitom i bihevioralne ekonomije predstavlja temelj istraživačkog okvira. PMT pretpostavlja da intenzivnija percepcija prijetnje potiče veću namjeru upravljanja rizicima. Također, percepcija korisnosti upravljanja kibernetičkim rizicima i samopouzdanje u provedbi mjera zaštite, pozitivno utječu na namjeru (Menard et al., 2017; Siponen et al., 2014; McMath i Prentice-Dunn, 2005). Nasuprot tome, percepcija troškova ima suprotan utjecaj na namjeru upravljanja kibernetičkim rizicima. Dokazana primjenjivost PMT-a u području informacijske sigurnosti osigurava njezinu relevantnost i u kontekstu kibernetičke sigurnosti (Haag et al., 2021; Boss et al., 2015). S druge strane, bihevioralna ekonomija promatra ljudsku sklonost nesavršenome i uvažava pristup donošenja odluka koji uključuje elemente izvan stroge logičke racionalnosti, naglašavajući ulogu kognitivnih pristranosti i emocija (Tversky i Kahneman, 1974). S obzirom na relativnu novost i nepredvidivost kibernetičkih rizika, postoji nesigurnost u procjeni tih rizika koja dovodi u pitanje apsolutnu racionalnost odluka. Ova nesigurnost usmjerava donositelje odluka na oslanjanje na procjene u kojima njihovi osobni osjećaji i percepcije mogu oblikovati njihove odluke.

Uzimajući u obzir ove dvije teorije, predložene hipoteze oslanjaju se na razumijevanje načina na koji donositelji odluka procjenjuju i reagiraju na kibernetičke rizike, s obzirom na kognitivne pristranosti i emocije. Kroz ovaj integrirani teorijski pristup, namjera je obuhvatnije istražiti

složenost donošenja odluka u vezi s upravljanjem kibernetičkim rizicima i pružiti holistički pristup koji uključuje kako racionalne, tako i emocionalne komponente procesa odlučivanja.

4.1.1. Uloga kognitivnih pristranosti u percepciji prijetnje koju predstavljaju kibernetički rizici

H1 Kognitivne pristranosti glavnih izvršnih menadžera značajno utječu na percepciju kibernetičke prijetnje kojoj je izložena poslovna organizacija

Kognitivne pristranosti odnose se na sustavni obrazac odstupanja od norme ili racionalnosti, pri čemu su zaključci i procjene donositelja odluke podložni pogreškama. Pristranosti su rezultat pokušaja ljudskog mozga da pojednostavni obradu informacija. Ono što je u kontekstu predloženog istraživanja važno jest da pristranosti dovode do iskrivljenja percepcije, netočne prosudbe, nelogičnog tumačenja ili općenito iracionalnosti u djelovanju (Haselton et al., 2015).

Uključivanje kognitivnih pristranosti u PMT model omogućilo bi sveobuhvatnije razumijevanje načina na koji pojedinci oblikuju percepciju prijetnje, iskazuju namjere i, u konačnici, donose odluke. S obzirom na specifičnosti predmeta proučavanja, predložen je utjecaj dviju kognitivnih pristranosti na oblikovanje percepcije prijetnje; *pristranosti optimizma i pristranosti dostupnosti*. Pretpostavlja se da će proširenje PMT modela za odabrane varijable doprinijeti objašnjenju zašto se kibernetički rizici kod populacije glavnih izvršnih menadžera ne percipiraju kao ozbiljna prijetnja, zbog čega izostaje namjera upravljanja kibernetičkim rizicima u poslovnim organizacijama (Hina et al., 2019; Hanus et al., 2018; Tu et al., 2015).

Predloženim su modelom tradicionalne ekonomske pretpostavke obogaćene spoznajama iz područja psihologije te omogućavaju potpunije razumijevanje djelovanja donositelja odluke. Kada donositelj odluke provodi procjenu rizika, s obzirom na složenost procesa, on se u pravilu ne pridržava Bayesovih pravila i spoznaja iz statistike (Protte et al., 2020). Kada se uzima u obzir donošenje odluka u organizacijama, za očekivati je da se iste temelje na zakonima vjerojatnosti. Međutim, karakteristika kibernetičkih rizika, pri čemu izdvajamo recentnost i promjenjivost, opravdava pretpostavku da donositelj odluka ne utjelovljuje savršeno racionalnog agenta, što klasični ekonomski modeli predviđaju. Pojavu kognitivnih pristranosti ne možemo ograničiti na populaciju laika, već ju je potrebno uvažiti i kod procjena i donošenja odluka stručnjaka i iskusnih istraživača (Sjöberg, 2000; Tversky i Kahneman, 1974).

Jalali et al. (2019) sugeriraju da u budućim istraživanjima postoji prostor za propitivanje pristranosti i izvora pristranosti u menadžerskom odlučivanju. Ovaj je fenomen dobio malo pozornosti u istraživanju kibernetičke sigurnosti, što je zabrinjavajuće, budući da menadžerova pristrana procjena kibernetičkih rizika može ugroziti sposobnost organizacije da odgovori na kibernetičke prijetnje. Sukladno istraživanju Chen et al. (2021) te Vrhovec i Mihelič (2021) koji su ukazali na potrebu proširenja PMT modela za spoznaje o pristranostima, u nastavku se predlažu hipoteze H1a i H1b.

H1a Pristranost optimizma kod donositelja odluka značajno i negativno utječe na percepciju kibernetičke prijetnje kojom je izložena poslovna organizacija

U predloženom istraživanju problematizira se uloga *pristranosti optimizma* (*engl. Optimism bias ili engl. Unrealistic optimism*)[28] kao oblika kognitivne pristranosti čija zastupljenost uvjetuje nižu razinu percepcije kibernetičke prijetnje. Naime, pristranost optimizma označava sklonost uvjerenju donositelja odluka kako je manje vjerojatno da će doživjeti negativan ishod, a više vjerojatno da će doživjeti pozitivan ishod u odnosu na usporednu populaciju (Shepperd et al., 2002; Weinstein, 1980; 1989).

Pristranost optimizma jedna je od najdosljednijih, najrasprostranjenijih i najsnažnijih pristranosti dokumentiranih u psihologiji, ali i u bihevioralnoj ekonomiji (Sharot, 2011; Klein i Helweg-Larsen, 2002). Pristranost optimizma je obrazac ponašanja koji se uočava u različitim područjima ljudskog djelovanja.[29] U kontekstu kibernetičkih rizika, očekuje se manja vjerojatnost da će donositelj odluka, odnosno organizacija kojoj donositelj odluka pripada, pretrpjeti kibernetički incident u odnosu na usporedne poslovne organizacije ili u odnosu na objektivni kriterij (npr. industrijski podaci koje objavljuje nadležno sektorsko tijelo).

U mnogim slučajevima, objektivne procjene vjerojatnosti budućeg ishoda nisu lako dostupne (Rhee et al., 2012). Stoga, donositelji odluka imaju poteškoća u izražavanju vjerojatnosti

[28] Sukladno Jefferson et al. (2017), psihološka literatura identificira oblike optimistične iluzije te je potrebno razlikovati; **iluziju kontrole** koja označava pretjeranu vjeru u vlastitu sposobnost kontrole neovisnih događaja, fenomen kojeg opisuju Langer i Roth (1975), potom **iluziju superiornosti** koja označava percepciju samog sebe odnosno onoga čemu pojedinac pripada kao dominantnijeg oblika u komparaciji – može proizaći iz sposobnosti te znanja (Brown, 2012) i konačno **pristranost optimizma** koja označava sklonost ljudi da vjeruju kako je manje vjerojatno da će doživjeti negativan ishod, a više vjerojatno da će doživjeti pozitivan ishod u odnosu na usporednu populaciju (Shepperd et al. 2002).

[29] Primjerice Gassen et al. (2021) navode da je pristranost optimizma ukorijenjena među ljudskom populacijom, a problematiziraju ulogu pristranosti optimizma u upravljanju rizikom od virusa COVID-19. S druge strane, Măirean et al. (2021) istražuju utjecaj pristranost optimizma na ponašanje za upravljačem prometnih vozila, a navedena lista problematiziranja uloge pristranosti optimizma može se bitno proširiti.

određenim brojem (Weinstein i Klein, 1996). Razlikujemo komparativni pristrani optimizam i apsolutni pristrani optimizam. Naime, komparativni pristrani optimizam označava situaciju u kojoj donositelj odluke procjenjuje vlastite izglede boljima od izgleda usporedne populacije, drugim riječima, očekuje da su pozitivni ishodi vjerojatniji, a negativni ishodi manje vjerojatni za organizaciju kojom upravlja u odnosu na druge organizacije. Apsolutni pristrani optimizam označava procjenu rizika donositelja odluka koja je nerealno optimistična u usporedbi s objektivnim kriterijem, poput aktuarske procjena rizika (Shepperd et al., 2013). Obilježja kibernetičkih rizika od kojih se posebno ističe nedostatak podataka, a ukoliko postoje, njihova manja produktivna snaga uslijed izraženih tehnoloških promjena, sugerira usmjerenje na komparativni pristrani optimizam što će slijediti i način operacionalizacije navedene varijable.

Pristranost optimizma razlikuje se od optimizma kao osobine ličnosti, gdje potonja označava generalnu tendenciju iščekivanja pozitivnog ishoda, a poznata je pod nazivom dispozicijski optimizam (Carver et al., 2010). Naime, generalna tendencija iščekivanja pozitivnog ishoda ne uključuje predviđanja u vezi konkretnih događaja kao što je, u okviru ovog istraživanja, postavljen kibernetički rizik.

Međutim, ono što je posebno važno za istaknuti, optimistična pristranost ima tendenciju pojavljivanja u sprezi s rizicima male vjerojatnosti i onima s kojima donositelj odluka ima malo iskustva (Weinstein, 1987) i o kojima ima malo znanja (Weinstein, 1989). Haltinner et al. (2015), Cho et al. (2010) i Campbell et al. (2007) potvrđuju da pojedinci smatraju da su drugi više izloženi kibernetičkim rizicima nego oni sami. Dodatno, Weinstein (1987) uočava da pojedinci iskazuju veću pristranost optimizma u situacijama koje odlikuje neizvjesnost.

Shepperd et al. (2002) ističu višestruke razloge zbog kojih nastupa pristranost optimizma, a među njima se ističu nepotpune informacije o populaciji s kojom se donositelj odluka uspoređuje i sklonost uspoređivanju s populacijom kod koje je vjerojatniji nastup neželjenog ishoda, čime se precjenjuje rizik druge strane. Chambers i Windschill (2004) ističu da se ljudi u pravilu boje negativnih događaja i njihovih posljedica, a uz iskazivanje pristranog optimizma postiže se svojevrsna utjeha, budući da se relativizira činjenica o izloženosti riziku. Warkentin et al. (2013) ističu pitanje vanjskog podražaja kao faktora koji utječe na prisutnost pristranosti optimizma, a među primjerima istaknut je način komunikacije menadžera koji može utjecati na pojavu pristranosti optimizma kod zaposlenika. Lei et al. (2023) problematiziraju nedovoljno znanje koje utječe na iskrivljenu prosudbu o rizicima, pri čemu uvode varijablu pristranost optimizma. Campbell et al. (2007) povezuje prisutnost optimizma s prosudbom o vlastitim mogućnostima kontrole, ali i poželjnosti iskustva.

Pristranost optimizma učestalija je pojava kod razmatranja prijetnje (negativan događaj), no što je slučaj s pozitivnim događajem, primjer čega je ishod igre na sreću. Time se zaključuje kako donositelji odluka više podcjenjuju vlastite rizike, nego što precjenjuju izglede za uspjeh.[30] Međutim, posljedice koje proizlaze iz dviju vrsta pogrešnih procjena prilično su različite (Shepperd et al., 2002). Precjenjivanje izgleda za uspjeh dovodi do osjećaja blagostanja, a ono što je za predloženo istraživanje važno jest da podcjenjivanje vjerojatnosti nastupa prijetnje može dovesti do izlaganja riziku ili zanemarivanja mjera opreza.

U cilju pojašnjenja uloge pristranosti optimizma, u okviru predloženog istraživanja, potrebno je istaknuti kako je do sada problematizirana veza između pristranosti optimizma i percepcije rizika, pri čemu se predviđa kako pristranost optimizma determinira percepciju prijetnje. Međutim, u kontekstu upravljanja rizicima, ne u području informacijskih ili kibernetičkih rizika, izdvajamo studiju Oakley et al. (2020) koja u okviru PMT teorije pridodaje pristranost optimizma ulozi determinante percepcije rizika, a veća se pristranost u optimizmu povezuje s nižim stupnjem percepcije rizika. Costa-Font et al. (2009) razmatraju tvrdnju kako pojedinci s izraženijim pristranostima optimizma bilježe nižu razinu percepcije rizika, što se djelomično potvrđuje. Istraživanja izvan područja kibernetičkih rizika potvrđuju da pristranost optimizma determinira percepciju rizika.[31]

U kontekstu upravljanja informacijskim rizicima, Chen et al. (2021) potvrđuju kako pristrano optimistični pojedinci iskazuju manji stupanj uvjerenja da će se negativni ishodi dogoditi upravo njima. Ranija istraživanja Rhee et al. (2012; 2005) potvrđuju kako su rukovoditelji informacijskih sustava iskazivali pristranost optimizma, odnosno smatrali su da je rizik informacijske sigurnosti njihovih tvrtki znatno niži od rizika njihovih poslovnih partnera, ali i općeg tržišta.

Integracija pristranosti optimizma u okviru PMT modela sugerirano je proširenje kojim se iskazuje kako iracionalnost utječe na procese razmišljanja. Naime, pristranost optimizma razlog je zbog kojeg ljudi umanjuju razinu percipirane prijetnje (Chen et al., 2021a). Definirajući pristranost optimizma kao razliku u prosudbi između rizika s kojim se suočava organizacija i rizika s kojim se suočava usporedni subjekt, pretpostavlja se da će donositelji odluka koji su

[30] U psihologiji se navedena pojava opisuje učinkom valencije (Gouveia i Clarke, 2001; Shepperd et al., 2002).

[31] U kontekstu investicijskog odlučivanja, izdvaja se rad Chen et al. (2022), u kontekstu upravljanja rizikom od virusa izdvaja se studija Park et al. (2021), a u kontekstu upravljanja motornim vozilima izdvaja se studija Măirean et al. (2021) kod kojih se potvrđuje da optimistično pristrani pojedinci smatraju da je njihov rizik niži.

pristrano optimistični iskazivati manju razinu percipirane prijetnje od kibernetičkih rizika. Tablični pregled istraživanja u vezi pristranosti optimizma vidljiv je u *prilogu (Prilog D)*.

U okviru predstavljenog istraživanja cilj je pružiti dodatnu dimenziju pristranosti optimizma na način da se uvaži stav donositelja odluka u vezi dugoročnih trendova. Način kako donositelji odluka u organizaciji opisuju svoj stav (pristup koji zauzimaju) u vezi pretpostavljenog scenarija za koji je predviđen izostanak negativnog iskustva, pružit će uvid u dimenziju pristranosti optimizma i ponuditi odgovor na pitanje: nastupa li pristranost optimizma zbog sklonosti uvjerenju kako će se povoljni ishod u ranijem razdoblju (povijesni obrazac događanja) nastaviti u budućnosti?

Pretpostavka je da će donositelji odluka koji iskazuju uvjerenje da će se pretpostavljeni povijesni obrasci preslikati u budućnosti, ujedno biti pojedinci koje opisujemo kao pristrano optimistične. Razmatrana zabluda posebno je važna u kontekstu kibernetičkih rizika koji postaju svakim danom sve značajnija prijetnja poslovanju. Time zauzimanje stava kako uočen obrazac u ranijem razdoblju, u konkretnom slučaju pozitivan ishod, doprinosi stvaranju slike o kibernetičkim rizicima koja odstupa od realne.

Očekuje se kako će pristrano optimistični donositelji odluka podcijeniti kibernetičke rizike kao prijetnju za poslovanje. S obzirom da je razmotrena isključivo pozitivna dimenzija u razmotrenom scenariju (izostanak negativnog ishoda) opravdano je govoriti o pristupu koji doprinosi razumijevanju dodatne dimenzije pojave koju prepoznajemo kao pristranost optimizma. Međutim, pristranost optimizma u konkretnom slučaju, pored uobičajenog pristupa koji predviđa komparaciju s usporednim poslovnim subjektom, proizlazi iz komparacije položaja organizacije u različitim točkama u vremenu. U ovom dijelu istraživanja ne razmatraju se izravna iskustva s kibernetičkim incidentima kao preduvjetom za formiranje percepcije o rizicima. Naime, ovdje je fokus na procjeni rizika baziranoj na pretpostavkama i uvjerenjima, koja može ili ne mora odražavati realnu kibernetičku prijetnju. Navedeno omogućava uvid kako optimistična pristranost može utjecati na procjenu kibernetičkih rizika unutar organizacije, neovisno o konkretnim iskustvima.

Pregledom literature uočava se da je razmatrana dimenzija u mjerenju pristranosti optimizma neaktualizirana, što uz ranije istaknute specifičnosti kibernetičkih rizika potvrđuje nužnost istraživanja uloge ove dimenzije pristranosti optimizma u oblikovanju percepcije o kibernetičkim rizicima i neizravne uloge koju ima u oblikovanju namjere upravljanja kibernetičkim rizicima. Tablični pregled istraživanja u vezi s razmatranom dodatnom

dimenzijom pristranosti optimizma prepoznajemo pod nazivom *zabluda povoljnog povijesnog ishoda* (*engl. Hot hand fallacy*) koja je istraživana izvan konteksta kibernetičkih rizika što je vidljivo u okviru *priloga (Prilog E i F).*

Zabluda povoljnog povijesnog ishoda identificirana je kod donošenja poslovnih odluka koje se tiču investiranja[32], a predloženim istraživanjem njihova se primjena stavlja u kontekst procjene i upravljanja kibernetičkim rizicima. Istraživanje Lin (2019) sugerira kako zabluda povijesnog ishoda ima primjenu na širi kontekst te su, u konkretnom slučaju, financijske odluke motivirane iskustvom bez gubitka.

H1b Pristranost dostupnosti kod donositelja odluka značajno pozitivno utječe na percepciju kibernetičke prijetnje kojom je izložena poslovna organizacija

Pristranost uvjetovana nedavnim vlastitim iskustvima i informacijama (pristranost dostupnosti) (engl. *Recency bias*) je kognitivna pristranost koja se odnosi na sklonost pojedinca pridavanju veće važnosti nedavnim iskustvima ili informacijama iz okoline prilikom procjena budućih događaja ili donošenja odluka. U odnosu na hipotezu H1a koja razmatra stavove donositelja odluka u odnosu na pretpostavljene (hipotetske) uvjete o izostanku nastupa kibernetičkih rizika, hipoteza H1b pruža drugačiju perspektivu. Njome se propituje uloga stvarnih, nedavnih negativnih iskustava te nedavnih informacija iz okoline, za što se pretpostavlja da će utjecati na percepciju kibernetičke prijetnje. Donositelj odluka koji je sklon pristranosti nedavnog negativnog iskustva precjenjuje objektivnu vjerojatnost pojavljivanja i utjecaj događaja, drugim riječima, nastup razmatranog događaja smatra vjerojatnijim događajem u budućnosti. Takav fenomen proizlazi iz heuristike dostupnosti[33] (Ma et al., 2014), čija je pretpostavka da donositelji odluke istu temelje, ne na potpunim informacijama, već na lako dostupnim informacijama (Tversky i Kahneman, 1974). U okviru predloženog istraživanja, usmjerenje je na informacijama koje proizlaze iz vlastitih iskustava, ali i informacijama koje su popraćene u medijima, industrijskim izvještajima te zbivanjima u okviru tržišta na kojima organizacija djeluje, a kojih se lako sjetiti. Usmjerenjem na pristranost dostupnosti prihvaća se nedavno vlastito iskustvo i nedavne informacije kojima je donositelj odluka bio izložen, kao čimbenik koji utječe na percepciju kibernetičkih rizika kao prijetnje.

[32] Primjerice, investitori ulažu sredstva u one fondove čiji su profesionalni upravitelji bilježili uspješne rezultate, vjerujući da će se uspjeh upravljanja fondom nastaviti (Barber et al., 2005). Konkretno, ljudi uglavnom kupuju fondove koji su u prošlosti bili uspješni, vjerujući u sposobnost menadžera da produže rekord uspješnosti.

[33] Heuristika dostupnosti stavlja naglasak na događaje kojih se lakše prisjetiti, međutim, nužno se ne temelji na vlastitom iskustvu te naglašeno ne usmjerava važnost na povijesni ishod.

Ono što karakterizira pristranost dostupnosti je oslanjanje na uzorak male veličine za kojeg se pretpostavlja da je reprezentativan. Kibernetički rizici, kao recentna kategorija rizika čija su obilježja promjenjiva, ograničava oslanjanje na uzorak većih razmjera, što ukazuje na moguću pojavu pristranosti dostupnosti.

Važno je istaknuti da je ova kategorija pristranosti, iako je riječ o pristranosti koja u pravilu dovodi do odluka koje odstupaju od optimalnih, nije nužno negativna, jer može potaknuti vodstvo organizacije na razmatranje kibernetičkih rizika kao ozbiljnije prijetnje. U kontekstu kibernetičke prijetnje, s obzirom na istaknuta obilježja kibernetičkih rizika, nedavne informacije mogu biti važnije od informacija koje proizlaze iz udaljenije prošlosti u stvaranju adekvatne procjene prijetnje, a u konačnici i u iskazivanju namjera i donošenju odluka. S obzirom na uvodno spomenute karakteristike rizika, očekuje se da ovaj oblik pristranosti neizravno, posredstvom povećane percepcije prijetnje, dovodi do organizacijskih promjena u upravljanju kibernetičkim rizicima i to na način da ih potiče.

Zaključuje se kako donositelji odluka, pod utjecajem pristranosti dostupnosti, daju prednost recentnim događajima ili informacijama, umanjujući značaj onih iz prošlosti. Nastupa svojevrsno odbacivanje dugoročnih trendova i povijesnog konteksta, što u slučaju kibernetičkih rizika ne mora nužno značiti nepovoljnu situaciju za organizaciju. U kontekstu kibernetičkih rizika, pristranost dostupnosti može navesti donositelje odluka da naglase važnost nedavnog kibernetičkog incidenta te posljedično većem stupnju procjenjuju kibernetičke rizike kao prijetnju za poslovanje organizacije. Međutim, istodobno se problematizira stvarno iskustvo poslovnih organizacija s kibernetičkim rizicima, pri čemu se u istraživanju očekuje potvrda niske razine iskustva s kibernetičkim incidentima.

Pored činjenice kako osobna iskustva imaju značajnu težinu u percepciji rizika (Lawrence et al. 2014; Terpstra et al. 2009), studija Ardaya et. al. (2017) naglašava ulogu informacija koje potječu iz bliske okoline, pri čemu izdvajaju ulogu obitelji i prijatelja u oblikovanju percepcije rizika. U kontekstu predstavljenog istraživanja, fokus je na poslovnoj okolini, stoga se izdvaja važnost informacija koje donositelji odluka dobivaju iz izvještaja za industriju, ali i prenesenih iskustava poslovnih organizacije koje su pretrpjele kibernetički rizik. Među neizravnim iskustvima potrebno je izdvojiti i informacije u medijima koje mogu pridonijeti pristranoj procjeni rizika (Morgan et al., 2001). Prema konceptu heuristike dostupnosti, donositelji odluka često donose procjene rizika na temelju informacija koje su im najdostupnije ili najsvježije u pamćenju, a ne nužno na temelju stvarnih ili objektivnih činjenica. U ovom kontekstu, pretpostavka je da mediji imaju značajnu ulogu, jer oblikuju i pružaju informacije. Zaključuje

se da je utjecaj neizravnih iskustava na percepciju rizika značajan i višestruk, što sugerira potrebu za razmatranjem u okviru istraživanja rizika (Lechowska et al. 2018). Ovim istraživanjem uvažava se pretpostavka da je percepcije rizika složena kategorija te da je oblikovana izravnim i neizravnim iskustvima koja su stalno posredovana osobnim, društvenim i medijskim kanalima. Posljedično, oba oblika iskustava pridonose sveobuhvatnijem razumijevanju percepcije rizika, naglašavajući nužnost njihovog istraživanja.

Dosadašnja istraživanja provedena su izvan konteksta kibernetičkih rizika i menadžerskih odluka, što upućuje na postojanje značajnog prostora za daljnje istraživanje i opravdanost istoga u ovoj specifičnoj domeni. Potreba za takvim istraživanjem posebno je izražena s obzirom na rastući utjecaj kibernetičkih rizika na poslovno odlučivanje. U ovom radu izvorna je literatura, iako neizravno povezana s kibernetičkim rizicima, korištena kao temelj za postavku hipoteze.

4.1.2. Utjecaj percepcije prijetnje na namjeru upravljanja kibernetičkim rizicima

Percipirana učestalost odnosi se na procjenu vjerojatnosti da će se kibernetički incident (prijetnja) realizirati pod uvjetom da se ne provodi aktivnost upravljanja kibernetičkim rizicima, odnosno da se ne provodi adaptivno ponašanje (Tu et al., 2015; Lee i Larsen, 2009).

U empirijskim istraživanjima temeljenim na PMT-u, uočeni su nedosljedni rezultati o povezanosti učestalosti pojavljivanja prijetnje i namjere upravljanja prijetnjom (adaptivnog ponašanja). Primjerice, Ifinedo (2012) Siponen et al. (2014) potvrđuju kako **percipirana vjerojatnost** nastupa kibernetičkog incidenta motivira na postupanje koje je sukladno politikama kibernetičke sigurnosti, s druge strane, do danas je čitav niz studija kod kojih izostaje potvrda rezultata prethodnih istraživanja. U *Prilogu G,* izložen je pregled studija od 2015. godine do danas koji obuhvaća istraživanja čiji je teorijski okvir utemeljen na PMT teoriji. Dodatno, fokus navedenih istraživanja je ponašanje u vezi informacijskih ili kibernetičkih rizika unutar organizacija. Temeljem pregleda rezultata empirijskih istraživanja, potvrđuje se izostanak konsenzusa o utjecaju percipirane učestalosti na namjeru upravljanja rizicima.

Percipirani intenzitet prijetnje predstavlja procjenu ozbiljnosti negativnog utjecaja kibernetičkih rizika (Tu et al., 2015; Lee i Larsen, 2009). U situaciji kada glavni izvršni menadžer percipira veći intenzitet negativnog utjecaja kibernetičke prijetnje, kao odgovor na intenzitet prijetnje, isti iskazuje veću namjeru prilagođavanja svojeg postupanja, odnosno opreznijeg postupanja i poduzimanja protumjera (Johnston i Warkentin, 2010). Prema Siponen

et al. (2014), percipirana ozbiljnost prijetnje motivirat će na opreznije postupanje, odnosno, prema Herath i Rao (2009) i Bulgurcu et al. (2010), pojedinac je manje oprezan ako percipira manji intenzitet prijetnje. Kako ističe Schuetz et al. (2020), ne postoji konsenzus u pogledu rezultata empirijskih istraživanja teze da je namjera određena ozbiljnošću prijetnje.

Prema Liang i Xue (2010), pojedinac uočava prijetnju tek kada je ranjiv, odnosno kada su posljedice prijetnje ozbiljne, a vjerojatnost nastupa prijetnje izgledna. Stoga, ukoliko glavni izvršni menadžer percipira da je organizacija ranjiva na kibernetičku prijetnju, kod istog se javlja izraženija namjera upravljanja kibernetičkim rizikom. Tu et al. (2015) razmatraju percepciju učestalosti i percepciju intenziteta kao jedinstvenu vrijednost[34] koja odražava ukupnu percepciju prijetnje. Potonje je sukladno Liang i Xue (2009) koji ističu važnost multiplikativnog utjecaja.

U pregledu literature o menadžerskoj perspektivi preuzimanja rizika, March i Shapira (1987) sugeriraju da je percepcija menadžera pod izraženijim utjecajem potencijalne veličine gubitka u odnosu na vjerojatnost gubitka, što dovodi do zaključka da menadžeri iskazuju odbojnost prema gubitku. Također, sugeriraju postojanje potencijalne prisutnosti odbojnosti prema žaljenju. Potonja relacija potvrđuje se i u istraživanjima Keil et al. (2000) te Reynolds i Nelson (2007).

Iako se PMT model primjenjivao u području informacijske sigurnosti na razini organizacija, rezultati su nedosljedni i kontradiktorni. Objašnjenje možemo pronaći u istraživanju Sommestad et al. (2015b) u kojem se istraživanja kategoriziraju prema tri obilježja: ***dobrovoljnost, specifičnost i cilj prijetnje,*** temeljem kojih se mogu objasniti razlike u značaju utjecaja ključnih varijabli PMT-a na zavisnu varijablu. Počevši od prvog kriterija, zaključak je kako je percepcija prijetnje izraženije povezana s namjerama kada je djelovanje pojedinca određeno unutar organizacijskim politikama i pravilima. Dodatno, pokušaj objašnjenja nedosljednih rezultata studija možemo potražiti u pitanju razlikovanja zavisne varijable koja može biti generalnog oblika (primjerice pridržavanje politika kibernetičke sigurnosti) odnosno konkretnog oblika (primjerice primjena softvera za enkripciju podataka). Sommestad et al. (2015b) u svojem detaljnom pregledu literature zaključuju da istraživanja koja za zavisnu varijablu primjenjuju specifičnu aktivnost/odluku/ponašanje bilježe bolja svojstva (veći stupanj objašnjene varijance). Kako je u velikom broju studija percepcija vjerojatnosti, odnosno percepcija intenziteta, mjerena na način da su istodobno usmjereni na pitanja o prijetnjama

[34] Operacionalizira se kao produkt mjera dvaju varijabli (varijabla učestalosti i varijabla intenzitet).

kojima su izložene osobe (ispitanici) odnosno o prijetnjama kojima su izložene organizacije, vidljiv je problem nekonzistentnosti u definiranju objekta koji je izložen prijetnji. Naime, objekt koji je izložen prijetnji nije jasno određen u svim istraživanjima. Međutim, kada se napravi jasna razlika u načinu mjerenja ključnih varijabli prijetnje, zaključuje se kako studije koje se bave percepcijom prijetnje kojima je izložen pojedinac, a ne organizacija, imaju snažniju povezanost s namjerom za adaptivnim ponašanjem (zaštitom/upravljanjem rizicima). Odgovor na ovaj izazov nudi se predloženim istraživanjem i to na način da se istraživanje provodi isključivo nad populacijom ključnih izvršnih menadžera koji, u odnosu na ostalu populaciju predstavnika poduzeća, bilježe veću izloženost, a time i veću usklađenost osobnih i poslovnih interesa.

U nastavku se iznosi pregled novijih istraživanja čiji su rezultati objavljeni nakon važnog meta istraživanja Sommestad et al. (2015b). Spoznaja o utjecaju triju kriterija, *dobrovoljnosti, specifičnosti i cilja prijetnje,* na uspješnost razumijevanja odluka/ponašanja te istaknuti ciljevi istraživanja, utjecali su na probiranje ključnih istraživačkih radova koji su istaknuti u *Prilogu G*. Naime, obuhvaćena su istraživanja koja razmatraju *osnovni PMT model*, pri čemu se *isključuje postojanje medijatora (neizravne veze između percepcije prijetnje i namjere adaptivnog odgovora)* i gdje se *fokus stavlja na odluke u kontekstu organizacija* (dominiraju istraživanja nad zaposlenicima, stručnjacima u području informacijske sigurnosti, a tek se jedno istraživanje bazira na uzorku glavnih izvršnih menadžera srednjih i malih poduzeća). Uspoređujući predstavljeno istraživanje i prethodno provedeno istraživanje Barlette et al. (2015), ključne razlike odražavaju se u metodološkom pristupu i opsegu istraživanja. Ranije istraživanje temeljilo se na uzorku glavnih izvršnih menadžera koji upravljaju isključivo malim i srednjim poduzećima. U ranijem istraživanju, analiziran je osnovni model teorije motivacije za zaštitom (PMT) bez integracije elemenata biheviooralne ekonomije, kao što su kognitivne pristranosti i emocije. Dodatno, zavisna varijabla u ranijem istraživanju nije u potpunosti razmatrala složenost koncepta zavisne varijable, posebno u kontekstu upravljanja rizicima, kao dijela šireg poslovnog procesa, temeljem čega se zaključuje da zavisna varijabla nije bila obuhvatna. Konačno, istraživanje je uključivalo manji broj ispitanika.

Li et al. (2019), Burns et al. (2017) i Sommestad et al. (2015b) i uspoređuju važnost utjecaja dvaju procesa, važnost utjecaja **procijene prijetnje** (percepcija kibernetičkih rizika) uspoređuju s važnosti utjecaja **procijene suočavanja** (percepcija sposobnosti upravljanja kibernetičkim rizicima) na namjeru adaptivnog ponašanja. Dolaze do zaključka kako percepcija prijetnje ima slabiju relativnu značajnost na namjeru upravljanja u odnosu na percepciju

suočavanja (percepcija suočavanja će biti razmotrena u okviru hipoteze 3). To je bio motiv uvođenja različitih varijabli u ulozi medijatora između percepcije prijetnje i namjere adaptivnog ponašanja.[35] Ono što u istraživanjima prednjači kada je riječ o medijatoru između percepcije prijetnje i namjere upravljanja kibernetičkim rizicima, jest varijabla *strah*. Istraživanja predvođena Boss et al. (2015) naglašavaju važnost posredničke uloge straha u PMT modelu, a prema Cram et al. (2019) njegovo izostavljanje može objasniti uočene nedosljednosti u pogledu utjecaja percipirane vjerojatnosti i intenziteta prijetnje na motive ponašanja. Riječ je o varijabli koja je inicijalno razmotrena kao element PMT modela u istraživanju Rogers (1983), međutim, u cilju zadržavanja kognitivnog/racionalnog PMT procesa/modela, Rogers se odlučio na isključenje varijable straha koja predstavlja emocionalni odgovor na prijetnju.

Na tragu nekonzistentnosti u rezultatima istraživanja utjecaja percepcije prijetnje na namjeru upravljanja kibernetičkim rizicima u organizacijskom kontekstu, te na tragu sugestija istraživanja Haag et al. (2021), Vrhovec i Mihelič (2021) te Boss et al. (2015), sugerira se uvođenje faktora kojeg problematizira bihevioralna ekonomija, a riječ je o emocijama. Stoga motivirani prazninom u literaturi, predloženim istraživanjem nastoji se odgovoriti na pitanje kakav će utjecaj imati emocije na ključno vodstvo organizacije u odlukama koje se tiču kibernetičkih.

4.1.3. Medijatorska uloga emocija u utjecaju percepcije prijetnje na namjeru upravljanja kibernetičkim rizicima

H2 Utjecaj percepcije prijetnje na namjeru upravljanja kibernetičkim rizicima posredovan je emocijama glavnog izvršnog menadžera.

Sukladno Loewenstein et al. (2001), važno je poštovati činjenicu kako se spoznajom o izloženosti prijetnji kod donositelja odluka javljaju emocije. U dosadašnjim je istraživanjima razmotrena varijabla strah koja je, sukladno ranije navedenom, bila u prijedlogu tvorca PMT modela, ali i kasnije, u empirijskim istraživanjima. Haag et al. (2021) sugeriraju da bi, osim do sada razmotrene varijable strah, u PMT model trebalo integrirati druge emocionalne reakcije,

[35] Primjerice, istraživanje Kianpour et al. (2019) uvodi varijablu *percipirana vrijednost kibernetičke sigurnosti* kao medijatora, međutim, pretpostavljana relacija empirijski se ne potvrđuje. Zatim, izdvajamo istraživanje Simonet i Teufel (2019) koji koriste varijablu *svijest o kibernetičkoj sigurnosti* u ulozi medijatora, što se potvrđuje kao statistički značajno u posredovanjuizmeđu percepcije prijetnje i ponašanja u području kibernetičke sigurnosti.

pri čemu se u predloženom istraživanju, pored straha, uvodi i emocija žaljenja. Riječ je o emocijama koje sukladno Sheeran et al. (2014) treba razlikovati, strah je emocija koja se pojavljuje u iščekivanju prijetnje, s druge strane, žaljenje je osjećaj koji donositelji odluka očekuju da će doživjeti. Obje emocije smatraju se važnim čimbenicima koji oblikuju namjere i ponašanje.

PMT je općenito dao prednost prijetnji pred strahom, stoga su istraživači izostavili razmatranje uloge straha. Međutim, strah dobiva na važnosti kada je prijetnji osobno izložen donositelj odluke (Lowry et al., 2023). Prema Stulz (1984), menadžeri su u značajnoj mjeri izloženi rizicima poslovne organizacije, jer imaju manju mogućnosti diversificiranja svojeg bogatstva u odnosu na vlasnike organizacija. U nastavku se predlažu hipoteze u kojima je predviđen medijatorski utjecaj emocija straha i žaljenja.

H2a Utjecaj percepcije prijetnje na namjeru upravljanja kibernetičkim rizicima posredovan je osjećajem straha kojeg iskazuje glavni izvršni menadžer

Sukladno Boss et al. (2015) i Ma (2022), strah je emocija sa snažnim psihološkim manifestacijama, a spoznaja o izloženosti prijetnji stvara strah koji je negativni emocionalni odgovor. Aurigemma i Mattson (2019) te Moody et al. (2018) ističu kako se strah manifestira kao osjećaj tjeskobe i zabrinutosti zbog izloženosti prijetnji, a stanje straha, kako ističu Posey et al. (2015), može znatno utjecati na stavove u vezi prijetnje, motivaciju, namjere ponašanja i stvarna ponašanja članova organizacije. Na tragu navedenoga, izdvajaju se istraživanja Moody et al. (2018) te Wall i Buche (2017) u kojima se navodi kako izostavljanje straha iz PMT modela može utjecati na nepotpuno razumijevanje procesa ponašanja, odnosno donošenja odluka u vezi zaštite od prijetnje.

Strah može imati pozitivan učinak na adaptivan odgovor (u kontekstu istraživanja upravljanja kibernetičkim rizicima), djelujući kao medijator između procjene prijetnje i motivacije za zaštitom (Floyd et al., 2000). Na temelju navedenih argumenata, u okviru istraživanja pretpostavka je kako će strah biti određen percepcijom prijetnje, ali isto tako da će strah kao emocija utjecati na motiviranost glavnog izvršnog menadžera na upravljanje kibernetičkim rizicima.

Temeljem uvida u literaturu (*Prilog H*), zaključuje se da je tek nekolicina studija, u kontekstu poslovnog okružja, razmatrala ulogu straha u okviru PMT teorije. Prema Posey et al. (2011), iako strah od prijetnje može biti važan prediktor u motivaciji za zaštitom, isti se ne potvrđuje kao faktor koji ima značajnu ulogu u motiviranju zaposlenika da se uključe u aktivnosti zaštite

od prijetnje kojima je izložena organizacija. Činjenicu kako se strah ne pretvara u pozitivnu motivaciju za zaštitu tvrtke, Burns et al. (2017) opravdavaju prirodom straha, koji je, kako je ranije istaknuto, emocionalni odgovor, i kojeg prema Fredrickson (2001) karakterizira prolazno stanje. Vrhovec i Mihelič (2021) u okviru PMT modela empirijski propituju, pored medijatorskog, i moderatorski utjecaj straha. Međutim, izostaje potvrda moderatorskog utjecaja.

U okviru predloženog istraživanja, pokušat će se dodatno propitati medijatorska uloga straha na vezu između percipirane prijetnje i namjere upravljanja kibernetičkim rizicima. Argument nastavku propitivanja varijable strah, pronalazi se u tvrdnji kako upravo strah može objasniti uočene nedosljednosti u pogledu utjecaja percipirane vjerojatnosti i intenziteta prijetnje na namjere ponašanja (Cram et al., 2019). Dodatno, u odnosu na ranija istraživanja, propituje se populacija glavnih izvršnih menadžera koji u odnosu na raniju istraživanu populaciju (zaposlenici ili menadžeri niže razine), bilježe veći stupanj izloženosti poslovnoj organizaciji.

Kada se percepcija donositelja odluka o ozbiljnosti kibernetičkih rizika kao prijetnje povećava, očekuje se da će se povećati i razina straha koju će glavni izvršni menadžeri kao ključni donositelji odluka doživjeti. Postoje dokazi koji podupiru odnos između percipirane ozbiljnosti prijetnje i straha (Boss et al., 2015, Burns et al., 2017, Ogbanufe i Pavur, 2022, Ma, 2022). Nadalje, očekuje se da će strah utjecati na stupanj motiviranosti upravljanja kibernetičkim rizicima na razini organizacije. Prethodna istraživanja su pronašla pozitivne odnose između straha i motivacije za zaštitom (Boss et al., 2015; Ogbanufe i Pavur, 2022, Ma, 2022).

Recentno istraživanje koje je zauzelo ovakav pristup je Ogbanufe i Pavur (2022), međutim, ono je provedeno u izvan organizacijskom kontekstu. Dodatno, dosadašnja istraživanja nisu razmatrala strah od kibernetičkih rizika u kontekstu odluka glavnih izvršnih menadžera. Upravo se u ovome istraživanju zauzima pristup da menadžer može osjećati straha i da je to sasvim opravdano, uzevši u obzir značajnu osobnu izloženost menadžera poslovnoj organizaciji.

Razmatrajući pristrani optimizam i strah kao bihevioralne čimbenike, važno je izdvojiti da različito utječu na proces odlučivanja u kontekstu kibernetičkih rizika te opravdati njihovo zajedničko razmatranje. Pristrani optimizam, identificiran u hipotezi H1a, vodi do podcjenjivanja kibernetičkih rizika, stvarajući nepravilnu predodžbu o sigurnosti organizacije. Nasuprot tome, strah djeluje kao čimbenik koji je oblikovan spoznajom o izloženosti kibernetičkom riziku kao prijetnji, a koji potiče adaptivan odgovor na izloženost kibernetičkim rizicima. Stoga će se ovo istraživanje usredotočiti na ispitivanje kako pristrani optimizam i strah

zajedno utječu na namjeru upravljanja kibernetičkim rizicima, pri čemu će se posebno analizirati kako pristranost optimizma djeluje na percepciju kibernetičkog rizika kao prijetnje te kako emocija strah u ulozi medijatora određuje namjeru upravljanja kibernetičkim rizicima. Navedeni pristup omogućava bolje razumijevanje načina na koje različiti bihevioralni čimbenici oblikuju percepciju rizika i odlučivanje u vezi upravljanja kibernetičkim rizicima. Model dobiva na dubini, reflektirajući kompleksnost odluke u kontekstu kibernetičkih rizika. Uključivanje i analiza oba čimbenika opravdani su, jer se njihovim međusobnim odnosom može bolje shvatiti proces donošenja odluka u kontekstu kibernetičkih rizika.

H2b Utjecaj percepcije prijetnje na namjeru upravljanja kibernetičkim rizicima posredovan je osjećajem žaljenja kojega iskazuje glavni izvršni menadžer

Fishburn (1982) i Loomes i Sugden (1982) razvijaju teoriju žaljenja te je smatraju alternativom racionalnom izboru kada se odluke donose u uvjetima nesigurnosti. Želja da se izbjegne žaljenje utjecat će na donesenu odluku (Bell, 1982). Jedna od često korištenih definicija specificira žaljenje kao više ili manje bolno kognitivno i emocionalno stanje prouzročeno gubitkom, nedostatkom, ograničenjem ili pogreškom (Landman, 1993). Dva su izvora iz kojih žaljenje proizlazi; *iskustvo ranijih odluka* (posljedica pogrešne odluke) odnosno *anticipirano žaljenje* vezano za projicirane posljedice donesene odluke (Zeelenberg et al., 1996). Očekivano žaljenje može se općenito klasificirati kao žaljenje zbog radnje ili žaljenje zbog nečinjenja. Žaljenje zbog radnje obuhvaća žaljenje koje proizlazi iz određenog ponašanja, dok žaljenje zbog nečinjenja proizlazi iz neuspjeha pojedinca da se uključi u određeno ponašanje (Brewer et al., 2016). Naime, kada se donositelj odluke suoči s kibernetičkom prijetnjom, negativni ishod koji dovodi do žaljenja bit će izraženiji ukoliko pojedinac ne potiče razvoj procesa upravljanja kibernetičkim rizicima, za razliku od onda kada te radnje poduzme. U okviru predloženog istraživanja, emocija žaljenja mjerit će se pomoću anticipiranog žaljenja[36].

Loomes i Sugden (1982) ističu kako je žaljenje primarna emocija u donošenju odluka te predstavlja negativnu emociju koju donositelj odluka želi izbjeći. Donesena odluka određena je činjenicom da pojedinac osjeća žaljenje (Carfora et al., 2017; Lazuras et al., 2017; Zeelenberg i Pieters, 2004), a prisutnost odbojnosti prema žaljenju motivira pojedinca na aktivnosti koje doprinose sprječavanju budućeg žaljenja (Shih i Schau, 2011). Opće zapažanje je da donositelji odluka pokušavaju izbjeći odluke koje dovode do suočavanja sa žaljenjem (Wangzhou et al.,

[36] Anticipirano žaljenje odražava anticipaciju negativne emocije koja je doživljena kada donositelj odluke shvati da je trenutni položaj mogao biti povoljniji da je drugačije postupio (Sandberg i Conner, 2008).

2021; Chen et al., 2018; Zeelenberg, 1999; Larrick i Boles, 1995). U istraživanju Richard et al. (1996) i Simonson (1992) potvrđuje se kako odbojnost prema žaljenju, mjerena očekivanim žaljenjem, potiče donositelja odluke na izbor sigurne alternative.

Posljednjih godina aktualizira se utjecaj kojeg očekivano žaljenje ima na odluke u vezi informacijske sigurnosti. Pokazalo se da očekivano žaljenje pozitivno utječe na namjere usvajanja dobrog ponašanja u vezi s informacijskom sigurnošću u kontekstu organizacijskih (Sommestad et al., 2015b) i osobnih (Verkijika, 2019; 2018) računalnih domena. Isto tako, studija Verkijika (2018) pokazala je da je očekivano žaljenje imalo pozitivan, značajan i izravan utjecaj na sigurnosno ponašanje. Ogbanufe i Baham (2022), Ogbanufe i Pavur (2022) i Chen i Li (2017) zaključuju kako je odbojnost prema žaljenju (mjerena anticipiranim žaljenjem) neophodan pokretač namjere da se usvoji mjera zaštite u polju informacijske sigurnosti, pri čemu Ogbanufe i Pavur (2022) emociju žaljenja razmatraju kao posljedicu percepcije rizika.

U okviru predloženog istraživanja, propituje se medijacijska uloga emocije žaljenje na vezu između percipirane prijetnje i namjere upravljanja kibernetičkim rizicima. Uvažava se pretpostavka da odbojnost prema žaljenju dobiva na važnosti kada je kibernetički rizik izraženije percipiran kao prijetnja za poslovanje organizacije. U *Prilogu I* iznosi se pregled istraživanja u okviru kojih se razmatra uloga emocije žaljenje na odluke unutar i izvan područja kibernetičkih rizika.

4.1.4. Utjecaj percepcije sposobnosti suočavanja organizacije s kibernetičkim rizicima na namjeru upravljanja kibernetičkim rizicima

H3 Percepcija glavnog izvršnog menadžera o sposobnosti suočavanja organizacije s kibernetičkim rizicima pozitivno utječe na namjeru upravljanja kibernetičkim rizicima

Sukladno Rogers (1983), pored procijenjene prijetnje, ključna procjena koju donositelj odluke treba provesti jest procjena/percepcija suočavanja. Isto se odnosi na procjenu koliko je zahtjevno upravljanje kibernetičkom prijetnjom. Percepcija suočavanja određena je pitanjem koliko su *učinkovite odluke* u vezi upravljanja kibernetičkim rizicima, koliko je organizacija sposobna *učinkovito primjenjivati aktivnosti zaštite* (upravljanja kibernetičkim rizicima) i naposljetku, koji su *troškovi* povezani s aktivnostima upravljanja kibernetičkim rizicima. Stoga, izdvajamo tri ključne varijable koje određuju percepciju suočavanja s prijetnjom, a riječ je o

percipiranoj učinkovitosti odgovora na prijetnju, percipiranoj samoučinkovitosti te percipiranim troškovima adaptivnog odgovora. Procjena učinkovitosti odgovora i samoučinkovitosti u njihovoj provedbi pozitivno utječu na namjeru upravljanja kibernetičkim rizicima. S druge strane, procjena troškova zauzima suprotan smjer utjecaja, pri čemu se očekuje kako povećanje troškova adaptivnog ponašanja obeshrabruje njezinu primjenu (Sommestad et al., 2015b).

Percipirana učinkovitost odgovora odnosi se na subjektivnu procjenu donositelja odluke u vezi učinkovitosti zaštitnih mjera (učinkovitost aktivnosti upravljanja rizicima) kojima se ublažavaju postojeće prijetnje. Istraživanja su potvrdila pozitivan utjecaj percipirane učinkovitosti odgovora na namjeru, odnosno motiviranost usvajanja zaštitnih radnji. Primjerice Johnston i Warkentin (2010), Liang i Xue (2010) te Lee i Larson (2009) potvrđuju pozitivan utjecaj na korištenje programa za zaštitu od špijunskog softvera. Nadalje, Herath i Rao (2009), Lee i Larsen (2009) i Ifinedo (2012) potvrđuju pozitivan utjecaj percipirane učinkovitosti odgovora na pridržavanje pravila/politika povezanih sa sigurnošću.

Samoučinkovitost se odnosi na procjenu sposobnosti organizacije da na učinkovit način primijeni adaptivan odgovor (upravlja kibernetičkim rizicima). Samoučinkovitost je određena raspoloživim znanjima, vještinama i iskustvom (Maddux i Rogers, 1983). Blythe i Coventry (2018) ističu da se samoučinkovitost odgovora odnosi na procjenu sposobnosti suočavanja sa prijetnjom, odnosno sposobnosti utjecaja na prijetnju. U kontekstu kibernetičke prijetnje, pretpostavlja se da će organizacije koje imaju visoke sigurnosne sposobnosti vjerojatnije slijediti sigurnosne prakse, budući da su učinkovitije u učenju kako ih slijediti i sposobnije za odgovarajuće ponašanje. Johnston i Warkentin (2010) pronašli su izravnu pozitivnu vezu između samoučinkovitosti i upotrebe programa za zaštitu od špijunskog softvera. Slično navedenome, Bulgurcu et al. (2010) i Ifinedo (2014; 2012) otkrili su pozitivan odnos između samoučinkovitosti i usklađenosti postupanja s politikom informacijske sigurnosti.

Konačno, komponenta percepcije suočavanja obuhvaća i procjenu troškova upravljanja kibernetičkim rizicima. Riječ je o procjeni angažmana resursa potrebnih za provedbu adaptivnog odgovora (upravljanja kibernetičkim rizicima). Prema Blythe i Coventry (2018), troškovi se mogu odnositi na novčane izdatke, utrošeno vrijeme, ali i druge negativne posljedice koje proizlaze iz izvršenja sigurnosnog ponašanja (primjerice praćenje protokola zaštite od informacijskih/kibernetičkih rizika usporava provedbu radnog procesa, što u konačnici ima

stvaranje oportunitetnih troškova[37]). Prema Ma (2022) i Lee i Larsen (2009), kada se cijena odgovora na prijetnju (izloženost riziku) poveća, smanjuje se vjerojatnost da će stručnjaci za informacijsku sigurnost izvesti adaptivne odgovore. Slični zaključci izvode se temeljem rezultata istraživanja Workman et al. (2008) te Wu i Wang (2005) u vezi motiviranosti korištenja sigurnosnih mjera. Istraživanje Herath i Rao (2009) potvrđuje negativan utjecaj troškova odgovora na motiv usklađenosti s politikom informacijske sigurnosti. S druge strane, u istraživanju Ifinedo (2012) izostaje empirijska potvrda pretpostavljene veze. U *Prilogu J* se iznosi pregled novijih istraživanja čiji je primarni fokus odlučivanje u organizacijskom kontekstu, gdje je za svaku studiju istaknuta značajnost utjecaja ključnih varijabli percepcije suočavanja za PMT model.

Burns et al. (2017), Li et al. (2019) i Sommestad et al. (2015b) u svojim istraživanjima navode da je procjena suočavanja značajno utjecajnija u razvoju motivacije za zaštitom nego procjena prijetnje. Međutim, segmentacija na odluke donesene u kontekstu organizacije te privatne odluke, navodi na sasvim suprotan zaključak. Naime, Sommestad et al. (2015b) zaključuju kako su odluke u vezi zaštite (upravljanja kibernetičkim rizicima) u kontekstu organizacije značajnije pod utjecajem percepcije prijetnje, nego pod utjecajem percepcije suočavanja, što je suprotno od odluka koje se odnose na pojedinca i koje obilježava veći stupanj slobode postupanja. Objašnjenje za navedeno jest u činjenici da procjena suočavanja donositelja odluke postaje manje važan faktor u slučaju postojanja jasnih pravila i obveze pridržavanja pravila/politika unutar organizacije, čija svrha je zaštita od prijetnje.

Menadžeri se od zaposlenika razlikuju po potrebi za strateškim promišljanjem, posebno kada je riječ o balansiranju između sigurnosti i efikasnog te profitabilnog poslovanja. Dok menadžeri donose ključne odluke vezane za upravljanje rizicima, poput integracije upravljanja kibernetičkim rizicima u procese upravljanja poslovnim rizicima, njihov kontekst odlučivanja često se preklapa s kontekstom odluka slobodnih pojedinaca, a ne s kontekstom zaposlenika koji su obično ograničeni u svom djelokrugu. U ovom kontekstu, percepcija sposobnosti menadžera da se suoči s prijetnjom postaje važnija od same percepcije prijetnje.

Međutim, u organizacijskom okruženju, procjena suočavanja je složena, pri čemu Schuetz et al. (2020) ističu kako organizacijska obilježja mogu utjecati na učinkovitost odgovora i povećanje troškova adaptivnog ponašanja.

[37] Istraživanja podupiru tezu da politike informacijske sigurnosti smanjuju produktivnost zaposlenika, a navedeni zaključci potvrđuju se u istraživanju Beautement et al. (2009).

Nakon razmotrenih rezultata istraživanja, zaključuje se kako mehanizmi procjene suočavanja s prijetnjom, u pravilu, imaju snažne učinke na motivaciju za zaštitom od informacijskih i kibernetičkih rizika, što je potvrda da komponenta percepcije suočavanja, koja prema Lee i Larsen (2009) odražava tradicionalni društveno-ekonomski model, učinkovito funkcionira u kontekstu informacijske/kibernetičke sigurnosti.

Istraživanjem je pretpostavljeno da su relacije između percepcije rizika i suočavanja, namjere upravljanja kibernetičkim rizicima te varijabli pristranosti i emocija kojima se produbljuje spoznaja o postavljenoj relaciji, uvjetovane obilježjima donositelja odluka i obilježjima organizacije.

Prilikom istraživanja veza između *percepcije prijetnje i percepcije suočavanja*, *kognitivne pristranosti* i *emocija* te *namjere upravljanja kibernetičkim rizicima*, uvažit će se **specifična obilježja donositelja odluka i obilježja organizacije**, što će omogućiti kontrolu i vjerodostojnost u procjeni rezultata, uz istodobno razumijevanje koja obilježja su značajna prilikom razmatranja veza između ključnih varijabli. Riječ je o kontrolnim varijablama, koje nisu primarno u fokusu istraživanja, ali njihovo postojanje se ne može zanemariti, budući da se očekuje da imaju utjecaj na zavisnu varijablu.

Veza između razmatranih relacija kontrolira se za obilježje donositelja: **iskustvo rada na IT poslovima** (Lee i Larsen, 2009; Herath Rao 2009) te za obilježje organizacije: **veličina poduzeća, industrijska pripadnost** (Bulgurcu et al. 2010; Lee i Larsen, 2009) te **digitalna zrelost**[38].

4.2. Konceptualni model istraživanja

Konceptualni model uporište pronalazi u teoriji motivacije za zaštitom. Predlaže se model istraživanja koji objašnjava utjecaj *percepcije kibernetičkih rizika kao prijetnje* (percepcija prijetnje) i *percepcije sposobnosti organizacije u upravljanju kibernetičkim rizicima*

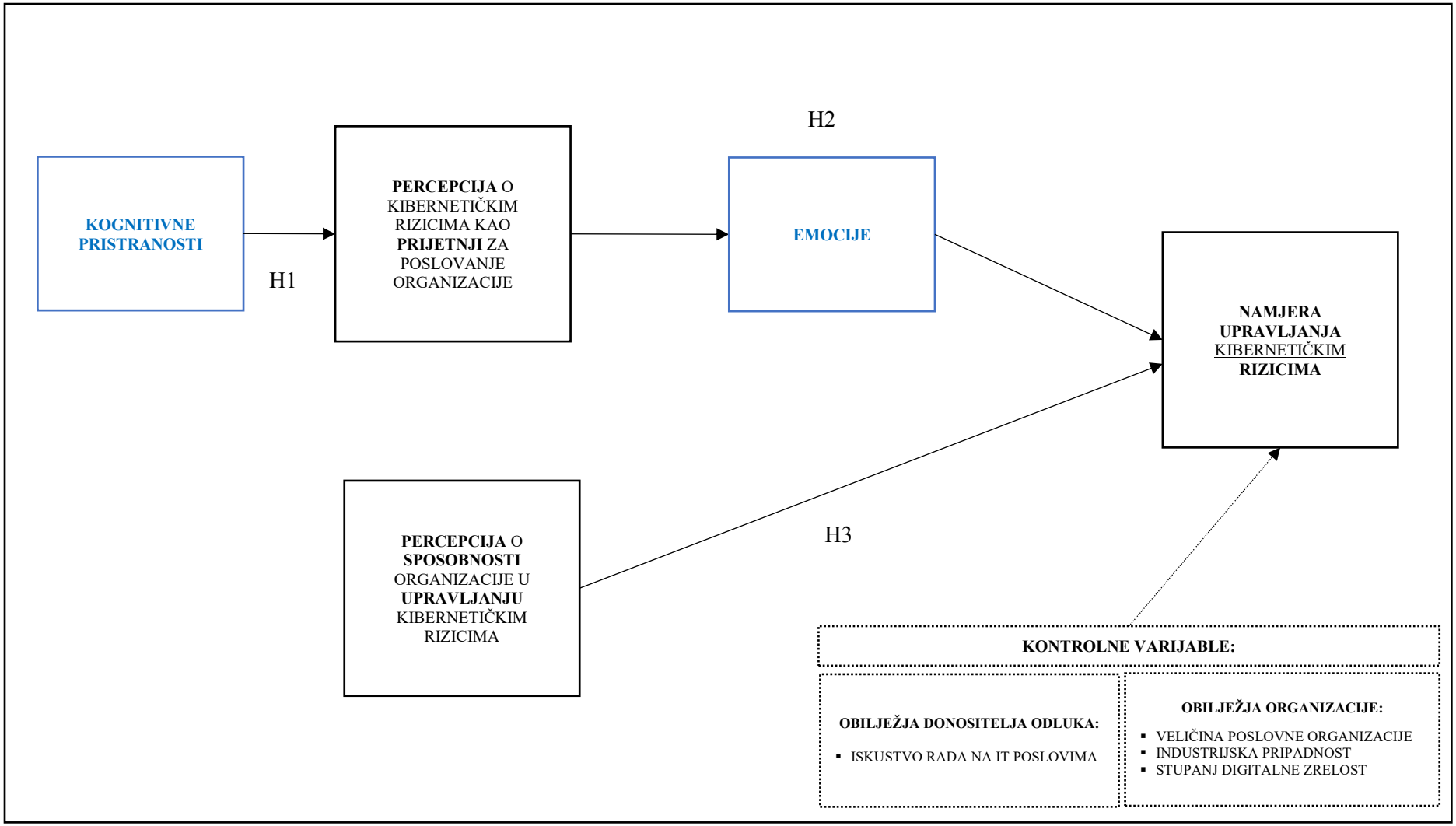
[38] Digitalna zrelost odnosi se na razinu stručnosti i sofisticiranosti koju organizacija ima u korištenju digitalnih tehnologija za postizanje svojih ciljeva (Berghaus i Back, 2016). Sukladno Gill i VanBoskirk (2016) i VanBoskirk et al. (2017), više je segmenata u kojima se digitalna zrelost postiže, pri čemu se za potrebe ovog rada ističe **digitalna kultura** *(pristup digitalnim inovacijama),* prihvaćanje novih **tehnologija** i usmjerenost na razvoj **digitalne strategije**.

(percepcija suočavanja) na namjeru upravljanja kibernetičkim rizicima. U pokušaju razumijevanja osnovnih varijabli PMT modela i njihovog međusobnog utjecaja, uvažavaju se pretpostavke bihevioralne ekonomije te se model proširuje za varijable **kognitivne pristranosti i emocija.**

Modelom se pretpostavlja da kognitivne pristranosti utječu na oblikovanje percepcije o kibernetičkim rizicima kao prijetnji za poslovanje organizacije (H1). Nadalje, modelom se pretpostavlja kako glavni izvršni menadžeri koji kibernetičke rizike percipiraju kao veću prijetnju za poslovanje organizacije posredstvom emocija, iskazuju veće namjere upravljanja kibernetičkim rizicima (H2). Sukladno osnovnom teorijskom modelu motivacije za zaštitom, pretpostavlja se kako donositelj odluka koji suočavanje s kibernetičkim rizicima percipira kao veći izazov za poslovnu organizaciju, izravno iskazuje manju namjeru upravljanja kibernetičkim rizicima kojima je izložena organizacija (H3).

Uporište izdvajanja čimbenika percepcija prijetnje i percepcija sposobnosti suočavanja pronalazi se u teoriji motivacije za zaštitom (PMT) koja je vodeći teorijski okvir u istraživanju odluka u vezi informacijske i kibernetičke sigurnosti (Haag et al., 2021; Kianpour et al., 2019; Li et al., 2019; Boss et al., 2015). Riječ je o teoriji koja je adekvatna za objašnjavanje odluka u organizacijskom kontekstu (Bode et al., 2022), a njezina primjena u kontekstu menadžerskog odlučivanja sugerira se u radu Connelly i Shi (2022). Uvođenjem varijabli koje pripadaju kognitivnoj pristranosti i emocijama, prihvaća se pretpostavka bihevioralne ekonomije kako ekonomski subjekti ne donose u potpunosti racionalne odluke te da na odluke utječu neracionalni čimbenici (Tversky i Kahneman, 1974).

Naime, klasično shvaćanje racionalnosti zahtijeva da donositelj odluka posjeduje apsolutna znanja te da je savršeno informiran, a takve uvjete zasigurno nije moguće postići kod upravljanja kibernetičkim rizicima koje odlikuje nedostatak informacija (Gomez i Villar 2018).



Slika 9. Koncept teorijskog modela temeljenog na teoriji motivacije za zaštitom

Izvor: Izrada autora

5. EMPIRIJSKO ISTRAŽIVANJE I VREDNOVANJE MODELA

Ovo poglavlje opisuje empirijsko istraživanja te se u prvom dijelu opisuje metodološki okvir istraživanja, uključujući metodu istraživanja, populaciju i uzorak istraživanja, postupak prikupljanja podataka te korišteni instrument za prikupljanje podataka.

U drugom dijelu, opisuju se rezultati empirijskog istraživanja, a navedeno uključuje analizu rezultata istraživanja s ekspertima i pilot istraživanje te analizu glavnog istraživanja koja je posebno segmentirana na analizu modela prve razine i modela druge razine. Analiza modela pretpostavlja analizu mjernog modela te analizu strukturalnog modela. Poglavlje pruža uvid u rezultate testiranja valjanosti modela te relevantne varijable modela namjere upravljanja kibernetičkim rizicima.

5.1. Metodološki okvir istraživanja

U ovom segmentu rada opisana je korištena znanstvena metoda, način odabira populacije te uzorka istraživanja, razvoj istraživačkog instrumenta uz predstavljanje istog te je opisan proces prikupljanja podataka.

5.1.1. Metoda

U svrhu ispitivanja relacije i utjecaja između percepcije kibernetičkih rizika kao prijetnje, percepcije suočavanja i namjere upravljanja kibernetičkim rizicima te kognitivnih pristranosti i emocija, primijenit će se **metoda modeliranje strukturalnim jednadžbama**[39] (*engl. Structural equation modeling – SEM*). Riječ je o multivarijatnoj metodi statističke analize čiji temelj predstavlja faktorska analiza, analiza putanje te višestruka regresijska analiza (Weston i Gore, 2006).

Prema Morrison et al. (2017) riječ je o složenoj metodi analize podataka koja pruža korist u vidu mogućnosti analiziranja i testiranja međusobnih odnosa između varijabli. Von der Embse (2016) ističe kako metoda strukturalno modeliranje omogućuje testiranje pretpostavljenih

[39] Pregledom literature uočava se korištenje alternativnih naziva za razmatranu metodu kao što su analiza strukture kovarijanci, uzročno modeliranje, uzročna analiza, simultano modeliranje jednadžbama i analiza latentnih varijabli.

odnosa koji nisu mogući tradicionalnim analitičkim metodama podataka kao što je to slučaj s regresijskom analizom.

Metoda strukturalno modeliranje je popularna zbog činjenice da, u odnosu na ostale opće linearne modele (*analiza varijance, multivarijatna analiza varijance, višestruka regresija*), gdje su varijable predstavljene jednom mjerom, a pogreška mjerenja nije modelirana, omogućava istraživaču da koristi više mjera za jednu varijablu, čime se rješava problem pogreške specifične za korištenu mjeru. Iz navedenog razloga, zaključci o testiranim hipotezama nisu pristrani zbog pogreške mjerenja.

Ključno je istaknuti prednost SEM metode u smislu da omogućava unutar modela integraciju složenih konstrukata (latentnih varijabli ili faktora) koje nije moguće direktno mjeriti, a što je u kontekstu predstavljenog istraživanja aktualno kada razmatramo *percepciju, pristranosti i emocije*.

Sukladno Kline (2015), Hair et al. (2021), razlikuju se dva pristupa strukturalnog modeliranja; CB-SEM metoda (*engl. Covariance-based Structural Equation Modeling*) i PLS-SEM metoda (*engl. Partial Least Squares Structural Equation Modeling*). Prva je bazirana na kovarijanci koja se koristi za potvrđivanje odnosno odbacivanje teza (teorije), tj. u konfirmatorne svrhe, a zahtjevi za minimalnom veličinom uzorka su stroži. Drugi navedeni pristup predstavlja metodu modeliranja strukturalnih jednadžbi s najmanjim kvadratima koja se koristi u svrhu statističke potvrde postavljenih hipoteza utemeljenih na teoriji na način da se usmjerava na objašnjenje varijance u zavisnim varijablama. Pored primijene u konfirmatorne svrhe (Hair et al. 2019; Hair et al. 2017a), primjenjuje se i kod proširenja teorije, tj. eksplanatornih istraživanja i prediktivnih istraživanja (Hair et al. 2021). Metoda je vrlo učinkovita s malim veličinama uzorka. Odabir tehnike procjene modela treba se temeljiti na ciljevima istraživanja, karakteristikama podataka i metode (Hair et al. 2017b; Hair et al., 2012), uzimajući u obzir obilježja kao što su veličina uzorka, distribucijska svojstva podataka te složenost konceptualnog modela, pri čemu treba imati na umu da nijedna tehnika nije superiorna u odnosu na drugu niti primjenjiva u svakoj situaciji (Hair et al., 2021; Petter, 2018).

Hair et al. (2021) sugerira korištenje PLS-SEM-a u slučaju testiranja teorijskog okvira iz perspektive predviđanja, potom, kada je strukturalni model složen (uključuje mnoge konstrukte i međusobne veze konstrukata). Preporuka je koristiti PLS-SEM kada se istraživanjem nastoji proširiti postavljena teorija (eksploratorno istraživanje), potom, kada model pretpostavlja jedan

ili više formativno izmjeren konstrukt ili ukoliko se istraživanje temelji na sekundarnim podacima te primjenjuje financijske omjere.

Postupak primjene metode strukturalno modeliranje predviđa analizu podataka u dvije faze; provođenje analize mjernog modela čime je cilj postići procjenu pouzdanosti i valjanosti mjernih ljestvica te analiziranje podataka metodom strukturalnih jednadžbi s ciljem testiranja veze iz predviđenog konceptualnog modela te procjena parametara.

Procjena pouzdanosti i valjanosti mjernih ljestvica razlikuje se ovisno o tome je li model sadržava reflektivne ili formativne indikatore koji su određeni pretpostavkom uzročnosti između konstrukta i njegovih indikatora (mjernih čestica). U reflektivnim mjernim modelima, uzima se u obzir kako su indikatori (mjerne čestice) međusobno snažno povezani i mogu se zamijeniti. Drugim riječima, mogu biti isključeni iz analize bez utjecaja na značenje faktora. S druge strane, formativni mjerni model temelji se na pretpostavci kako indikator uzrokuje konstrukt (faktor ili latentna varijabla) pri čemu se dodavanjem ili uklanjanjem indikatora (mjerne čestice) mijenja konceptualno značenje faktora (Kline, 2015). U bihevioralnim istraživanjima dominira pristup prema kojem konstrukt odražava indikator pri čemu su indikatori razmatrani kao posljedice konstrukta. Koncepti poput stavova i bihevioralnih namjera analiziraju se koristeći reflektivni mjerni model (Vuković, 2022). Stoga se u okviru istraživanja zauzima pristup procjene reflektivnog mjernog modela koji predviđa postupak procjene prezentiran u *Tablici 9*.

Tablica 9. Pregled korištenih pokazatelja za vrednovanje pouzdanosti i valjanosti reflektivnih mjernih konstrukata

Analiza		**Pokazatelj**	**Opis**
Pouzdanost	**Pouzdanost indikatora**	Faktorsko opterećenje (*engl. Factor loading*)	Mjeri razinu koreliranosti između konstrukta (faktora) i indikatora (mjernih čestica). Referentna vrijednost je =>0,5, a manje od <=0,95 (Hair et al., 2010)
	Interna pouzdanost	Cronbach alfa (*engl. Cronbach's alpha*)	Mjeri koliko su indikatori (mjerne čestice) namijenjeni mjerenju konkretnog konstrukta unutar skupa svih indikatora (npr. upitnika) koherentni među sobom u pogledu onoga što mjere. Ako je skup

Analiza		Pokazatelj	Opis
			indikatora snažno koreliran, to sugerira da sve one mjere isti koncept. Referentna vrijednost je =>0,7, a manje od <=0,95 (Hair et al., 2021; Hair et al., 2017a).
	Kompozitna pouzdanost	CR (*engl. Composite reliability*)	Mjeri ukupnu pouzdanost skupa indikatora (mjernih čestica) predviđenih u mjerenju konstrukta (Hair, et al., 2010). Temelji se na vrijednosti vanjskih opterećenja te ne pretpostavlja da su svi indikatori jednako pouzdani zbog čega se smatra kako pruža preciznije procjene pouzdanosti u odnosu na Cronbach alpha (Geldhof et al., 2014). Referentna vrijednost je =>0,7, a manje od <=0,95 (Hair et al., 2021; Hair et al., 2017a).
Valjanost	**Konvergentna konstruktna valjanost**	AVE - Prosječna izlučena (ekstrahirana) varijanca (*engl. Average variance extracted - AVE*)	Predstavlja prosječan postotak objašnjene varijance koju konstrukt objašnjava među indikatorima. Referentna vrijednost je =>0,5 (Hair et al., 2021; Fornell i Larcker, 1981).
	Konvergentna diskriminantna valjanost	Unakrsno opterećenje (*engl. Cross loadings*)	Otkriva je li indikator (mjerna čestica) snažno korelira s više konstrukata (faktorima) (Hair et al., 2010).
		Fornell Larcker kriterij	Diskriminantna valjanost konstrukta ostvaruje se kada je kvadrirani korijen njegove prosječno izlučene varijance (AVE) veći od koeficijenta korelacije razmatranog konstrukta i ostalih konstrukata. (Hair et al., 2021; Fornell i Larcker, 1981)
		Heterotrait-monotrait omjer	Omjer između korelacija latentnih varijabli različitih konstrukata

Analiza		Pokazatelj	Opis
		(*engl. Heterotrait-Monotrait Ratio of Correlations - HTMT*)	(heterotrait) i prosječnih korelacija stavki unutar istog konstrukta (monotrait). Pokazuje se kao efikasniji način testiranja diskriminantne validnosti u odnosu na unakrsno opterećenje te Fornell Larcker kriterij. Vrijednost HTMT bliže 1 ukazuje na problem s diskriminantnom valjanosti odnosno kako se konstrukti (faktori) ne razlikuju dovoljno. Vrijednosti manje od 0,85 sugeriraju na prihvatljivu diskriminantnu valjanost (Hair et al., 2021; Henseler et al., 2015).

Izvor: Izrada autora

U nastavku, u okviru *Tablice 10*, pružen je pregled korištenih pokazatelja namijenjenih vrednovanju strukturalnog modela.

Tablica 10. Pregled korištenih pokazatelja za vrednovanje strukturalnog modela

Analiza	Pokazatelj	Opis
Multikolinearnost strukturalnog modela	VIF (*engl. Variance inflation factor*)	Mjeri stupanj kolinearnosti između neovisnih varijabli u strukturalnom modelu. Vrijednost VIF-a manja od 5 sugerira da nema problema s multikolinearosti. (Hair et al., 2021; Hair et al., 2017a).
Značajnost i relevantnost veza u strukturalnom modelu	t-vrijednost / p-vrijednost	Statistički test koji se koristi za procjenu značajnosti putanje između konstrukata u okviru strukturalnog modela. Ukoliko je t-vrijednost iznad kritične granice (1,96 za p=0,05), putanja je statistički značajna. (Hair et al., 2021; Hair, et al., 2017a).
Prediktivna relevantnost	R^2 (Koeficijent determinacije)	Pokazuje koliko postotka varijance zavisne varijable je objašnjeno

Analiza	Pokazatelj	Opis
		neovisnim varijablama u modelu (Hair et al., 2021; Hair, et al., 2017a).
	f^2 i v^2 efekt (Veličina efekta)	Mjeri snagu pojedinačnog prediktora u objašnjavanju varijance zavisne varijable.
	Q^2 efekt	Pokazatelj prediktivne relevantnosti za model. Kada je Q^2 veći od 0, model ima prediktivnu relevantnost za određene endogene konstrukte. (Hair et al., 2021; Hair, et al., 2017a).

Izvor: Izrada autora

U cilju empirijske procijene modela kojim se pokušava razumjeti namjera glavnih izvršnih menadžera glede upravljanja kibernetičkim rizicima u poslovnim organizacijama na prostoru Republike Hrvatske, korištena je PLS-SEM procedura procjene modela. Potonja se smatra opravdanom s obzirom na specifičnosti konceptualnog modela, specifičnost prikupljenih podataka te karakteristike PLS-SEM tehnike koja je sukladno pravilima Hair et al. (2021), pogodna za procjenu modela koji imaju eksplorativna obilježja, a što je usklađeno s ciljevima predstavljenog istraživanja. Dodatan argument za primjenu PLS-SEM tehnike temeljen je u činjenici kako je isti dominantan procjenitelj za modele strukturalnih jednadžbi u istraživanjima iz područja kibernetičkih i informacijskih rizika. Procjena modela pomoću PLS-SEM tehnike provedena je u uz pomoć specijaliziranog statističkog paketa SmartPLS, verzija 4.

5.1.2. Populacija i uzorak istraživanja

S obzirom da je cilj razumjeti namjere glavnih izvršnih menadžera u vezi upravljanja kibernetičkim rizicima u organizacijskom kontekstu, ciljani ispitanici su glavni izvršni menadžeri u poslovnim organizacijama. Suočeni s ograničenjem u vezi veličine hrvatskog gospodarstva te veličine proučavane populacije – glavnih izvršnih menadžera u trgovačkim društvima na prostoru Republike Hrvatske, koja bilježi iznimno nisku stopu uključenosti u anketna istraživanja, okvir uzorka predviđa niži stupanj homogenosti u odnosu na istraživanje koje se koncentrira isključivo na točno određenu veličinu organizacije ili industriju. Svjesni

navedene činjenice, istraživanje pretpostavlja uvođenje kontrolnih varijabli unutar testiranog modela; *veličina* te *industrijska pripadnost poslovne organizacije*.

Primaran cilj je bio usredotočiti se na organizacije s većim brojem zaposlenih, no takav pristup bi značajno suzio veličinu populacije (okvir uzorka). Uz to, trebalo je uzeti u obzir kvalitetu kontakt podataka kako se ne bi ugrozila provedivost istraživanja.

Istraživanje putem anketa među glavnim izvršnim direktorima (*engl. Chief Executive Officer – CEO*) povezano je s nizom izazova u smislu njegove provedbe. Naime, glavni izvršni menadžeri mogu na sudjelovanje u istraživanju gledati kao na aktivnost koja oduzima dragocjene resurse, prvenstveno vrijeme (Solarino i Aguinis, 2021; Baruch, 1999; Mintzberg, 1973). Stoga je neophodno pripremiti anketu koja će biti sažeta, pojednostaviti sudjelovanje u anketi, a istodobno artikulirati uvjerljive argumente o korisnosti i važnosti sudjelovanja u anketi (Cycyota, 2002). Pitanje povjerenja dodatno čini složenom provedbu istraživanja; sumnja prema namjerama koje stoje iza istraživanja i povjerljivosti podataka (D'Aveni, 1995), osobito ako je istraživanje inicirano od strane eksternih entiteta, kao što je u ovom istraživanju slučaj, a što može obeshrabriti na uključivanje u istraživanje. Ova problematika je još izraženija u svjetlu potencijalnih negativnih posljedica na poslovanje organizacije čemu su direktno izloženi. Glavni izvršni menadžeri su skloni izbjegavanju sudjelovanja ako procijene da su rizici preveliki. Naposljetku, ukoliko ciljevi ankete nisu u korelaciji s korporativnim prioritetima, moguća je niska razina angažmana od strane glavnih izvršnih menadžera (Cycyota i Harrison, 2002). Stoga je važno na adekvatan način predstaviti *istraživanje, istraživača te instituciju* u okviru koje se istraživanje organizira.

Odabran je pristup prema kojem su kontaktirane poslovne organizacije koje broje 4 i više zaposlenih. Prema ovom kriteriju, među aktivnim poslovnim organizacijama identificirano je njih 33.825. Odabrani pristup je kompromis između postizanja većeg stupnja homogenosti uzorka i mogućnosti provedbe istraživanja.

U cilju pružanja argumentacije za zadržavanje šireg okvira uzorka, ističe se pregled literature pružen u okviru točke 2.1.3. koja ukazuje na utjecaj kibernetičkih rizika na poslovanje organizacija s obzirom na njihova obilježja. Naime, kibernetički rizici jesu prijetnja za poslovne organizacije bez obzira na njihovu veličinu ili industrijsku pripadnost.

Tablica 11. Struktura populacije prema veličini i industriji

	Broj zaposlenih u organizaciji							
Djelatnost (Industrija)	*<6*	*6-10*	*11-20*	*21-50*	*51-100*	*101-250*	*>250*	**Ukupno**
A - POLJOPRIVREDA, ŠUMARSTVO I RIBARSTVO	201	264	161	101	20	21	11	779
B - RUDARSTVO I VAĐENJE	14	13	22	20	10	1	2	82
C - PRERAĐIVAČKA INDUSTRIJA	1.269	1.657	1.320	971	400	256	151	6.024
D - OPSKRBA ELEKTRIČNOM ENERGIJOM, PLINOM, PAROM I KLIMATIZACIJA	31	29	24	21	7	5	6	123
E - OPSKRBA VODOM; UKLANJANJE OTPADNIH VODA, GOSPODARENJE OTPADOM TE DJELATNOSTI SANACIJE OKOLIŠA	53	87	112	145	63	46	16	522
F - GRAĐEVINARSTVO	1.687	1.839	1.134	653	177	86	23	5.599
G - TRGOVINA NA VELIKO I NA MALO; POPRAVAK MOTORNIH VOZILA I MOTOCIKALA	2.313	2.157	1.187	662	180	105	79	6.683
H - PRIJEVOZ I SKLADIŠTENJE	480	445	275	186	64	46	33	1.529
I - DJELATNOSTI PRUŽANJA SMJEŠTAJA TE PRIPREME I USLUŽIVANJA HRANE	1.377	1.161	655	255	55	47	19	3.569
J - INFORMACIJE I KOMUNIKACIJE	442	520	328	204	50	43	20	1.607
K - FINANCIJSKE DJELATNOSTI I DJELATNOSTI OSIGURANJA	45	37	10	8		4	4	108
L - POSLOVANJE NEKRETNINAMA	157	147	68	38	5	3	2	420
M - STRUČNE, ZNANSTVENE I TEHNIČKE DJELATNOSTI	1.666	1.355	627	257	48	34	5	3.992
N - ADMINISTRATIVNE I POMOĆNE USLUŽNE DJELATNOSTI	421	421	246	148	57	37	25	1.355
O - JAVNA UPRAVA I OBRANA; OBVEZNO SOCIJALNO OSIGURANJE		3	1	1		1	1	7
P - OBRAZOVANJE	93	103	33	10				239
Q - DJELATNOSTI ZDRAVSTVENE ZAŠTITE I SOCIJALNE SKRBI	92	109	53	23	11	1		289
R - UMJETNOST, ZABAVA I REKREACIJA	82	63	55	33	20	6	7	266
S - OSTALE USLUŽNE DJELATNOSTI	358	168	59	31	8	7	1	632
Ukupno	**10.781**	**10.578**	**6.370**	**3.767**	**1175**	**749**	**405**	**33.825**

Napomena: Obuhvaćena su aktivna poduzeća koja redovno podnose izvještaje o poslovanju te koja broje 4 i više zaposlene osobe

Izvor. Izrada autora prema Bureau van Dijk Electronic Publishing Ltd (2023) i Hrvatska gospodarska komora (2023).

Nastavno na ranije istaknuto, predviđeno je uključiti industriju kao kontrolnu varijablu pri čemu će se formirati grupe ovisno o činjenici je li djelatnost koju obavlja/industrija kojoj pripada poslovna organizacija identificirana kao ključna usluga ili digitalna usluga u okviru **Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/2018)**. **Kontroliranje utjecaja varijabli, koje su u fokusu istraživanja, na zavisnu varijablu, za industrijsku pripadnost, uvažava se i zakonodavni okvir.**

Pretragom Hrvatska gospodarska komora (2023), Bureau van Dijk Electronic Publishing Ltd. (2023) i Fininfo (2023) prikupljeni su kontakt podaci za 26.700 poduzeća nakon čega je elektronička poruka s poveznicom za ispunjavanje ankete odaslana pomoću specijaliziranog alata za slanje anekta - Qualtrics. Anketa je uspješno isporučena na 25.976 elektroničkih adresa (poslovnih organizacija), time je kontaktirano iznad 75 % populacije. U razdoblju od 24. svibnja 2023. godine do 1. srpnja 2023. godine prikupljena su 673 odgovora, što ukazuje kako je postotak odaziva na anketu iznosio 2,6 %. S obzirom na iskustveno nizak odaziv menadžerskih pozicija u anketnim istraživanjima (Bednar i Westphal, 2006), odaziv na anketu bio je predviđen.

Najveći dio korištenih podataka odnosi se na primarne podatke prikupljene pomoću strukturiranog elektroničkog upitnika. Također, u istraživanju su se, pored primarnih podataka, koristili i sekundarni podaci (*podaci o industrijskoj pripadnosti, ostvarenom prihodu, broju zaposlenih i rezultatu poslovanja*).

5.1.3. Razvoj istraživačkog instrumenta

U cilju pripreme za glavno istraživanje, provedeno je predistraživanje koje uključuje dvije faze. **Prva faza** odnosi se na *kvalitativan dio* istraživanja, a uključuje konzultacije s ekspertima u svrhu provjere sadržajne valjanosti i jasnoće instrumenta istraživanja te *kvantitativan dio* koji se odnosi na anketno pilot testiranje, čija je svrha dobivanje uvida u pouzdanost i valjanost postavljenih pitanja kvantitativnim pristupom.

U **drugoj fazi**, provodi se primarno prikupljanje podataka pomoću strukturiranog elektroničkog anketnog upitnika te istraživanje obuhvaća glavne izvršne menadžere trgovačkih društava (*društvo s ograničenom odgovornosti, dioničko društvo, jednostavno društvo s ograničenom odgovornosti, komanditno društvo te javno trgovačko društvo*).

Tablica 12. Uzorak prema fazama aktivnosti istraživanja

Faza	Aktivnost istraživanja	Uzorak	Veličina uzorka
I. faza	Angažman eksperata	*Provedeno je namjerno uzorkovanje. U uzorak su uključeni eksperti u svrhu provjere sadržajne valjanosti i jasnoće.*	N = 9
	Anketno pilot istraživanje	*Provedeno je namjerno uzorkovanje. U uzorak su uključeni studenti prve godine diplomskog studija Poslovne ekonomije na Ekonomskom fakultetu Sveučilišta u Splitu koji su sudjelovali u simulaciji tržišnog natjecanja kao ključni donositelji odluka. Svrha istraživanja je bila provjera pouzdanosti i valjanosti mjernog modela.*	N = 53
II. Faza	Glavno anketno istraživanje	*U uzorak su uključeni glavni izvršni menadžeri poslovnih organizacija (trgovačkih društva) u Republici Hrvatskoj*	N = 673

Izvor: Izrada autora

U društvenim znanostima, anketni upitnik predstavlja temeljni mjerni instrument za prikupljanje podataka, te je u kontekstu ovog istraživanja, ključno sredstvo u prikupljanju podataka potrebnih za provedbu empirijskog dijela istraživanja. Primjena ankete omogućuje izravno kvantificiranje subjektivnih stavova ispitanika te se smatra korisnom metodom za prikupljanje podataka (Mejovšek, 2008). S obzirom na specifične karakteristike istraživačkog modela, primarno se usmjeravajući na prirodu varijabli koje nisu izravno mjerljive te zahtijevaju posredno mjerenje, prikupljanje podataka je uputno provoditi pomoću strukturiranog elektroničkog upitnika (anketa).

Pregled relevantnih studija pružio je uvid u definicije izabranih varijabli, potencijalne odrednice i načine mjerenja, te dao širu sliku o pojedinoj varijabli kako u procesu upravljanja rizicima tako i njihovoj primjeni u kontekstu kibernetičkih rizika. Sustavan pregled literature nije bio dovoljan kako bi se postiglo doslovno preuzimanje čestica za potrebe razvoja istraživačkog instrumenta. Naime, bilo je potrebno provesti prilagođavanje tvrdnji (mjernih čestica ili indikatora) u anketnom upitniku. S obzirom na potonje, za potrebe razvoja istraživačkog instrumenta angažirani su eksperti te je provedeno pilot istraživanje.

Angažman eksperata

Sukladno Straub et al. (2004), angažman eksperata doprinosi postizanju sadržajne valjanosti mjernih čestica pri čemu je svrha angažmana eksperata procijeniti stupanj u kojem čestice

predstavljaju konstrukt koji mjere. Potrebno je osigurati da korišteni instrument kao skup mjernih čestica (indikatora) mjeri ono što bi trebao mjeriti (Haynes et al., 1995). Kako bi se utvrdila sadržajna valjanost, angažirani su eksperti u području *upravljanja rizicima*, *informacijske odnosno kibernetičke sigurnosti* te *bihevioralne ekonomije*, a koji istovremeno imaju iskustvo u primjeni **SEM metodologije**. Dodatno, eksperti su se očitovali u vezi jasnoće predloženih mjernih čestica.

Sadržajna valjanost se računa prema uputi temeljenoj na radu Lawshe (1975) putem **pokazatelja omjera sadržajne valjanosti** (*engl. Content validity ratio – CVR*). Sukladno navodima Ayre i Scally (2014) i Wilson et al. (2012) riječ je o metodi koja je primijenjena u različitim područjima istraživanja u cilju potvrde sadržajne valjanosti. Tojbi i Sugianto (2006)[40] temeljem pregleda literature u području informacijske sigurnosti, sistematiziraju korištene instrumente u cilju provjere sadržajne valjanosti mjernih čestica, a temeljem istog, vidljiva je primjena CVR pokazatelja u navedenim istraživanjima.

Kako bi se definirao *CVR*, potrebno je svakoj čestici dodijeliti vrijednost na skali od tri stupnja pri čemu vrijedi:

1 - čestica je neophodna u mjerenju konstrukta,

2 - čestica je korisna u mjerenju konstrukta, ali nije nužna,

3 - čestica nema važnost u mjerenju konstrukta.

Odabirom jedne od tri vrijednosti ukazuje se na važnost predložene mjerne čestice. Nakon čega se CVR izračunava prema sljedećem izrazu:

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

Pri čemu je:

$CVR - omjer\ sadržajne\ valjanosti$

$n_e - broj\ eksperata\ koji\ procjenjuju\ pojedinu\ česticu\ kao\ neophodnu\ u\ mjerenju\ konstrukta$

$N - ukupna\ broj\ eksperata\ koji\ su\ sudjelovali\ u\ procjeni\ sadržajne\ valjanosti$

[40] Pregledni rad sadržava uvid u 62 članka objavljena u 5 najistaknutijih časopisa u razdoblju od 1989 do 2005 godine u području informacijske sigurnosti.

Vrijednosti CVR pokazatelja kreću se u rasponu od -1 (*potpuno složna odluka eksperata kako čestica nema važnost u mjerenju konstrukta*) do +1 (*potpuno složna odluka eksperata kako je čestica neophodna u mjerenju konstrukta*), a uspoređuje se sa kritičnom vrijednosti koja je prezentirana u *Tablici 13*, pri čemu se kritična vrijednost mijenja ovisno o broju eksperata.

Tablica 13. Kritične vrijednosti omjera sadržajne valjanosti prema broju angažiranih eksperata

Broj eksperata	Minimalna vrijednost CVR pokazatelja	Minimalan broj eksperata koji procjenjuju pojedinu česticu kao neophodnu
5	0,99	5
6	0,99	6
7	0,99	7
8	0,78	7
9	0,75	7
10	0,62	7
15	0,49	8
20	0,42	9
25	0,37	10
30	0,33	10

Izvor: Lawshe (1975)

Sadržajna valjanost u kontekstu navedenog istraživanja se računa i pomoću **prosječne vrijednosti relativne važnosti** (*engl. Averaged value of relative imporatnce – AVRI*). Riječ je o pokazatelju koji se dobije izračunom aritmetičke sredine svih dodijeljenih vrijednosti kojima se ukazuje na važnost predložene mjerne čestice (Lewis et al., 1995). Ukoliko je većina eksperata procijenila česticu kao potrebnu, pokazatelj AVRI bilježi vrijednost manju od 2.

Uvođenjem kritike prema predloženim mjernim česticama na način da se testira njihova sadržajna valjanost, postiže se snažnije teorijsko uporište kod primjene instrumenta kao osnove tumačenja varijabli i odnosa između varijabli (Bagozzi, 2011). Primjenom CVR i AVRI pokazatelja olakšana je identifikacija mjernih čestica koje je potrebno ukloniti, izmijeniti u cilju poboljšanja njene sadržajne valjanosti.

Pilot istraživanje

U okviru istraživanja u području društvenih znanosti, uobičajeno je prije glavnog istraživanja provesti istraživanje manjeg razmjera, poznato kao pilot istraživanje, a u svrhu dobivanja sugestija za unapređenje glavnog istraživanja (Ismail et al., 2017). Provođenje pilot studije ne pruža samo priliku za identifikacijom potencijalnih problema u postupcima prikupljanja podataka i metodama analize, već i za testiranje izvedivosti cjelovite studije. Na tragu De Vaus (2013), posebno se izdvaja doprinos pilot istraživanja u smislu da otkriva neadekvatni razvoj istraživačkog dizajna. Prepoznavanje izazova istraživanja, čemu doprinosi pilot istraživanje, omogućava istraživačima da osiguraju provođenje glavne studije, optimizirajući pritom vrijeme i resurse. Takav pristup osigurava pouzdanost rezultata i dodatno potvrđuje valjanost korištenih metoda. Stoga, sljedeći segment pripremne faze uključuje pilot istraživanje koje se provodi sa svrhom identifikacije potencijalnih problema u vezi dizajna istraživanja. U razmatranom istraživanju, primjenom pilot istraživanja omogućena je provjera pouzdanosti i valjanosti mjernog instrumenta.

Pilot istraživanje provedeno je u razdoblju od 18. travnja do 28. travnja 2023. godine na grupi studenta prve godine diplomskog studija Poslovne ekonomije na Ekonomskog fakultetu Sveučilišta u Splitu. Naime, ciljano je odabrana grupa studenata koja je u zimskom semestru ak. godine 2022./2023. godine bila upisana na kolegij Marketing menadžment što je osiguralo da se u pilot istraživanje uključe studenti sa iskustvom sudjelovanja u simulaciji tržišnog natjecanja pod nazivom „Marketing game“. Anketa je distribuirana prema potencijalnim ispitanicima pomoću specijaliziranog alata Qualtrics (*Prilog O*), a prilikom poziva na sudjelovanje u istraživanju uključeno je i popratno pismo koje uključuje poveznicu na anketu (*Prilog N*).

5.1.4. Istraživački instrument

Istraživački instrument segmentiran je na šest dijelova (*Tablica 14*). Prvi dio se odnosi na obilježja ispitanika i organizacije koju ispitanici predstavljaju. Drugi dio obuhvaća pitanja koja se odnose na procjenu kibernetičkih rizika kao prijetnje za organizaciju. Treći dio se odnosi na procjenu sposobnosti organizacije u upravljanju kibernetičkim rizicima. Četvrti dio uključuje pitanja vezana uz procjenu namjere da se na razini organizacije upravlja kibernetičkim rizicima. Peti dio obuhvaća pitanja vezana uz procjenu jačine emocija koje se pojavljuju u vezi s

kibernetičkim rizicima. Posljednji, šesti dio ankete sadrži pitanja usporedbe organizacije s drugim poduzećima u industriji te nedavna iskustva u vezi kibernetičkih rizika.

Tablica 14. Varijable i mjerne čestice

Naziv kategorije u okviru korištenih teorija	Oznaka mjere	Varijabla i način mjerenja	Metrika		Prilagođeno prema izvoru
Percepcija kibernetičkog rizika kao prijetnje za poslovanje organizacije	***Procjena vjerojatnosti nastupa kibernetičkog rizika***		Likertova skala od 1-5		
	PROB1	Procijenite vjerojatnost pojave kibernetičkog rizika u organizaciji kojom upravljate	1 - veoma mala vjerojatnost pojave	5 - veoma visoka vjerojatnost pojave	Ogbanufe i Pavur (2022); Vrhovec i Mihelič (2021); Simonet i Teufel (2019); Boss et al. (2015); Tu et al. (2015); Johnston i Warkentin (2010)
	Procijenite vjerojatnost pojave kibernetičkog rizika u organizaciji kojom upravljate		Likertova skala od 1-5		
	PROB2_1	Rizik temeljem kojeg će nastupiti gubitak ili krađa povjerljivih informacija	1 - veoma mala vjerojatnost pojave	5 - veoma visoka vjerojatnost pojave	Ma (2022); Menard et al. (2018)
	PROB2_2	Rizik temeljem kojeg će nastupiti prekid rada ili šteta na informacijsko-komunikacijskoj infrastrukturi (ICT infrastrukturi)	1 - veoma mala vjerojatnost pojave	5 - veoma visoka vjerojatnost pojave	
	PROB2_3	Rizik temeljem kojeg će nastupiti financijski gubitak	1 - veoma mala vjerojatnost pojave	5 - veoma visoka vjerojatnost pojave	Li et al. (2019); Barlett et al. (2017); Barlette et al. (2015); Hearth i Rao (2009)
	PROB2_4	Rizik temeljem kojeg će nastupiti gubitak ugleda	1 - veoma mala vjerojatnost pojave	5 - veoma visoka vjerojatnost pojave	
	Procjena intenziteta utjecaja kibernetičkog rizika		Likertova skala od 1-5		
	SEV1	Kada bi se u organizaciji kojom upravljam realizirao kibernetički rizik	1 - izostao bi negativan utjecaj	5 - ugrozila bi se održivost poslovanja	Slapničar et al. (2022)
	Pod pretpostavkom da kod organizacije kojom upravljam nastupi		Likertova skala od 1-5		
	SEV1_1	… gubitak ili krađa povjerljivih informacija, procjenjujem da bi utjecaj na organizaciju bio	1 - u potpunosti bezopasan	5 - u potpunosti štetan	Vrhovec i Mihelič (2021); Ifinedo (2012); Liang i Xue (2010)
	SEV1_2	… prekid rada ili šteta na ICT infrastrukturi, procjenjujem da bi utjecaj na organizaciju bio	1 - u potpunosti bezopasan	5 - u potpunosti štetan	
	SEV1_3	… kibernetički rizik, procjenjujem da bi utjecaj na financijski gubitak bio	1 - u potpunosti bezopasan	5 - u potpunosti štetan	Barlette et al. (2015); Tu et al. (2015); Vance et al. (2012)
	SEV1_4	… kibernetički rizik, procjenjujem da bi utjecaj na gubitak ugleda bio	1 - u potpunosti bezopasan	5 - u potpunosti štetan	Barlette et al. (2015); Vance et al. (2012)
Percepcija sposobnosti	***Percepcija korisnosti uspostave upravljanja kibernetičkim rizicima u organizaciji***		Likertova skala od 1-5		

Naziv kategorije u okviru korištenih teorija	Oznaka mjere	Varijabla i način mjerenja	Metrika		Prilagođeno prema izvoru
suočavanja organizacije s kibernetičkim rizicima	Upravljanje kibernetičkim rizicima doprinosi				
	EFF1_1	… smanjenju vjerojatnosti pojavljivanja kibernetičkih rizika	1 - u potpunosti se ne slažem	5 - u potpunosti se slažem	Ogbanufe i Pavur (2022); Simonet i Teufel (2019); Barlette et al. (2015); Tu et al. (2015); Ifinedo (2012); Vance et al. (2012)
	EFF1_2	… smanjenju financijskih gubitaka koji nastaju zbog kibernetičkih rizika	1 - u potpunosti se ne slažem	5 - u potpunosti se slažem	
	EFF1_3	… smanjenju negativnog utjecaja na ugled koji nastaje zbog kibernetičkih rizika	1 - u potpunosti se ne slažem	5 - u potpunosti se slažem	
	Percepcija sposobnosti organizacije u upravljanju kibernetičkim rizicima		Likertova skala od 1-5		
	Organizacija kojom upravljam				
	SEFF1_1	... raspolaže financijskim resursima potrebnim za upravljanje kibernetičkim rizicima	1 - u potpunosti se ne slažem	5 - u potpunosti se slažem	Ma (2022); Simonet i Teufel (2019); Li et al. (2019); Menard et al. (2017); Barlette et al. (2015), Vance et al. (2012); Ifinedo (2012); Herath i Rao (2009)
	SEFF1_2	... raspolaže tehničkim resursima *(alati za skeniranje ranjivosti, sustav za otkrivanje upada u mrežu, alati za prevenciju gubitka podataka, alati za zaštitu pristupa podacima, sustavi upravljanja identitetom i pristupom i sl.)* potrebnim za upravljanje kibernetičkim rizicima	1 - u potpunosti se ne slažem	5 - u potpunosti se slažem	
	SEFF1_3	... ima stručnost i znanje potrebno za upravljanje kibernetičkim rizicima	1 - u potpunosti se ne slažem	5 - u potpunosti se slažem	
	SEFF1_4	... može efikasno upravljati kibernetičkim rizicima	1 - u potpunosti se ne slažem	5 - u potpunosti se slažem	
	Percepcija o troškovima upravlja kibernetičkim rizicima u organizaciji		Likertova skala od 1-5		
	Upravljanje kibernetičkim rizicima zahtjeva od organizacije kojom upravljam				
	COST1_1	… značajna ulaganja u tehnologiju i napredna rješenja zaštite od kibernetičkih rizika	1 - u potpunosti se ne slažem	5 - u potpunosti se slažem	Ma (2022); Simonet i Teufel (2019); Li et al. (2019); Menard et al. (2017); Barlette et al. (2015), Vance et al. (2012); Ifinedo (2012); Herath i Rao (2009)
	COST1_2	... mnogo vremena i truda zaposlenika u obrazovanju i treningu	1 - u potpunosti se ne slažem	5 - u potpunosti se slažem	
	COST1_3	… mnogo vremena i truda zaposlenika u uvođenju naprednih tehnologija i kreiranju rješenja zaštite	1 - u potpunosti se ne slažem	5 - u potpunosti se slažem	
Namjera	***Razina namjeravanog upravljanja kibernetičkim rizicima***		Likertova skala od 1-5		
	Poslovna organizacija pod mojim upravljanjem planira u razdoblju od sljedećih 12 mjeseci				
	INT1_1	… poticati aktivnosti kojima je cilj zaštita od kibernetičkih rizika	1 - u potpunosti se ne slažem	5 - u potpunosti se slažem	Stine et al. (2020); Miloš Sprčić et al. (2017); Miloš Sprčić et al. (2015); Barlette et al. (2015); Yoon i Kim
	INT1_2	… ulagati u resurse za potrebe upravljanja kibernetičkim rizicima	1 - u potpunosti se ne slažem	5 - u potpunosti se slažem	

Naziv kategorije u okviru korištenih teorija	Oznaka mjere	Varijabla i način mjerenja	Metrika		Prilagođeno prema izvoru
	INT1_3	… nadograđivati politike i pravila upravljanja kibernetičkim rizicima	1 - u potpunosti se ne slažem	5 - u potpunosti se slažem	(2013) Workman et al. (2008)
	INT1_4	… primjenjivati suvremene standarde upravljanja kibernetičkim rizicima	1 - u potpunosti se ne slažem	5 - u potpunosti se slažem	
	INT1_5	… razvijati plan upravljanja identificiranim kibernetičkim rizicima	1 - u potpunosti se ne slažem	5 - u potpunosti se slažem	
	INT1_6	… jačati svijesti kod zaposlenika o kibernetičkim rizicima i njihovom doprinosu u promicanju sigurnosti organizacije	1 - u potpunosti se ne slažem	5 - u potpunosti se slažem	
Emocije	***Strah***		Likertova skala od 1-5		
	Procijenite razinu straha koju kod Vas stvaraju sljedeće spoznaje:				
	FEAR1_1	Spoznaja da kibernetički rizik može dovesti do gubitka ili krađe povjerljivih informacija koje pripadaju organizaciji kojom upravljam	1 - ne osjećam strah	5 – strah je intenzivno izražen	Vrhovec i Mihelič (2021); Boss et al. (2015)
	FEAR1_2	Spoznaja da kibernetički rizik može utjecati na uspješnost poslovanja organizacije kojom upravljam	1 - ne osjećam strah	5 – strah je intenzivno izražen	
	FEAR1_3	Spoznaja da kibernetički rizik može utjecati na ugled organizacije kojom upravljam	1 - ne osjećam strah	5 – strah je intenzivno izražen	
	Žaljenje		Likertova skala od 1-5		
	U kojoj mjeri biste osjećali žaljenje ako bi organizacija kojom upravljate				
	REG1_1	… pretrpjela kibernetički rizik	1 - ne bih žalio/la	5 - osjećaj žaljenja bi bio intenzivno izražen	Verkijika (2018; 2019); Sommested et al. (2015a)
	REG1_2	... pretrpjela kibernetički rizik, a nisu uloženi raspoloživi resursi za upravljanje kibernetičkim rizicima	1 - ne bih žalio/la	5 - osjećaj žaljenja bi bio intenzivno izražen	Robinson et al. (2021); Verkijika (2018; 2019); Sommested et al. (2015a)
	REG1_3	… pretrpjela kibernetički rizik, što je negativno utjecalo na rezultat poslovanja	1 - ne bih žalio/la	5 - osjećaj žaljenja bi bio intenzivno izražen	Verkijika (2018; 2019); Sommested et al. (2015); Li et al. (2009)
	REG1_4	... pretrpjela kibernetički rizik, što je negativno utjecalo na ugled organizacije	1 - ne bih žalio/la	5 - osjećaj žaljenja bi bio intenzivno izražen	
Kognitivne pristranosti	***Pristranost optimizma temeljena na usporedbi s drugim organizacijama***		Likertova skala od 1-5		
	Kada organizaciju kojom upravljam usporedim s drugom organizacijom usporedne veličine i djelatnosti, uvjerenja sam kako				
	OPBI1_1	… je kibernetički rizik više svojstven drugoj (usporednoj) organizaciji	1 - u potpunosti se ne slažem	5 - u potpunosti se slažem	Chen et al. (2021); Hewitt et al. (2020); Rhee (2012; 2005);

Naziv kategorije u okviru korištenih teorija	Oznaka mjere	Varijabla i način mjerenja	Metrika		Prilagođeno prema izvoru
	OPBI1_2	… je manja vjerojatnost da će se u organizaciji kojom upravljam realizirati kibernetički rizik	1 - u potpunosti se ne slažem	5 - u potpunosti se slažem	
	OPBI1_3	… bi posljedice kibernetičkog rizika manje ugrozile poslovanje organizacije kojom upravljam	1 - u potpunosti se ne slažem	5 - u potpunosti se slažem	
	OPBI1_4	… je organizacija kojom upravljam manje osjetljiva na kibernetičke rizike	1 - u potpunosti se ne slažem	5 - u potpunosti se slažem	
	Pristranost optimizma temeljena na povoljnim povijesnim ishodima		Likertova skala od 1-5		
	Izostanak negativnog iskustva s kibernetičkim rizicima na razini organizacije kojom upravljam, potaknuo bi moje uvjerenje				
	OPBI2_1	… kako je organizacija sigurna od kibernetičkih rizika u sljedećih 12 mjeseci	1 - u potpunosti se ne slažem	5 - u potpunosti se slažem	Ossareh et al. (2021); Chen et al. (2021); Hewitt et al. (2020); Shepperd et al. (2017); Rhee (2012; 2005;);
	OPBI2_2	… da neće biti financijskog gubitka zbog djelovanja kibernetičkih rizika u sljedećih 12 mjeseci	1 - u potpunosti se ne slažem	5 - u potpunosti se slažem	
	OPBI2_3	… da neće biti negativnog utjecaja na ugled organizacije zbog djelovanja kibernetičkih rizika u sljedećih 12 mjeseci	1 - u potpunosti se ne slažem	5 - u potpunosti se slažem	
	Pristranost uvjetovana nedavnim vlastitim iskustvima		Likertova skala od 1-5		
	U zadnjih 12 mjeseci realizirani kibernetički rizik u organizaciji kojom upravljam				
	REC1_1	… rezultirao je gubitkom ili krađom povjerljivih podataka	1 - u potpunosti se ne slažem	5 - u potpunosti se slažem	Izrada autora
	REC1_2	… uzrokovao je financijske gubitke	1 - u potpunosti se ne slažem	5 - u potpunosti se slažem	
	REC1_3	… uzrokovao je negativni utjecaj na ugled	1 - u potpunosti se ne slažem	5 - u potpunosti se slažem	
	Pristranost uvjetovana nedavnim informacijama		Likertova skala od 1-5		
	Na moje mišljenje o kibernetičkim rizicima kao izazovima za poslovanje organizacije kojom upravljam su utjecali				
	REC2_1	… aktualni izvještaji u medijima	1 - u potpunosti se ne slažem	5 - u potpunosti se slažem	Izrada autora
	REC2_2	… aktualni izvještaji za industriju	1 - u potpunosti se ne slažem	5 - u potpunosti se slažem	
	REC2_3	…aktualna iskustva organizacija koja su bila izložena kibernetičkim rizicima	1 - u potpunosti se ne slažem	5 - u potpunosti se slažem	
	REC2_4	… aktualna osobna iskustva iz privatnog života	1 - u potpunosti se ne slažem	5 - u potpunosti se slažem	

Izvor: Izrada autora

U *Prilogu R* nalazi se upitnik pripremljen za glavno istraživanje koji pored pitanja namijenjenih mjerenju ključnih konstrukata, sadržava i pitanja koja se odnose na obilježja pojedinca i organizacije.

Izuzev dijela ankete koji se odnosi na demografske karakteristike, anketa sadržava tvrdnje na koje ispitanik, ovisno o tome u kojoj mjeri navedena tvrdnja opisuje ispitanikova uvjerenja i stavove, izražava svoju razinu slaganja. Korištena je ordinalna Likertova ljestvica sa skalom mjere od 1 do 5.

Sukladno ranije prezentiranom, anketa je distribuirana prema potencijalnim ispitanicima, a prilikom poziva na sudjelovanje u istraživanju uključeno je i popratno pismo koja uključuje poveznicu na anketu (*Prilog P*).

5.2. Rezultati empirijskog istraživanja

U ovom dijelu rada opisani su rezultati empirijskog istraživanja. Zasebno se predstavljaju rezultati *istraživanja s ekspertima*, *pilot istraživanje* te analiza glavnog dijela istraživanja koja se segmentira na *opis uzorka glavnog istraživanja*, *analizu modela prvog reda i analizu modela drugog reda.*

5.2.1. Analiza rezultata istraživanja s ekspertima

U ovom dijelu rada analiziraju se rezultati istraživanja provedenog s ekspertima. Analiza rezultata uključuje opisivanje ekspertne skupine i iznesenih stavova u vezi predloženih mjernih čestica. Analiza je provedena sukladno Lawishovoj metodologiji, opisanoj u dijelu koji se odnosi na razvoj istraživačkog instrumenta.

Sukladno postavljenom modelu procjene namjere upravljanja kibernetičkim rizicima, formirano je 7 konstrukata. Pregledom literature predloženo je 57 čestica kojima će se konstrukti mjeriti. Istraživanje je započelo u ožujku 2023. godine i trajalo je do travnja 2023. godine, a od upućenih 11 molbi za sudjelovanje u istraživanju s ekspertima (*Prilog K i I*), u procjenu sadržajne valjanosti instrumenta istraživanja uključilo se 9 eksperata.

Tablica 15. Instrument istraživanja koji je predmetom analize eksperata

Područje ekspertize	***Skupina varijabli***	***Varijabla (konstrukt)***	***Inicijalno predložen broj čestica***	***Temeljem sugestija eksperata zadržane čestice***	***Temeljem sugestija eksperata dodane čestice***	***Ukupan broj čestica po konstruktu nakon zaključene analize eksperata***
/	*/*	*/*	***(1)***	***(2)***	***(3)***	***(4)=(2)+(3)***
Upravljanje rizicima / Kibernetički rizici	Percepcija o kibernetičkim rizicima kao prijetnji za poslovanje organizacije	*Procjena vjerojatnosti nastupa kibernetičkog rizika*	8	8		8
		Procjena intenziteta utjecaja kibernetičkog rizika	6	4	1	5
	Percepcija o sposobnosti organizacije u upravljanju kibernetičkim rizicima	*Percepcija korisnosti uspostave upravljanja kibernetičkim rizicima u organizaciji*	4	3		3
		Percepcija sposobnosti organizacije u upravljanju kibernetičkim rizicima	5	3		3
		Percepcija o troškovima upravlja kibernetičkim rizicima u organizaciji	3	2	1	3
	Namjera upravljanja kibernetičkim rizicima	*Razina namjeravanog upravljanja kibernetičkim rizicima*	7	5		5
Bihevioralna ekonomija	Emocije	*Strah*	4	3		3
		Žaljenje	4	4		4
	Kognitivne pristranosti	*Pristranost optimizma temeljena na usporedbi s drugim poduzećima*	4	4		4
		Pristranost optimizma temeljena na povoljnim povijesnim ishodima	5	3		3
		Pristranost uvjetovana nedavnim vlastitim iskustvom	3	3		3
		Pristranost uvjetovana nedavnim informacijama	4	3	1	4
Ukupan broj mjernih čestica			**57**	**45**	**3**	**48**

Izvor: Izrada autora

U nastavku je prezentirana struktura ispitanika prema demografskim obilježjima (*Tablica 16*), temeljem čega je vidljivo kako su se svi eksperti izjasnili o spolu pri čemu je u više bilo zastupljenih eksperata ženskog spola.

Tablica 16. Struktura eksperata prema spolu

Spol	Frekvencija	Udio
Muško	4	44,44 %
Žensko	5	55,56 %
Ne želim se izjasniti	/	/
Ukupno	**9**	**100 %**

Izvor: Izrada autora

Među ekspertima najdominantnije su zastupljeni pojedinci sa završenim doktoratom kao razinom obrazovanja (*Tablica 17*).

Tablica 17. Struktura eksperata prema razini obrazovanja

Obrazovanje	Frekvencija	Udio
Visoka stručna sprema	2	22,22 %
Magisterij ili specijalistički poslijediplomski studij	/	/
Doktorat	7	77,78 %
Ukupno	**9**	**100 %**

Izvor: Izrada autora

Temeljem uvida u strukturu eksperata prema radnom mjestu (*Tablica 18*) vidljivo je kako su najzastupljeniji pojedinci iz akademske zajednice i to docenti.

Tablica 18. Struktura eksperata prema radnom mjestu

Struktura eksperata prema radnom mjestu	Frekvencija	Udio
Redoviti profesor/ica	2	22,22 %
Docent/ica	3	33,34 %
Asistent/istraživač	1	11,11 %
Savjetnik/ica za informacijsku sigurnost	1	11,11 %
Direktor/ica	2	22,22 %
Ukupno	**9**	**100 %**

Izvor: Izrada autora

Grupa eksperata bilježi prosjek od 12,44 godina ukupnog radnog iskustva, a struktura radnog iskustva prema grupama je prezentirana u *Tablici 19*.

Tablica 19. Struktura eksperata prema godinama radnog iskustva

Struktura eksperata prema godinama radnog iskustva	Frekvencija	Udio
6 - 10 godina	4	44,45 %
11 - 15 godina	3	33,33 %
16 - 20 godina	1	11,11 %
Preko 20 godina	1	11,11 %
Ukupno	**9**	**100 %**

Izvor: Izrada autora

Eksperti su provodili samoprocjenu razine stručnosti i to za kategorije kako je vidljivo u *Tablici 20* pri čemu je bilo moguće vrednovati razinu stručnosti prema sljedećim ponuđenim razinama: 1 (*Ne poznajem područje*), 2 (*Imam dostatno znanje*), 3 (*Vrlo dobro poznajem*), 4 (E*kspert*). Uočava se kako su eksperti kao grupa najmanju stručnost procijenili u polju odabrane statističke metode namijenjene empirijskom dijelu istraživanja – SEM metodologija. S druge strane, najviše stručnosti procjenjuju u polju kibernetičkih rizika.

Tablica 20. Samoprocjena razine ekspertize

Struktura eksperata prema razini ekspertize u izdvojenim područjima	Prosječna vrijednost samoprocjene razine stručnosti
Upravljanje rizicima	2,89
Kibernetički rizici	3,44
Bihevioralna ekonomija	2,89
SEM metodologija	2,78

Izvor: Izrada autora

Za procjenu sadržajne valjanosti izračunati su omjer sadržajne valjanosti (CVR) i prosječna vrijednosti relativne važnosti (AVRI) kako je opisano u potpoglavlju 5.1.3.

Na temelju dobivenih rezultata (*Prilog M*) iz mjernog instrumenta isključene su čestice koje su imale vrijednost CVR < 0,75. Riječ je o graničnoj (minimalnoj) vrijednosti koja je definirana za 9 eksperata prema Lawsheovom kriteriju kao i one čestice koje su imale AVRI > 2.

Tablica 21. Rezultati procjene valjanosti predloženih čestica od strane eksperata

	Mjerne čestice	**Struktura u odnosu na predložen broj čestica**
Predložen broj čestica	57	**100 %**
CVR pokazatelj < 0,75	12	21,05 %
AVRI pokazatelj >2	/	/
Dodane čestice prema sugestiji eksperata	3	5,26 %
Ukupna broj čestica	**48**	84,21 %

Oznake: CVR - omjer sadržajne valjanosti; AVRI - prosječna vrijednost relativne valjanosti

Izvor: Izrada autora

Eksperti su bili složni da se iz razmatranja izuzme 12 čestica za koje je procijenjeno kako nemaju važnost u mjerenju konstrukata. Ujedno, eksperti su predložili tri dodatne čestice kojima se mjeri: *intenzitet utjecaja kibernetičkog rizika/prijetnje za organizaciju* (1 dodana čestica), *percepcija o troškovima upravljanja kibernetičkim rizicima u organizaciji* (1 dodana čestica) te *utjecaj nedavnog iskustva* (1 dodana čestica). S obzirom da je od eksperata zatraženo da se procijeni jasnoća (razumljivost) mjernih čestica, valja ukazati kako su eksperti predložili vrijedne sugestije u cilju promicanja jasnoće mjernih čestica.

5.2.2. Analiza rezultata pilot istraživanja

U nastavku se opisuje pilot istraživanje što uključuje opis uzorka istraživanja te analizu rezultata. *Tablica 22* prezentira distribuciju studenata prema spolu, pri čemu su svi ispitanici naveli svoj spol. Utvrđeno je da ispitanice čine dominantnu grupu s udjelom od 77,4 %, dok ispitanici predstavljaju 22,6 % ukupnog uzorka.

Tablica 22. Struktura studenata prema spolu

Spol	**Frekvencija**	**Udio**
Muško	12	22,6 %
Žensko	41	77,4 %
Ne želim se izjasniti	/	/
Ukupno	**53**	**100 %**

Izvor: Izrada autora

Sukladno *Tablici 23*, najzastupljeniji upisan studijski smjer među studentima unutar uzorka bio je smjer Računovodstvo i revizija s 28,3 % studenata. Smjer Financijski menadžment sljedeći je najzastupljeniji s udjelom od 22,6 %, dok su smjerovi Menadžment i Informatički menadžment zastupljeni s približno jednakim udjelima, odnosno 18,9 % i 17,0 %. Najmanje zastupljen studijski smjer među studentima uključenim u istraživanje bio je Marketing s udjelom od 13,2 %. Prosječna dob studenata uključenih u istraživanje iznosila 24 i pol godine.

Tablica 23. Struktura studenata prema studijskom smjeru

Studijski smjer	Frekvencija	Udio
Financijski menadžment	12	22,64 %
Informatički menadžment	9	16,98 %
Menadžment	10	18,87 %
Marketing	7	13,21 %
Računovodstvo i revizija	15	28,30 %
Ukupno	**53**	**100 %**

Izvor: Izrada autora

Tablica 24 pruža uvid koliko je studenata u uzorku pohađalo edukaciju na temu kibernetičkih rizika ili kibernetičke sigurnosti ili informacijskih rizika te koliko je među njima samoinicijativno istraživalo razmatrano područje. U uzorku je 9,4 % ispitanika navelo je da je pohađalo barem neki oblik edukacije, dok je dominantna većina, 86,8 %, navela kako nije pohađala edukaciju. Preostalih 3,8 % ispitanika bilo je neodlučno ili nije moglo precizno potvrditi jesu li pohađali relevantnu edukaciju. Što se tiče samoinicijative istraživanja kibernetičkih rizika ili kibernetičke sigurnosti ili informacijskih rizika, u uzorku se potvrđuje kako je 30,2 % ispitanika istaknulo da su samostalno istraživali barem neku od navedenih tema, dok je 62,3 % izjavilo, sasvim suprotno, kako nisu istraživali.

Među ispitanicima koji su pohađali edukaciju, 60 % je samoinicijativno istraživalo navedena područja. Kod studenata koji nisu pohađali formalni oblik edukacije, 26,1 % je pokazalo samoinicijativu za istraživanje ovih područja, dok većina, 65,2 %, nije pokazala interes za dodatnim razumijevanjem područja kibernetičkih rizika i njima srodnih područja.

Tablica 24. Struktura studenata prema pohađanju edukacije i samoinicijativnom istraživanju teme kibernetičkih rizika i sigurnosti

			Samoinicijativno istraživanje			Ukupno
			Da	Ne	Nisam siguran/a	
Pohađanje edukacije	Da	N	3	2	0	**5**
		Udio	60,0 %	40,0 %	0,0 %	**100 %**
	Ne	N	12	30	4	**46**
		Udio	26,1 %	65,2 %	8,7 %	**100 %**
	Nisam siguran/a	N	1	1	0	**2**
		Udio	50,0 %	50,0 %	0,0 %	**100 %**
Ukupno		**N**	**16**	**33**	**4**	**53**
		Udio	**30,2 %**	**62,3 %**	**7,5 %**	**100 %**

Izvor: Izrada autora

Temeljem analize strukture ispitanika prema tržišnom mjestu koje su zauzeli u simulaciji tržišnog natjecanja (*Tablica 25*), uočava se kako je 28,3 % ispitanika zauzelo prvo mjesto u industriji. Udio studenata koji su u tržišnom natjecanju zauzeli drugo i treće mjesto pojedinačno je iznosilo 26,4 %. Četvrto mjesto je zauzelo 15,1 % ispitanika. Najmanje studenata uključenih u pilot istraživanje, njih 3,8 %, zauzelo je peto mjesto u igri tržišnog natjecanja.

Tablica 25. Struktura studenata prema tržišnom mjestu koje su zauzeli u simulaciji/igri tržišnog natjecanja

Studijski smjer	Frekvencija	Udio
1. mjesto u industriji	15	28,3 %
2. mjesto u industriji	14	26,4 %
3. mjesto u industriji	14	26,4 %
4. mjesto u industriji	8	15,1 %
5. mjesto u industriji	2	3,8 %
Ukupno	**53**	**100 %**

Izvor: Izrada autora

U cilju razvoja istraživačkog instrumenta primijenjen je kvantitativan pristup, a riječ je o analizi podataka dobivenih u okviru pilot istraživanja. U okviru pilot istraživanja ukupno su razmotrene 52 mjerne čestice (anketna pitanja) pri čemu je većina pitanja, njih 48, dobilo odgovarajuću potvrdu kroz angažman eksperata, a s obzirom da je bilo moguće provesti

evaluaciju za dodatna pitanja, odlukom istraživača su dodatna 4 pitanja. U nastavku je vidljiva *Tablica 26* koja prikazuje distribucije mjernih čestica (anketnih pitanja) prema područjima ekspertize, skupinama varijabli (konstrukata) i konstruktima.

Tablica 26. Proces odabira mjernih čestica namijenjenih pilot istraživanju

Područje ekspertize	***Skupina varijabli***	***Varijabla (konstrukt)***	***Inicijalno predložen broj čestica (pitanja)***	***Temeljem sugestija eksperata zadržane čestice***	***Temeljem sugestija eksperata dodane ili izmijenjene čestice***	***Ukupan broj čestica po konstruktu nakon zaključene analize eksperata***	***Odlukom istraživača zadržane čestice kako bi se testirale u okviru pilot istraživanja***	***Ukupno zadržano čestica u provedbi pilot istraživanja***
/	*/*	*/*	***(1)***	***(2)***	***(3)***	***(4)=(2)+(3)***	***(5)***	***(6)=(4)+(5)***
Upravljanje rizicima / Kibernetički rizici	Percepcija o kibernetičkim rizicima kao prijetnji za poslovanje organizacije	*Procjena vjerojatnosti nastupa kibernetičkog rizika*	8	8		8		8
		Procjena intenziteta utjecaja kibernetičkog rizika	6	4	1	5		5
	Percepcija o sposobnosti organizacije u upravljanju kibernetičkim rizicima	*Percepcija korisnosti uspostave upravljanja kibernetičkim rizicima u organizaciji*	4	3		3	1	4
		Percepcija sposobnosti organizacije u upravljanju kibernetičkim rizicima	5	3		3	1	4
		Percepcija o troškovima upravlja kibernetičkim rizicima u organizaciji	3	2	1	3		3
	Namjera upravljanja kibernetičkim rizicima	*Razina namjeravanog upravljanja kibernetičkim rizicima*	7	5		5	1	6
Bihevioralna ekonomija	Emocije	*Strah*	4	3		3	1	4
		Žaljenje	4	4		4		4
	Kognitivne pristranosti	*Pristranost optimizma temeljena na usporedbi s drugim poduzećima*	4	4		4		4
		Pristranost optimizma temeljena na povoljnim povijesnim ishodima	5	3		3		3
		Pristranost uvjetovana	3	3		3		3

Područje ekspertize	*Skupina varijabli*	*Varijabla (konstrukt)*	*Inicijalno predložen broj čestica (pitanja)*	*Temeljem sugestija eksperata zadržane čestice*	*Temeljem sugestija eksperata dodane ili izmijenjene čestice*	*Ukupan broj čestica po konstruktu nakon zaključene analize eksperata*	*Odlukom istraživača zadržane čestice kako bi se testirale u okviru pilot istraživanja*	*Ukupno zadržano čestica u provedbi pilot istraživanja*
/	*/*	*/*	*(1)*	*(2)*	*(3)*	*(4)=(2)+(3)*	*(5)*	*(6)=(4)+(5)*
		nedavnim vlastitim iskustvom						
		Pristranost uvjetovana nedavnim informacijama	4	3	1	4		4
Ukupan broj mjernih čestica			**57**	**45**	**3**	**48**	**4**	**52**

Izvor izrada autora

Nakon što su prikupljeni podaci u okviru pilot istraživanja, uslijedila je kvantitativna analiza. U okviru pilot istraživanja, glavni cilj bio je provjeriti pouzdanost i valjanost mjernih čestica. Pouzdanost mjernih čestica potvrđena je korištenjem Cronbach alfe, koja procjenjuje unutarnju konzistentnost skupa čestica, pri čemu vrijednost bliže 1 sugerira visoku pouzdanost. Osim toga, CR služi kao dodatni pokazatelj pouzdanosti, s prihvaćenim vrijednostima koje su veće od 0,7. Valjanost mjernih čestica ocijenjena je kroz nekoliko metoda. Konvergentna valjanost procijenjena je koristeći AVE, gdje vrijednost veća od 0,5 ukazuje na adekvatnu valjanost. Korišten je kriteriji HTMT, koji pruža uvid u diskriminantnu valjanost. Provedeni koraci osiguravaju sveobuhvatan pristup u validaciji mjernih čestica, udovoljavajući standardima primjene SEM metodologije.

Proveden je test pouzdanosti i valjanosti mjernih čestica modela koji sadržava 52 mjerne čestice, te modela koji zadržava 47 mjernih čestica. Pregled rezultata provedenog testa vidljiv je u *Tablici 27*. Analizirajući percepciju o kibernetičkim rizicima kao poslovnoj prijetnji, uočava se kako smanjenje broja mjernih čestica za procjenu vjerojatnosti nastupa kibernetičkog rizika s 8 na 5 dovodi do blagog pada Cronbach alfa koeficijenta s 0,825 na 0,805, dok je CR pokazatelj marginalno smanjen s 0,866 na 0,863. Važno je napomenuti da je AVE pokazatelj povećan s 0,454 na 0,559. Slično tome, pri analizi percepcije o sposobnosti organizacije u upravljanju kibernetičkim rizicima, smanjenje broja čestica za percepciju korisnosti uspostave upravljanja s 4 na 3 rezultiralo je padom Cronbach alfa s 0,916 na 0,906, uz marginalno smanjenje CR-a s 0,939 na 0,938. Međutim, AVE je zabilježio rast s 0,795 na 0,836.

Tablica 27. Proces odabira mjernih čestica namijenjenih glavnom istraživanju

Područje ekspertize	*Skupina varijabli*	*Varijabla (konstrukt)*	*Čestice testirane u okviru pilot istraživanja*	*Cronbach alpha*	*CR*	*AVE*	*Čestice testirane u okviru pilot istraživanja*	*Cronbach alpha*	*CR*	*AVE*
			52 mjerne čestice testirane				*47 mjernih čestica testirano*			
Upravljanje rizicima / Kibernetički rizici	Percepcija o kibernetičkim rizicima kao prijetnji za poslovanje organizacije	*Procjena vjerojatnosti nastupa kibernetičkog rizika*	8	0,825	0,866	0,454	5	0,805	0,863	0,559
		Procjena intenziteta utjecaja kibernetičkog rizika	5	0,905	0,928	0,722	5	0,905	0,928	0,722
	Percepcija o sposobnosti organizacije u upravljanju kibernetičkim rizicima	*Percepcija korisnosti uspostave upravljanja kibernetičkim rizicima u organizaciji*	4	0,916	0,939	0,795	3	0,906	0,938	0,836
		Percepcija sposobnosti organizacije u upravljanju kibernetičkim rizicima	4	0,921	0,942	0,803	4	0,921	0,942	0,803
		Percepcija o troškovima upravlja kibernetičkim rizicima u organizaciji	3	0,882	0,928	0,811	3	0,882	0,928	0,811
	Namjera upravljanja kibernetičkim rizicima	*Razina namjeravanog upravljanja kibernetičkim rizicima*	6	0,968	0,974	0,864	6	0,968	0,974	0,864
Bihevioralna ekonomija	Emocije	*Strah*	4	0,924	0,947	0,816	3	0,937	0,959	0,887
		Žaljenje	4	0,889	0,924	0,754	4	0,889	0,924	0,754
	Kognitivne pristranosti	*Pristranost optimizma temeljena na usporedbi s drugim poduzećima*	4	0,846	0,780	0,491	4	0,846	0,773	0,482
		Pristranost optimizma temeljena na povoljnim povijesnim ishodima	3	0,947	0,964	0,900	3	0,947	0,964	0,899
		Pristranost uvjetovana nedavnim vlastitim iskustvom	3	0,921	0,950	0,863	3	0,921	0,950	0,863
		Pristranost uvjetovana nedavnim informacijama	4	0,708	0,765	0,470	4	0,708	0,759	0,464
Ukupan broj mjernih čestica			**52**	/	/	/	**47**	/	/	/

Izvor: Izrada autora

Kada se analizira emocija straha, zapaženo je kako smanjenje broja mjernih čestica s 4 na 3 dovodi do povećanja Cronbach alfa s 0,924 na 0,937, povećanja CR-a s 0,947 na 0,959 te rasta AVE s 0,816 na 0,887. Za emociju žaljenje nije bilo značajnih promjena. U pogledu kognitivnih pristranosti, za pristranost optimizma temeljenu na usporedbi s drugim poduzećima, iako broj čestica ostaje nepromijenjen, CR se blago smanjio s 0,780 na 0,773, dok se AVE smanjen s 0,491 na 0,482. Slično tome, pristranost dostupnosti pokazuje marginalno smanjenje CR-a s 0,765 na 0,759 i AVE-a s 0,470 na 0,464, uz konstantan broj čestica. Za ostale analizirane varijable nisu zabilježene promjene.

Premda su u oba razmatrana modela koja se razlikuju prema broju mjernih čestica prisutne vrijednosti AVE pokazatelja nešto niže od preporučenih 0,5, za iste konstrukte je utvrđena vrijednost CR pokazatelja veća od 0,7. Kako je riječ o pokazatelju koji također doprinosi zaključku o konvergentnoj valjanosti, zauzima se stav, sukladan Lam (2012), kako je varijabla udovoljila zahtjevima znanstvene metodologije koja će se primijeniti u okviru glavnog istraživanja.

Dodatno se ispituje diskriminantna valjanost pomoću HTMT pokazatelja, a s obzirom da su sve vrijednosti ispod 0,85, smatra se da je kriterij diskriminatne valjanosti ispunjen u slučaju modela koji sadržava 52 mjerne čestice (*Tablica 28*).

Tablica 28. Rezultati analize diskriminantne valjanosti prema HTMT pokazatelju – pilot istraživanje

	COST1	EFF1	FEA1	INT1	OPBI1	OPBI2	PROB	REC1	REC2	REG1	SEFF1	SEV
COST1												
EFF1	0,476											
FEA1	0,500	0,335										
INT1	0,438	0,315	0,485									
OPBI1	0,114	0,267	0,162	0,392								
OPBI2	0,105	0,214	0,051	0,044	0,455							
PROB	0,576	0,213	0,533	0,342	0,228	0,156						
REC1	0,141	0,121	0,361	0,070	0,449	0,236	0,381					
REC2	0,514	0,340	0,196	0,395	0,394	0,229	0,367	0,121				
REG1	0,409	0,488	0,765	0,566	0,252	0,112	0,272	0,110	0,212			
SEFF1	0,107	0,160	0,100	0,329	0,399	0,087	0,180	0,306	0,122	0,100		
SEV	0,341	0,312	0,348	0,135	0,212	0,314	0,596	0,213	0,210	0,170	0,165	

Izvor: Izrada autora

Također, diskriminantna valjanosti je potvrđena i u slučaju modela koji sadržava 47 mjernih čestica (*Tablica 29*).

Tablica 29. Rezultati analize diskriminantne valjanosti prema HTMT pokazatelju – pilot istraživanje

	COST1	EFF1	FEA1	INT1	OPBI1	OPBI2	PROB	REC1	REC2	REG1	SEFF1	SEV
COST1												
EFF1	0,486											
FEA1	0,471	0,326										
INT1	0,440	0,296	0,491									
OPBI1	0,114	0,273	0,157	0,404								
OPBI2	0,105	0,210	0,053	0,050	0,455							
PROB	0,473	0,108	0,514	0,303	0,214	0,138						
REC1	0,141	0,126	0,345	0,078	0,449	0,236	0,382					
REC2	0,514	0,324	0,186	0,392	0,394	0,229	0,259	0,121				
REG1	0,409	0,474	0,764	0,574	0,252	0,112	0,273	0,110	0,212			
SEFF1	0,107	0,154	0,089	0,343	0,399	0,087	0,176	0,306	0,122	0,100		
SEV	0,341	0,281	0,315	0,138	0,212	0,314	0,594	0,213	0,210	0,170	0,165	

Izvor: Izrada autora

Temeljem analize zaključuje se kako kvaliteta mjernih svojstava, usprkos smanjenju broja pitanja, nije narušena. U cilju optimizacije broja čestica u upitniku, što je posebno korisno s aspekta povećanja vjerojatnosti dobivanja odgovora na anketu, odlučeno je da se u glavnom istraživanju koristi 47 mjernih čestica. Naime, sužavanje upitnika povećava vjerojatnost sudjelovanja ispitanika u istraživanju, što doprinosi uspješnosti provedbe prikupljanja podataka, a što je posebno važno kada je proučavana populacija glavnih izvršnih menadžera.

U nastavku, u okviru *Tablice 30,* prezentirana je konačna struktura mjernih čestica pri čemu se 47 mjernih čestica odnose na konstrukte predviđene teorijom motivacije za zaštitom te bihevioralnom ekonomijom. Navedenom je pridodano 9 pitanja koja se odnose na obilježja glavnog izvršnog menadžera i poslovnih organizacija.

Tablica 30. Konačna struktura mjernih čestica (pitanja) u instrumentu istraživanja

Područje ekspertize	***Skupina varijabli***	***Varijabla (konstrukt)***	***Finalna struktura pitanja u instrumentu istraživanja***
Upravljanje rizicima / Kibernetički rizici	Percepcija o kibernetičkim rizicima kao prijetnji za poslovanje organizacije	*Procjena vjerojatnosti nastupa kibernetičkog rizika*	5
		Procjena intenziteta utjecaja kibernetičkog rizika	5
	Percepcija o sposobnosti organizacije u upravljanju kibernetičkim rizicima	*Percepcija korisnosti uspostave upravljanja kibernetičkim rizicima u organizaciji*	3
		Percepcija sposobnosti organizacije u upravljanju kibernetičkim rizicima	4
		Percepcija o troškovima upravlja kibernetičkim rizicima u organizaciji	3
	Namjera upravljanja kibernetičkim rizicima	*Razina namjeravanog upravljanja kibernetičkim rizicima*	6
Bihevioralna ekonomija	Emocije	*Strah*	3
		Žaljenje	4
	Kognitivne pristranosti	*Pristranost optimizma temeljena na usporedbi s drugim poduzećima*	4
		Pristranost optimizma temeljena na povoljnim povijesnim ishodima	3
		Pristranost uvjetovana nedavnim vlastitim iskustvom	3
		Pristranost uvjetovana nedavnim informacijama	4
Mjerne čestice vezana uz karakteristike poslovne organizacije i karakteristike glavnog izvršnog menadžera			**9**
Ukupan broj mjernih čestica			**56**

Izvor: Izrada autora

5.2.3. Opis uzorka glavnog istraživanja

Uzorak glavnog istraživanja čine 673 glavna izvršna menadžera koji predstavljaju trgovačka društva kojima upravljaju (poslovnu organizaciju). Deskriptivnom statistikom cilj je utvrditi osnovne karakteristike uzorka istraživanja što je provedeno u statističkom paketu Statistical Package for the Social Sciences 24 (SPSS 24).

Sudionici u anketi uglavnom su se identificirali kao muškarci, čineći 63,2 % ukupnog uzorka. Muškarci u dobi od 36-45 i 46-55 godina najzastupljenije su podskupine, čineći 21,0 % i 20,1 % ukupnih ispitanika. Žene su činile 35,7 % ukupnog uzorka. Najbrojnija dobna skupina unutar ženske grupe ispitanika bila je 46-55 godina starosti, predstavljajući 13,8 % ukupnih ispitanika. Marginalnih 1,2 % ukupnih sudionika odlučilo se ne izjasniti u vezi spola. Što se tiče dobi za sve ispitanike, kategorija dobi 46-55 najviše je zastupljena, čineći 34,5 % ukupnih ispitanika. Odmah za njom slijedi kategorija 36-45, koja čini 32,2 % ukupnog broja. Nasuprot tome, kategorija dobi 18-25 bila je najmanje zastupljena, čineći tek 0,7 % ukupnog uzorka.

Tablica 31. Struktura glavnih izvršnih menadžera prema dobi i spolu

			Dob						Ukupno
			18-25	26-35	36-45	46-55	56-65	66 i više	
Spol	Muško	N	2	35	141	135	86	26	**425**
		Udio	0,30 %	5,20 %	21,00 %	20,10 %	12,80 %	3,90 %	**63,20 %**
	Žensko	N	3	35	74	93	30	5	**240**
		Udio	0,40 %	5,20 %	11,00 %	13,80 %	4,50 %	0,70 %	**35,70 %**
	Ne želim se izjasniti	N	0	1	2	4	1	0	**8**
		Udio	0,00 %	0,10 %	0,30 %	0,60 %	0,10 %	0,00 %	**1,20 %**
Ukupno		N	**5**	**71**	**217**	**232**	**117**	**31**	**673**
		Udio	**0,70 %**	**10,50 %**	**32,20 %**	**34,50 %**	**17,40 %**	**4,60 %**	**100 %**

Izvor: Izrada autora

Ispitanici su svrstani u pet kategorija obrazovanja: srednja stručna sprema, viša stručna sprema, visoka stručna sprema, magisterij ili specijalistički poslijediplomski studij te doktorat. Najveći postotak glavnih izvršnih menadžera (47,55 %) ima visoku stručnu spremu. Podaci ukazuju na visoku razinu formalnog obrazovanja među ispitanicima. Srednja stručna sprema i viša stručna sprema su podjednako zastupljene među ispitanicima, svaka s udjelom od 15,90 %.

Dodatno, 18,13 % ispitanika je steklo magisterij ili je završilo specijalistički poslijediplomski studij. Ovaj podatak sugerira da postoji značajan broj ispitanika koji su ostvarili visoku razinu specijalizacije u svojem obrazovanju. Najmanje zastupljena kategorija obrazovanja je doktorat, sa svega 2,53 % ispitanika.

Tablica 32. Struktura glavnih izvršnih menadžera prema obrazovanju

Obrazovanje	Frekvencija	Udio	Kumulativ
Srednja stručna sprema	107	15,90 %	15,90 %
Viša stručna sprema	107	15,90 %	31,80 %
Visoka stručna sprema	320	47,55 %	79,35 %
Magisterij ili specijalistički poslijediplomski studij	122	18,13 %	97,47 %
Doktorat	17	2,53 %	100 %
Ukupno	**673**	**100 %**	

Izvor: Izrada autora

Tablica 33 prikazuje distribuciju ispitanika prema godinama iskustva rada na poziciji glavnog izvršnog menadžera. Najveći udio ispitanika, čak 59,88 %, ima više od deset godina iskustva na navedenoj poziciji. Najmanje su zastupljeni ispitanici s manje od godinu dana iskustva, samo 3,27 %. Analizom se potvrđuje kako značajan broj ispitanika iskazuje dugogodišnje iskustvo, konkretnije, čak 75,48 % ispitanika bilježi 7 ili više godina iskustva rada na poziciji glavnog izvršnog menadžera.

Tablica 33. Struktura glavnih izvršnih menadžera prema godinama iskustva rada na poziciji glavnog izvršnog menadžera

Iskustvo rada	Frekvencija	Udio	Kumulativ
<1	22	3,27 %	3,27 %
1-3	53	7,88 %	11,14 %
4-6	90	13,37 %	24,52 %
7-10	105	15,60 %	40,12 %
>10	403	59,88 %	100 %
Ukupno	**673**	**100 %**	

Izvor: Izrada autora

Od ukupnog broja ispitanika, 32,2 % je izjavilo da nije imalo prethodnog iskustva u IT zadacima. Među njima, 18,1% nije imalo iskustva u upravljanju rizicima, dok je 7,4 % imalo značajno (>5 godina) iskustvo u poslovima upravljanja rizicima. Od ukupnog broja ispitanika, 28,1 % izjavilo je da nije imalo prethodnog iskustva na zadacima upravljanja rizicima. Među njima, 56,2 % nije imalo iskustva rada na IT zadacima. S druge strane, 23,0 % ispitanika koji nemaju iskustva rada na IT zadacima, imaju više od pet godina iskustva u poslovima upravljanja rizicima. Oni koji su radili na IT zadacima manje od godinu dana činili su 7,6 % ukupnog broja ispitanika. U ovoj skupini, 41,2 % ima manje od godinu dana iskustva u upravljanju rizicima, dok 21,6 % ima više od pet godina iskustva u istom.

Ispitanici s iskustvom od 1 do 5 godina na IT poslovima činili su 19,9 % ukupnog uzorka. Unutar ove kategorije, najzastupljenija grupa s 39,4 % ima iskustvo od 1-5 godina u upravljanju rizicima. Slijedi ih grupa s više od pet godina iskustva u poslovima upravljanja rizicima, čineći 28,0 % unutar ove kategorije. Ispitanici s više od pet godina iskustva na IT zadacima predstavljali su najveću skupinu, čineći 40,6 % svih ispitanika. Od ovih, dominantna grupa (70,0%) također ima više od pet godina iskustva u upravljanju rizicima. Sveukupno, 42,9 % ispitanika ima više od pet godina iskustva u upravljanju rizicima, dok 28,1 % nije imalo ranija iskustva na IT zadacima.

Tablica 34. Struktura glavnih izvršnih menadžera prema iskustvu rada na IT zadacima i zadacima upravljanja rizicima

			Iskustvo rada na zadacima upravljanja rizicima (god.)				Ukupno
			Nemam ranija iskustva	<1	1-5	>5	
Iskustvo rad na IT zadacima (god.)	Nemam ranija iskustva	N	122	11	34	50	**217**
		Udio	56,2 %	5,1 %	15,7 %	23,0 %	**100 %**
	<1	N	11	21	8	11	**51**
		Udio	21,6 %	41,2 %	15,7 %	21,6 %	**100 %**
	1-5	N	27	16	52	37	**132**
		Udio	20,5 %	12,1 %	39,4 %	28,0 %	**100 %**
	>5	N	29	13	40	191	**273**
		Udio	10,6 %	4,8 %	14,7 %	70,0 %	**100 %**
Ukupno		N	**189**	**61**	**134**	**289**	**673**
		Udio	**28,1 %**	**9,1 %**	**19,9 %**	**42,9 %**	**100 %**

Izvor: Izrada autora

Tablica 35 prikazuje distribuciju poslovnih subjekata (trgovačkih društava) iz uzorka po različitim sektorima i veličini (pri čemu je veličina određena brojem zaposlenih u poslovnoj organizaciji) te strukturu uspoređuje u odnosu na populaciju (okvir uzorka).

U uzorku se izdvaja sektor M s najvećom zastupljenošću od 24,81 %, međutim, navedeni sektor je zastupljen na razini od 11,77 % među populacijom poslovnih organizacija. Razlika ukazuje na značajnu zastupljenost sektora M u uzorku u usporedbi s ukupnom populacijom. Značajnije odstupanje vidljivo je u sektoru J u smislu da je veća zastupljenost poduzeća iz sektora J u uzorku u odnosu na populaciju. Sektor G i sektor C također čine značajan dio uzorka s 15,90 % odnosno 16,34 %. Međutim, njihov udio u populaciji je nešto veći i iznosi 19,82 % odnosno 17,88 %, što ukazuje na blagu podzastupljenost u uzorku. Sektor F predstavlja 6,98 % uzorka, ali doprinosi znatno većem udjelu populacije (16,54 %). To sugerira da je građevinski sektor izrazito podzastupljen u uzorku. Među značajnije podzastupljenim sektorom unutar uzorka u odnosu na populaciju izdvaja se sektor I. Ostali sektori imaju odstupanja zastupljenosti u uzorku u odnosu na populaciju u rasponu manjem od 2,3 p.p. Usporedba strukture poslovnih organizacija između uzorka i ukupne populacije sugerira da postoji nesklad, a zaključku o odstupanju doprinose sektori M, F, J i I (poredani prema apsolutnom odstupanju).

U uzorku pretežito dominiraju manja poduzeća pri čemu 42,94 % je zapošljavalo između 5 i 10 zaposlenih, a 15,90 % manje od 5 zaposlenih. Navedeni podaci prilično dobro oslikavaju strukturu unutar populacije gdje poduzeća u kategoriji zapošljavanja 5 do 10 zaposlenika čine 44,58 %, a ona s manje od 5 zaposlenih 18,57 %. Kada se usporedi struktura poslovnih organizacija prema veličini u uzorku i u populaciji, odstupanja su relativno mala. Stoga se uzorak prema kriteriju veličine može razmatrati kao adekvatan u prikazu populacije, posebno uzimajući u obzir izazov savršenog preslikavanja složenog poslovnog okružja.

Tablica 35. Pregled poslovnih organizacija u uzorku prema kriteriju industrijska pripadnost i veličini mjerenoj brojem zaposlenih

Djelatnost (Industrija)	*<5*	*5-10*	*11-20*	*21-50*	*51-100*	*101-249*	*>249*	Ukupno	Struktura uzorka (1)	Struktura populacije (2)	Razlika (3)=(1)-(2)
A - poljoprivreda, šumarstvo i ribarstvo	2	4	4					10	1,49 %	2,24 %	-0,75 p.p.
B - rudarstvo i vađenje				1				1	0,15 %	0,30 %	-0,15 p.p.
C - prerađivačka industrija	13	38	16	18	14	4	7	110	16,34 %	17,88 %	-1,54 p.p.
D - opskrba električnom energijom, plinom, parom i klimatizacija					1		1	2	0,30 %	0,30 %	0,00 p.p.
E - opskrba vodom; uklanjanje otpadnih voda, gospodarenje otpadom te djelatnosti sanacije okoliša		3	4	3	1	2	1	14	2,08 %	1,49 %	0,59 p.p.
F - građevinarstvo	2	16	11	11	3	4		47	6,98 %	16,54 %	-9,56 p.p.
G - trgovina na veliko i na malo; popravak motornih vozila i motocikala	17	57	17	13	2		1	107	15,90 %	19,82 %	-3,92 p.p.
H - prijevoz i skladištenje	6	4	2	7	2	1	1	23	3,42 %	4,47 %	-1,05 p.p.
I - djelatnosti pružanja smještaja te pripreme i usluživanja hrane	6	8	8	4	4	1	1	32	4,75 %	10,58 %	-5,83 p.p.
J - informacije i komunikacije	12	30	13	16	1	3	2	77	11,44 %	4,77 %	6,67 p.p.
K - financijske djelatnosti i djelatnosti osiguranja		2		1				3	0,45 %	0,30 %	0,15 p.p.
L - poslovanje nekretninama	1	6	5					12	1,78 %	1,19 %	0,59 p.p.
M - stručne, znanstvene i tehničke djelatnosti	35	93	24	13	2			167	24,81 %	11,77 %	13,04 p.p.
N - administrativne i pomoćne uslužne djelatnosti	8	18	8	1	4	3		42	6,24 %	4,02 %	2,22 p.p.
O - javna uprava i obrana; obvezno socijalno osiguranje	/	/	/	/	/	/	/	/	0,00 %	0,00 %	0,00 p.p.
P - obrazovanje	1	2	2					5	0,74 %	0,75 %	-0,01 p.p.
Q - djelatnosti zdravstvene zaštite i socijalne skrbi	1	4	1					6	0,89 %	0,89 %	0,00 p.p.
R - umjetnost, zabava i rekreacija		4	1	1				6	0,89 %	0,75 %	0,14 p.p.
S - ostale uslužne djelatnosti	3		2	2		2		9	1,34 %	1,94 %	-0,60 p.p.
Ukupno	107	289	118	91	34	20	14	673	100 %	100 %	/
Struktura uzorka (1)	15,90 %	42,94 %	17,53 %	13,52 %	5,05 %	2,97 %	2,08 %	100 %			
Struktura populacije (2)	18,57 %	44,58 %	18,87 %	11,14 %	3,42 %	1,19 %	2,23 %	100 %			
Razlika (3) = (1) - (2)	-2,67 p.p.	-1,64 p.p.	-1,34 p.p.	2,38 p.p.	1,63 p.p.	1,78 p.p.	-0,15 p.p.	/			

Izvor: Izrada autora

Tablica 36 prikazuje deskriptivnu statistiku za tri varijable kojim se opisuje razmatrani uzorak, a odnose se na prihod (u tisućama EUR), broj zaposlenih te rezultat poslovanja (u tisućama EUR). Podaci su iskazani u eurima i konvertirani iz hrvatske kune prema tečaju 1 EUR = 7,5345 HRK. Konvertirane su vrijednosti sadržane u izvješću za 2021. godinu, što je najnovije dostupno izvješće u trenutku provođenja ankete.

Populacija s obzirom na sve tri razmatrane varijable iskazuje visoko asimetričnu distribuciju, pri čemu se uočava kako je u uzorku prisutan velik broj manjih organizacija s nižim razinama prihoda i skromnim rezultatom poslovanja pri čemu je mala zastupljenost organizacija koje broje više od 100 zaposlenih.

Tablica 36. Deskriptivna statistika za varijable prihod, broj zaposlenih i rezultat poslovanja

	N	Min.	Maks.	Aritmetička sredina	Standardna devijacija	Koeficijent asimetrije	Koeficijent zaobljenosti
Prihod (u tis. EUR)	673	12,46	794.570,17	4.802,68	38.106,51	2,24	41,83
Broj zaposlenih	673	4	4.056	37,04	190,30	15,88	307,55
Rezultat poslovanja (u tis. EUR)	673	-1.410,11	88.410,67	374,96	3.619,05	2,91	69,61

Izvor: Izrada autora

Tablica 37 prikazuje kako su glavni izvršni menadžeri identificirali poslovne organizacije kojima upravljaju u pogledu uloge operatora ključnih usluga (OKU) ili davatelja digitalnih usluga (DDU).

Tablica 37. Struktura ispitanika koja se identificirala kao OKU ili DDU

Identifikacija kao OKU ili DDU	Frekvencija	Postotak
Da	71	10,55 %
Ne	497	73,85 %
Nisam siguran/a	105	15,60 %
Ukupno	**673**	**100,00%**

Izvor: Izrada autora

Vidljivo je kako je 10,55 % potvrdilo svoju ulogu kao operator ključnih usluga ili davatelji digitalnih usluga. Najveći broj organizacija, 73,85 %, nije identificiran kao operator ključnih usluga ili davatelj digitalnih usluga. Značajan broj organizacija, 15,60 %, nisu bili sigurni u

potvrdu jesu li operatori ključnih usluga ili davatelji digitalnih usluga. Izostanak konkretnog odgovora može biti pokazatelj složenosti i dinamičnosti područja kibernetičkih rizika, ali i teškoće u razumijevanju propisa i njegove provedbe.

S obzirom da Zakon o kibernetičkoj sigurnosti za ovu skupinu predviđa aktivnosti promicanja kibernetičke sigurnosti, za očekivati je da će ova grupa bilježiti veću vrijednost mjere zavisne varijable (namjere u upravljanju kibernetičkim rizicima), što se potvrđuje uvidom u *Tablicu 38*, Međutim, namjera upravljanja kibernetičkim rizicima i kod skupine koja se identificira kao OKU ili DDU nije izričito potvrdna, već se prosječna vrijednost ovisno o mjernoj čestici namjere upravljanja kibernetičkim rizicima kreće između 3,52 i 3,89.

Tablica 38. Prosječni rangovi iskazane namjere upravljanja kibernetičkim rizicima u poslovnoj organizaciji s obzirom na identifikaciju poslovne organizacije kao OKU ili DDU

Identifikacija kao OKU ili DDU		**N**	**Aritmetička sredina**	**Standardna devijacija**	**Prosječni rang**	**Pokazatelj P-vrijednosti**
INT1_1	Da	71	3,55	1,12	397,27	0,011
	Ne	497	3,09	1,26	326,54	
	Nisam siguran/a	105	3,24	1,21	345,77	
	Ukupno	**673**	**3,16**	**1,24**	/	
INT1_2	Da	71	3,52	1,11	403,08	0,002
	Ne	497	3,03	1,20	323,47	
	Nisam siguran/a	105	3,26	1,14	356,33	
	Ukupno	**673**	**3,12**	**1,19**	/	
INT1_3	Da	71	3,62	1,07	415,73	0,000
	Ne	497	3,05	1,22	322,14	
	Nisam siguran/a	105	3,25	1,15	354,09	
	Ukupno	**673**	**3,14**	**1,21**	/	
INT1_4	Da	71	3,70	1,13	415,48	0,000
	Ne	497	3,15	1,15	321,17	
	Nisam siguran/a	105	3,39	1,11	358,85	
	Ukupno	**673**	**3,25**	**1,16**	/	
INT1_5	Da	71	3,56	1,09	415,79	0,000
	Ne	497	3,01	1,17	322,65	

Identifikacija kao OKU ili DDU		N	Aritmetička sredina	Standardna devijacija	Prosječni rang	Pokazatelj P-vrijednosti
	Nisam siguran/a	105	3,18	1,08	351,65	
	Ukupno	**673**	**3,09**	**1,16**	/	
INT1_6	Da	71	3,89	0,95	395,50	0,015
	Ne	497	3,44	1,21	327,51	
	Nisam siguran/a	105	3,58	1,05	342,36	
	Ukupno	**673**	**3,51**	**1,17**	/	

Izvor: Izrada autora

Koristeći Kruskal-Wallis test, statistički značajne razlike u prosječnim rangovima su identificirane kroz svih šest mjera namjere upravljanja kibernetičkim rizicima (INT1_1 do INT1_6), s p-vrijednostima u rasponu od 0,000 do 0,015. Glavni izvršni menadžeri koji su identificirali poslovnu organizaciju kojom upravljaju kao OKU ili DDU, odnosno kao organizaciju na koju se primjenjuje Zakon o kibernetičkoj sigurnosti, konzistentno su iskazivali najviše prosječne vrijednosti za varijablu namjere upravljanja kibernetičkim rizicima (prosječne rangove u okviru Kruskal-Wallis testa). Time rezultati ukazuju na izraženiju namjeru upravljanja kibernetičkim rizicima u usporedbi s glavnim izvršnim menadžerima koji nisu sigurni u primjenu Zakona o kibernetičkoj sigurnosti na poslovnu organizaciju kojom upravljaju ili iskazuju kako se Zakon na organizaciju kojom upravljaju ne odnosi na njih.

S obzirom da Zakon o kibernetičkoj sigurnosti predviđa djelatnosti u okviru kojih je potrebno promicati kibernetičku sigurnost, moguće je u određenoj mjeri provjeriti koliko dobro su glavni izvršni menadžeri identificirali organizaciju kojom upravljaju kao OKU ili DDU.

Tablica 39. Struktura organizacija prema industrijskoj pripadnosti te identifikaciji kao OKU ili DDU

			Identifikacija kao OKU ili DDU			Ukupno
			Da	Ne	Nisam siguran/a	
Industrija	**A**	**N**	0	10	0	**10**
		Udio	0,0 %	100 %	0,0 %	**100 %**
	B	**N**	0	1	0	**1**
		Udio	0,0 %	100 %	0,0 %	**100 %**
	C	**N**	6	88	16	**110**
		Udio	5,5 %	80,0 %	14,5 %	**100 %**

			Identifikacija kao OKU ili DDU			Ukupno
			Da	Ne	Nisam siguran/a	
	D	N	1	1	0	**2**
		Udio	50,0 %	50,0 %	0,0 %	**100 %**
	E	N	1	12	1	**14**
		Udio	7,1 %	85,7 %	7,1 %	**100 %**
	F	N	0	38	9	**47**
		Udio	0,0 %	80,9 %	19,1 %	**100 %**
	G	N	9	79	19	**107**
		Udio	8,4 %	73,8 %	17,8 %	**100 %**
	H	N	3	16	4	**23**
		Udio	13,0 %	69,6 %	17,4 %	**100 %**
	I	N	2	26	4	**32**
		Udio	6,3 %	81,3 %	12,5 %	**100 %**
	J	N	30	40	7	**77**
		Udio	39,0 %	51,9 %	9,1 %	**100 %**
	K	N	2	1	0	**3**
		Udio	66,7 %	33,3 %	0,0 %	**100 %**
	L	N	1	8	3	**12**
		Udio	8,3%	66,7%	25,0 %	**100 %**
	M	N	10	132	25	**167**
		Udio	6,0 %	79,0 %	15,0%	**100 %**
	N	N	6	27	9	**42**
		Udio	14,3 %	64,3 %	21,4 %	**100 %**
	P	N	0	2	3	**5**
		Udio	0,0 %	40,0 %	60,0 %	**100 %**
	Q	N	0	5	1	**6**
		Udio	0,0 %	83,3 %	16,7 %	**100 %**
	R	N	0	4	2	**6**
		Udio	0,0 %	66,7 %	33,3 %	**100 %**
	S	N	0	7	2	**9**
		Udio	0,0 %	77,8 %	22,2 %	**100 %**
Ukupno		N	**71**	**497**	**105**	**673**
		Udio	**10,5 %**	**73,8 %**	**15,6 %**	**100 %**

Izvor: Izrada autora

Industrija K ističe se s 66,7 % organizacija koje su se identificirale u navedenoj kategoriji. Slijede je industrija D s 50,0 % i industrija J s 39,0 %. Mnoge industrije pokazuju nisku ili izrazito nisku identifikaciju u ovom kontekstu, primjer čega su industrije A, B, F, P, Q, R, S.

S obzirom da Zakon o kibernetičkoj sigurnosti identificira usluge za koje treba osigurati kibernetičku sigurnost odnosno upravljati rizicima koji se pojavljuju pružanjem ključnih usluga, pri čemu analizom te usluge povezujemo s industrijama D, E, H, J, K i Q, razvidno je kako je određeni broj glavnih izvršnih menadžera identificirao svoju poslovnu organizaciju kao OKU ili DDU premda pripadaju industrijama C, G, I i N za koje ne možemo govoriti da se Zakon o kibernetičkoj sigurnosti na iste odnosi. Navedeni podatak može biti indikativan u vezi razumijevanja Zakona o kibernetičkoj sigurnosti i njegove primjene u poslovanju, ali i problema u procesu identifikacije OKU ili DDU od strane nadležnih sektorskih tijela.

Tablica 40. Struktura poslovnih organizacija prema procjeni glavnih izvršnih menadžera o digitalnoj zrelosti organizacija kojima upravljaju

Digitalna zrelost	Frekvencija	Udio	Kumulativ
1	104	15,45 %	15,45 %
2	155	23,03 %	38,48 %
3	170	25,26 %	63,74 %
4	186	27,64 %	91,38 %
5	58	8,62 %	100 %
Ukupno	**673**	**100 %**	

Izvor: Izrada autora

U *Tablici 41* prikazana je struktura poslovnih organizacija prema industrijskoj pripadnosti i procjeni digitalne zrelosti. Industrije koje se izdvajaju po visokoj digitalnoj zrelosti su industrije K i S, među kojima 66,7 % organizacija unutar uzorka bilježi najviše ocjene digitalne zrelosti (ocjene digitalne zrelosti 4 i 5). Navedeno sugerira da organizacije u spomenutim industrijama teže uskladiti poslovne strategije i aktivnosti s najnovijim digitalnim trendovima i praksama. Njihova sposobnost da ostvare visoke ocjene u ovom segmentu sugerira da su usvojile digitalne tehnologije i procese kako bi unaprijedile svoje poslovanje, povećale konkurentsku prednost i zadovoljile potrebe svojih klijenata u digitalnom dobu. Industrija J slijedi s 53,2 %, a industrije Q i R također pokazuju visoku zrelost s postotkom od 50,0 %. U slučaju industrije Q i R razvidno je kako je veliki postotak organizacija koje imaju najnižu ocjenu digitalne zrelosti (ocjena digitalne zrelosti 1), u oba slučaja, njih čak trećina, što upućuje na nehomogenost

industrije prema kriteriju digitalna zrelost. Industrije u kojima dominiraju poslovne organizacije s manjim stupnjem digitalne zrelosti (ocjene digitalne zrelosti 1 i 2) su industrija I s 59,4 % potom C s 49,1 %.

Tablica 41. Struktura poslovnih organizacija prema industrijskoj pripadnosti i procjeni glavnih izvršnih menadžera o digitalnoj zrelosti organizacija kojima upravljaju

			Digitalna zrelost					Ukupno
			1	2	3	4	5	
Industrija	A	N	2	2	4	2	0	**10**
		Udio	20,0 %	20,0 %	40,0 %	20,0 %	0,0 %	**100 %**
	B	N	0	0	1	0	0	**1**
		Udio	0,0 %	0,0 %	100 %	0,0 %	0,0 %	**100 %**
	C	N	21	33	23	29	4	**110**
		Udio	19,1 %	30,0 %	20,9 %	26,4 %	3,6 %	**100 %**
	D	N	0	0	2	0	0	**2**
		Udio	0,0 %	0,0 %	100 %	0,0 %	0,0 %	**100 %**
	E	N	3	3	3	4	1	**14**
		Udio	21,4 %	21,4 %	21,4 %	28,6 %	7,1 %	**100 %**
	F	N	11	6	13	16	1	**47**
		Udio	23,4 %	12,8 %	27,7 %	34,0 %	2,1 %	**100 %**
	G	N	13	28	30	30	6	**107**
		Udio	12,1 %	26,2 %	28,0 %	28,0 %	5,6 %	**100 %**
	H	N	2	8	6	3	4	**23**
		Udio	8,7 %	34,8 %	26,1 %	13,0 %	17,4 %	**100 %**
	I	N	5	14	5	8	0	**32**
		Udio	15,6 %	43,8 %	15,6 %	25,0 %	0,0 %	**100 %**
	J	N	11	9	16	21	20	**77**
		Udio	14,3 %	11,7 %	20,8 %	27,3 %	26,0 %	**100 %**
	K	N	0	0	1	0	2	**3**
		Udio	0,0 %	0,0 %	33,3 %	0,0 %	66,7 %	**100 %**
	L	N	0	3	6	2	1	**12**
		Udio	0,0 %	25,0 %	50,0 %	16,7 %	8,3 %	**100 %**
	M	N	24	36	47	49	11	**167**
		Udio	14,4 %	21,6 %	28,1 %	29,3 %	6,6 %	**100 %**

			Digitalna zrelost					Ukupno
			1	2	3	4	5	
	N	N	5	11	10	11	5	**42**
		Udio	11,9 %	26,2 %	23,8 %	26,2 %	11,9 %	**100 %**
	P	N	1	0	2	1	1	**5**
		Udio	20,0 %	0,0 %	40,0 %	20,0 %	20,0 %	**100 %**
	Q	N	2	0	1	2	1	**6**
		Udio	33,3 %	0,0 %	16,7 %	33,3 %	16,7 %	**100 %**
	R	N	2	1	0	2	1	**6**
		Udio	33,3 %	16,7 %	0,0 %	33,3 %	16,7 %	**100 %**
	S	N	2	1	0	6	0	**9**
		Udio	22,2 %	11,1 %	0,0 %	66,7 %	0,0 %	**100 %**
Ukupno		N	**104**	**155**	**170**	**186**	**58**	**673**
		Udio	**15,5 %**	**23,0 %**	**25,3 %**	**27,6 %**	**8,6 %**	**100 %**

Izvor: Izrada autora

U kontekstu kibernetičkih rizika i njihova utjecaja na organizacije (*Tablica 42*), primjetno je da velika većina ispitanika, 83,66 % navodi da kibernetički rizik tijekom dosadašnjeg poslovanja nije značajno negativno utjecao na njihovu organizaciju. S druge strane, 9,96 %, potvrdilo je da su doživjeli značajan negativan utjecaj kibernetičkog rizika na svoju organizaciju, a 6,93 % ispitanika nije sigurno o utjecaju kibernetičkih rizika na njihovu organizaciju.

Tablica 42. Struktura organizacija prema iskustvu s kibernetičkim rizicima

Iskustvo	Frekvencija	Udio	Kumulativ
Da	67	9,96 %	9,96
Ne	563	83,66 %	93,61
Nisam siguran/a	43	6,39 %	100 %
Ukupno	**673**	**100 %**	

Izvor: Izrada autora

Ukoliko se podaci u vezi iskustva s kibernetičkim rizicima dodatno analiziraju (*Tablica 43*), uočava se kako industrija K - Financijske djelatnosti i djelatnosti osiguranja (33,3 %) te industrija S - Ostale uslužne djelatnosti (33,3 %) ističu kao industrije s najvećim postotkom potvrđenog negativnog utjecaja.

Tablica 43. Struktura organizacija prema industriji i iskustvu s kibernetičkim rizicima

			Iskustvo			Ukupno
			Da	Ne	Nisam siguran/a	
Industrija	A	N	1	8	1	**10**
		Udio	10,0 %	80,0 %	10,0 %	**100 %**
	B	N	0	1	0	**1**
		Udio	0,0 %	100 %	0,0 %	**100 %**
	C	N	10	91	9	**110**
		Udio	9,1 %	82,7 %	8,2 %	**100 %**
	D	N	0	2	0	**2**
		Udio	0,0 %	100 %	0,0 %	**100 %**
	E	N	0	13	1	**14**
		Udio	0,0 %	92,9 %	7,1 %	**100 %**
	F	N	4	42	1	**47**
		Udio	8,5 %	89,4 %	2,1 %	**100 %**
	G	N	15	84	8	**107**
		Udio	14,0 %	78,5 %	7,5 %	**100 %**
	H	N	1	20	2	**23**
		Udio	4,3 %	87,0 %	8,7 %	**100 %**
	I	N	3	26	3	**32**
		Udio	9,4 %	81,3 %	9,4 %	**100 %**
	J	N	7	65	5	**77**
		Udio	9,1 %	84,4 %	6,5 %	**100 %**
	K	N	1	2	0	**3**
		Udio	33,3 %	66,7 %	0,0 %	**100 %**
	L	N	1	10	1	**12**
		Udio	8,3 %	83,3 %	8,3 %	**100 %**
	M	N	17	142	8	**167**
		Udio	10,2 %	85,0 %	4,8 %	**100 %**
	N	N	3	35	4	**42**
		Udio	7,1 %	83,3 %	9,5 %	**100 %**
	P	N	0	5	0	**5**
		Udio	0,0 %	100 %	0,0 %	**100 %**

			Iskustvo			Ukupno
			Da	Ne	Nisam siguran/a	
	Q	N	0	6	0	**6**
		Udio	0,0 %	100 %	0,0 %	**100 %**
	R	N	1	5	0	**6**
		Udio	16,7 %	83,3 %	0,0 %	**100 %**
	S	N	3	6	0	**9**
		Udio	33,3 %	66,7 %	0,0 %	**100 %**
Ukupno		N	**67**	**563**	**43**	**673**
		Udio	**10,0 %**	**83,7 %**	**6,4 %**	**100 %**

Izvor: Izrada autora

U nastavku je prikazana deskriptivna analiza za predviđene konstrukte (faktore) modela. Svakom konstruktu pridruženi su indikatori pomoću kojih se isti mjeri, a za iste je pružen uvid u mjere središnje tendencije (aritmetička sredina, medijan i mod) te pokazatelje distribucije (standardnu devijaciju, koeficijent zaobljenosti i asimetrije).

Razmatrajući srednje vrijednosti za mjerne čestice konstrukta vjerojatnost pojave kibernetičkog rizika (*Tablica 44*), uočava se kako se srednje vrijednosti kreću između 2,374 do 2,597. S obzirom da je odgovore bilo moguće ponuditi na Likertovoj skali od 1 (veoma mala vjerojatnost pojave) do 5 (veoma visoka vjerojatnost pojave), zaključuje se kako glavni izvršni menadžeri uglavnom percipiraju nisku do umjerenu vjerojatnost pojave kibernetičkih rizika u poslovnim organizacijama kojima upravljaju. Važno je primijetiti da ispitanici smatraju gubitak ili krađu informacija i oštećenje ICT infrastrukture (PROB2_1, PROB2_2) kao nešto vjerojatnije u usporedbi s financijskim gubicima ili gubitkom ugleda (PROB2_3 i PROB2_4).

Prema George i Mallery (2010), vrijednosti asimetrije i zaobljenosti unutar raspona od -2 do +2 ukazuju na normalnu distribuciju podataka. Međutim, u kontekstu primjene SEM-a, Brown (2006) ističe da su vrijednosti unutar raspona od -3 do +3 također prihvatljive. S obzirom na analizirane vrijednosti, može se zaključiti da odgovori ispitanika slijede normalnu distribuciju.

Razmatrajući percepciju ozbiljnosti utjecaja kibernetičkih rizika na poslovanje organizacije kao dodatnu dimenziju percepcije prijetnje, uočava se kako prosječni ispitanik percipira da bi realizacija kibernetičkog rizika rezultirala neznačajnim prekidom rada, te bi nastupom kibernetičkog rizika, mala količina podataka bila ugrožena (SEV1). Nadalje, prosječni ispitanik smatra da bi gubitak ili krađa povjerljivih informacija (SEV2_1), kao i prekid rada ili šteta na

ICT infrastrukturi (SEV2_2), imali umjeren negativni utjecaj na njihovu organizaciju. Potonji zaključak dodatno se potvrđuje kroz mjerne čestice (SEV2_3 i SEV2_4) odnosno njihove prosječne vrijednosti koje sugeriraju kako glavni izvršni menadžeri smatraju kako bi kibernetički rizik doveo do umjerenog financijskog gubitka za organizaciju odnosno da bi i utjecaj na ugled poslovne organizacije bio umjerene štetnosti. Razmatrajući oblik distribucije, zaključuje se kako su odgovori uglavnom koncentrirani oko srednje vrijednosti pri čemu distribucija može biti opisana oblikom normalne distribucije.

Tablica 44. Deskriptivna statistika faktora percepcija prijetnje kibernetičkog rizika

Čestica	Aritmetička sredina	Medijan	Mod	Standardna devijacija	Koeficijent zaobljenosti	Koeficijent asimetrije
PROB1	2,597	3	3	0,919	-0,384	-0,167
PROB2_1	2,501	3	3	0,957	-0,382	0,120
PROB2_2	2,474	2	3	0,961	-0,294	0,260
PROB2_3	2,349	2	2	0,971	-0,127	0,463
PROB2_4	2,374	2	2	1,071	-0,372	0,463
SEV1	2,480	2	2	0,827	0,763	0,776
SEV2_1	2,945	3	3	0,997	-0,589	0,282
SEV2_2	2,945	3	3	0,956	-0,448	0,069
SEV2_3	2,774	3	3	0,967	-0,437	0,228
SEV2_4	2,661	3	2	1,085	-0,661	0,242

Izvor: Izrada autora

Temeljem uvida u *Tablicu 45*, zaključuje se kako glavni izvršni menadžeri smatraju da upravljanje kibernetičkim rizicima generalno doprinosi njihovom smanjenju te očekuju koristi. Kada se radi o smanjenju vjerojatnosti pojavljivanja kibernetičkih rizika (EFF1), smanjenju financijskih gubitaka (EFF2) i smanjenju negativnog utjecaja na ugled (EFF3), aritmetička sredina za te stavke kreće se između 3,880 i 3,958, što upućuje kako među glavnim izvršnim menadžerima prevladava stav o postojanju korisnosti za organizacije koje primjenjuju upravljanje kibernetičkim rizicima. Medijan i mod za ove stavke također potvrđuju rezultat analize.

U kontekstu resursa i sposobnosti organizacije za upravljanje kibernetičkim rizicima, ispitanici iskazuju neutralnije stajalište. Srednje vrijednosti za tvrdnje o financijskim i tehničkim

resursima (SEFF1_1, SEFF1_2), kao i stručnosti i znanju potrebnom za upravljanje kibernetičkim rizicima (SEFF1_3) te konačno efikasnosti upravljanja (SEFF1_4), kreću se između 3,040 i 3,174.

Kada je riječ o troškovima upravljanja kibernetičkim rizicima, srednje vrijednosti za stavke povezane s ulaganjima u tehnologiju (COST1_1), obrazovanje i trening zaposlenika (COST1_2), kao i uvođenje naprednih tehnologija (COST1_3), kreću se između 3,419 i 3,467, što upućuje kako među glavnim izvršnim menadžerima prevladava stav kako je upravljanje kibernetičkim rizicima troškovno zahtjevno.

S obzirom da se vrijednosti asimetrije i zaobljenosti nalaze u odgovarajućem rasponu za dokazivanje normalnosti distribucije, potvrđuje se kako odgovori prate oblik normalne distribucije. Sagledavajući sve tri dimenzije percepcije sposobnosti organizacije u vezi suočavanja s prijetnjom, zaključuje se kako ispitanici prepoznaju važnost i doprinos upravljanja kibernetičkim rizicima, ali također prepoznaju izazove i troškove koji su s tim povezani.

Tablica 45. Deskriptivna statistika faktora percepcija sposobnosti suočavanja s kibernetičkim rizikom kao prijetnjom

Čestica	Aritmetička sredina	Medijan	Mod	Standardna devijacija	Koeficijent zaobljenosti	Koeficijent asimetrije
EFF1_1	3,958	4	4	0,974	1,576	-1,231
EFF1_2	3,895	4	4	0,976	1,455	-1,160
EFF1_3	3,880	4	4	0,990	1,141	-1,075
SEFF1_1	3,138	3	4	1,108	-0,616	-0,334
SEFF1_2	3,174	3	4	1,139	-0,752	-0,357
SEFF1_3	3,058	3	4	1,150	-0,818	-0,160
SEFF1_4	3,040	3	3	1,130	-0,732	-0,178
COST1_1	3,467	4	4	1,008	-0,211	-0,485
COST1_2	3,431	4	4	1,038	-0,445	-0,374
COST1_3	3,419	4	4	1,056	-0,607	-0,322

Izvor: Izrada autora

Na temelju pruženih podataka unutar *Tablice 46*, može se zaključiti da ispitanici pod upravljanjem rizicima poslovnih organizacija pokazuju umjereno pozitivnu sklonost prema mjerama upravljanja kibernetičkim rizicima u narednih 12 mjeseci.

Analizirajući stavove ispitanika prema poticanju aktivnosti usmjerenih na zaštitu od kibernetičkih rizika (INT1_1), ulaganju u resurse (INT1_2), nadogradnji politika i pravila (INT1_3), primjeni suvremenih standarda (INT1_4) te razvoju planova upravljanja identificiranim rizicima (INT1_5), primjećujemo da se aritmetičke sredine većinom kreću oko vrijednosti 3, što ukazuje na neutralno do blago pozitivno stajalište u smislu iskazivanja namjere upravljanja kibernetičkim rizicima u narednom razdoblju od 12 mjeseci. Kada je u pitanju jačanje svijesti o kibernetičkim rizicima kod zaposlenika (INT1_6), gdje aritmetička sredina doseže vrijednost od 3,513 s medijanom i modom na razini 4, zaključuje se kako je pozitivnu promjenu glede upravljanja kibernetičkim rizicima u organizacijama najvjerojatnije očekivati upravo u segmentu jačanja svijesti kod zaposlenika. S obzirom da se vrijednosti asimetrije i zaobljenosti nalaze u odgovarajućem rasponu za dokazivanje normalnosti distribucije, potvrđuje se kako odgovori prate oblik normalne distribucije.

Tablica 46. Deskriptivna statistika faktora namjera upravljanja kibernetičkim rizicima s kojima je suočena poslovna organizacija

Čestica	Aritmetička sredina	Medijan	Mod	Standardna devijacija	Koeficijent zaobljenosti	Koeficijent asimetrije
INT1_1	3,165	3	4	1,241	-0,863	-0,343
INT1_2	3,119	3	4	1,192	-0,818	-0,336
INT1_3	3,138	3	4	1,208	-0,836	-0,323
INT1_4	3,250	3	4	1,155	-0,618	-0,445
INT1_5	3,094	3	3	1,156	-0,711	-0,287
INT1_6	3,513	4	4	1,169	-0,351	-0,651

Izvor: Izrada autora

Kada se analiziraju odgovori na pitanja vezana za osjećaj straha među glavnim izvršnim menadžerima (*Tablica 47*), zaključuje se kako je strah blago do umjereno prisutan. Detaljnije razmotrene prosječne vrijednosti mjernih čestica, ukazuje kako ispitanici pokazuju blago do umjereni strah prema gubitku ili krađi povjerljivih informacija (FEA1_1), utjecaju na uspješnost poslovanja (FEA1_2) i potencijalnom negativnom utjecaju na ugled organizacije

(FEA1_3). Srednje vrijednosti za sve tri mjerne čestice konstrukata kreću se između 2,585 do 2,709.

Međutim, kada se razmotre odgovori na pitanja vezana za osjećaj žaljenja kod ispitanika vezano za potencijalne kibernetičke rizike (*Tablica 47*), primjećuje se izraženiji intenzitet ove emocije u odnosu na strah. Ispitanici bi osjećali veće žaljenje ukoliko bi organizacija kojom upravljaju pretrpjela kibernetički rizik (REG1_1. REG1_2), posebno ako bi to negativno utjecalo na poslovni rezultat (REG1_3) ili ugled organizacije (REG1_4). Navedene vrijednosti se kreću od 3,661 do 3,826, sugeriraju da je osjećaj žaljenja izražen među većinom ispitanika, posebno ako nisu uloženi raspoloživi resursi za upravljanje kibernetičkim rizicima ili ako kibernetički rizik negativno utječe na poslovne rezultate ili ugled organizacije.

Razmatrajući oblik distribucije, zaključuje se kako su odgovori uglavnom koncentrirani oko srednje vrijednosti pri čemu oblik distribucije može biti opisan oblikom normalne distribucije. Distribucijska svojstva upućuju na to da su ispitanici općenito više skloni žaljenju zbog potencijalnih posljedica kibernetičkog rizika nego što osjećaju izravan strah zbog samih rizika.

Tablica 47. Deskriptivna statistika faktora emocija

Čestica	Aritmetička sredina	Medijan	Mod	Standardna devijacija	Koeficijent zaobljenosti	Koeficijent asimetrije
FEA1_1	2,709	3	3	1,087	-0,643	0,110
FEA1_2	2,730	3	3	1,104	-0,697	0,105
FEA1_3	2,585	3	3	1,165	-0,861	0,191
REG1_1	3,661	4	4	1,019	-0,243	-0,568
REG1_2	3,648	4	4	1,053	-0,172	-0,608
REG1_3	3,826	4	4	1,000	0,047	-0,728
REG1_4	3,722	4	4	1,075	-0,150	-0,690

Izvor: Izrada autora

Ispitanici su umjereno skloni usporedbi položaja poslovne organizacije kojom upravljaju s drugim usporednim (prema veličini i djelatnosti) poslovnim organizacijama. Naime, umjerena sklonost glavnih izvršnih menadžera da percipiraju organizaciju kao manje podložnu kibernetičkim rizicima u odnosu na usporedne poslovne organizacije potvrđuje se kroz sve predviđene mjerne čestice (OPBI1_1, OPBI1_2, OPBI1_3, OPBI1_4) pri čemu se prosječna vrijednost kreće između 3,048 do 3,211. Kada se razmotri sklonost projiciranja povijesnih

ishoda, u konkretnom slučaju, pozitivnih ishoda (izostanak negativnog ishoda) na buduće razdoblje, prema svim mjernim česticama (OPB2_1, OPBI2_2 i OPBI2_3) potvrđuje se umjerena sklonost preslikavanju povijesnih ishoda na buduće ishode. Prosječna vrijednost za sve mjerne čestice kreće se između 2,987 i 3,076. Razmatrajući oblik distribucije za mjerne čestice u okviru koncepta optimistična pristranost, potvrđuje se kako iste slijede oblik normalne distribucije.

Stavljajući fokus na stvarna ranija iskustva, sukladno očekivanjima, potvrđuje se kako dominantna većina ispitanika iskazuje kako se u potpunosti ne slaže s tvrdnjom kako su imali negativne posljedice poput gubitka podataka (REC1_1), negativnog utjecaja na financijski rezultat (REC1_2) ili ugled (REC1_3). Prosječne vrijednosti pruženih odgovora za sve tri mjerne čestice kreću se između 1,416 i 1,428. Razmatrajući dodatnu dimenziju koncepta pristranosti dostupnosti, razmatra se utjecaj nedavnih informacija pri čemu se posebno izdvajaju podaci o utjecaju medija (REC2_1), industrijskih izvještaja (REC2_2) čije se prosječne vrijednosti odgovora kreću između 2,859 i 2,966, dok se iskustva drugih organizacija (REC2_3) i osobna iskustva (REC2_4) pojavljuju s nešto izraženijom potvrdom utjecaja na formiranje mišljenja glavnih izvršnih menadžera o kibernetičkim rizicima kao izazovima za poslovanje organizacija. Što se tiče distribucijskih svojstava, koeficijenti zaobljenosti sugeriraju značajno odstupanje od normalne distribucije u slučaju nedavnih vlastitih iskustava (REC1_1, REC1_2, REC1_3) pri čemu mjerne čestice iskazuju pozitivnu asimetriju, što sugerira kako je veći broj ispitanika ponudio tvrdnje u kojima se u potpunosti ne slaže s postojanjem negativnog iskustva u vezi kibernetičkih rizika. Dodatno, uočena je visoka vrijednost za koeficijent zaobljenosti, što sugerira kako su podaci za ove mjerne čestice izrazito koncentrirani oko srednje vrijednosti s malim brojem varijacija. Ostale varijable u okviru faktora (koncepta) kognitivna pristranost pokazuju svojstva normalne distribucije.

Tablica 48. Deskriptivna statistika faktora kognitivna pristranost

Čestica	Aritmetička sredina	Medijan	Mod	Standardna devijacija	Koeficijent zaobljenosti	Koeficijent asimetrije
OPBI1_1	3,048	3	3	0,948	0,120	-0,210
OPBI1_2	3,211	3	3	0,928	0,148	-0,341
OPBI1_3	3,137	3	3	0,913	0,123	-0,297
OPBI1_4	3,125	3	3	0,955	0,052	-0,272
OPBI2_1	2,987	3	3	1,003	-0,446	-0,266

Čestica	Aritmetička sredina	Medijan	Mod	Standardna devijacija	Koeficijent zaobljenosti	Koeficijent asimetrije
OPBI2_2	3,056	3	3	0,992	-0,282	-0,306
OPBI2_3	3,076	3	3	1,008	-0,377	-0,283
REC1_1	1,428	1	1	0,891	4,103	2,180
REC1_2	1,416	1	1	0,868	4,465	2,224
REC1_3	1,416	1	1	0,887	4,638	2,272
REC2_1	2,966	3	4	1,166	-0,880	-0,374
REC2_2	2,859	3	3	1,142	-0,859	-0,267
REC2_3	3,245	3	4	1,146	-0,475	-0,591
REC2_4	3,128	3	4	1,189	-0,726	-0,392

Izvor: Izrada autora

5.2.4. Analiza modela prvog reda u okviru glavnog istraživanja

Sukladno ranije prezentiranom teorijskom konceptu (modelu), pomoću PLS-SEM tehnike testira se model koji predviđa kognitivne pristranosti (pristranost optimizma, pristranost dostupnosti) te percepciju sposobnosti suočavanja kao egzogene latentne varijable. Istovremeno se percepcija kibernetičkih rizika kao prijetnje, emocije (strah i žaljenje) i namjera upravljanja kibernetičkim rizicima razmatraju kao endogene latentne varijable. Prilikom procjene modela, prema uzoru na prethodna istraživanja, korišten je reflektivni mjerni model koji pretpostavlja kako su korištene mjere (mjerne čestice ili indikatori) posljedica razmatranog konstrukta.

S obzirom da je u razmatranom istraživanju predviđeno proširenje teorije motivacije za zaštitom kroz integraciju pretpostavki bihevioralne ekonomije što istodobno predviđa kompleksan model koji sadržava veći broj strukturalnih veza te da nije ispunjena pretpostavka normalnosti distribucije za potpuni skup indikatora (izostaje za mjere REC1_1, REC1_2 i REC1_3), u nastavku empirijske analize koristi se PLS-SEM procjena modela.

U skladu sa smjernicama za strukturalno modeliranje, inicijalni model uključivao je sve stavke ankete kao indikatore latentnih varijabli. Kako bi se ostvario kvalitetan mjerni model, indikatori su sukcesivno uklanjani temeljem njihovih vanjskih opterećenja i konzistentnosti koju su

postigli. Pouzdanost i konzistentnost evaluirana je kroz tri ključna pokazatelja: Cronbach Alpha, CR i AVE.

Indikatori koji su ostali zadržani u konačnom modelu prikazani su u *Tablici 49*.

Tablica 49. Rezultati analize pouzdanosti i konvergentne valjanosti PLS-SEM modela

Faktori i čestice	Vanjsko faktorsko opterećenje	Cronbach alpha	CR	AVE
Percepcija o kibernetičkim rizicima kao prijetnji za poslovanje organizacije				
PROB1	0,806***	0,865	0,902	0,650
PROB2_1	0,851***			
PROB2_2	0,781***			
PROB2_3	0,817***			
PROB2_4	0,772***			
SEV1	0,712***	0,878	0,911	0,674
SEV2_1	0,857***			
SEV2_2	0,819***			
SEV2_3	0,863***			
SEV2_4	0,845***			
Percepcija o sposobnosti organizacije u upravljanju kibernetičkim rizicima				
SEFF1_1	0,733***	0,875	0,916	0,733
SEFF1_2	0,846***			
SEFF1_3	0,914***			
SEFF1_4	0,919***			
Namjera upravljanja kibernetičkim rizicima				
INT1_4	0,940***	0,919	0,949	0,860
INT1_5	0,934***			
INT1_6	0,909***			
Emocije				
FEA1_1	0,951***	0,894	0,950	0,904
FEA1_3	0,951***			
REG1_1	0,877***	0,920	0,943	0,806
REG1_2	0,902***			

Faktori i čestice	Vanjsko faktorsko opterećenje	Cronbach alpha	CR	AVE
REG1_3	0,921***			
REG1_4	0,891***			
Kognitivne pristranosti				
OPBI1_2	0,747***	0,840	0,883	0,603
OPBI1_3	0,763***			
OPBI1_4	0,817***			
OPBI2_1	0,740***			
OPBI2_3	0,812***			
REC1_1	0,778***	0,762	0,837	0,467
REC1_2	0,780***			
REC1_3	0,784***			
REC2_1	0,556***			
REC2_2	0,613***			
REC2_3	0,538***			

Napomena: *p<0,05; **p<0,01; ***p<0,001

Izvor: Izrada autora

Faktorska opterećenja ukazuju na statističku značajnost, a za sve indikatore zabilježena vrijednost je veća od 0,5, što ukazuje na to da dobro odražavaju latentnu varijablu koju mjere.

Cronbach alpha je mjera unutarnje konzistentnosti (pouzdanosti) skupa indikatora (mjernih čestica) konstrukta kojeg mjere, preporučena vrijednost je veća od 0,7, a manja od 0,95. S obzirom da se vrijednosti kreću u rasponu od 0,762 do 0,920, zaključuje se kako je postignuta konzistentnosti skupa indikatora. Slično Cronbach alpha pokazatelju, CR je mjera unutarnje konzistentnosti, ali se često koristi u SEM analizi te se smatra primjerenijom u odnosu na Cronbach alpha pokazatelj. S obzirom da se vrijednosti kreću od 0,837 do 0,950, smatra se da su svi konstrukti iskazali unutarnju konzistentnost. Konačno, razmatra se konvergentna valjanost pomoću AVE pokazatelja koji bi prema preporuci trebao iznositi 0,5 ili više. Za sve konstrukte, izuzev konstrukta pristranosti dostupnosti (REC), AVE pokazatelj premašuje vrijednost 0,5 što ukazuje kako je svakim konstruktom objašnjeno barem 50 % varijance u svojim indikatorima. Sukladno, Fornellu i Larckeru (1981), čak i ako je AVE manji od 0,5, ali je kompozitna pouzdanost (CR) veća od 0,6, konvergentna valjanost konstrukta je i dalje

zadovoljavajuća. Što se tiče konstrukta pristranosti dostupnosti, vrijednost pokazatelja AVE je približna preporučenoj vrijednosti 0,5, točnije iznosi 0,467 što se automatski ne isključuje iz razmatranja, već se paralelno promatra vrijednost CR pokazatelja koji prema Lam (2012) također doprinosi zaključku o konvergentnoj valjanosti, i koji iznosi 0,837 te premašuje preporučenih 0,7. Stoga se u cilju zadržavanja što većeg broja indikatora za konstrukt pristranosti dostupnosti, zaključuje kako je mjerna ljestvica konstrukta pristranost dostupnosti ispunila predviđen kriterij pouzdanosti i valjanosti te će se koristiti u nastavku istraživanja. Sukladno analizi svih relevantnih pokazatelja pouzdanosti i valjanosti, može se zaključiti da selektirani indikatori adekvatno reprezentiraju faktore koje su namijenjeni predstavljati.

U nastavku se analizira diskriminantna valjanosti procijenjenog modela prema trima kriterijima; *unakrsno opterećenje, Fornell-Larcker kriteriju te Heterotrait-monotrait omjeru korelacije*.

Tablica 50 prezentira rezultate diskriminantne valjanosti pomoću unakrsnih opterećenja. Vrijednosti izvan dijagonale predstavljaju unakrsna opterećenja te bi trebala biti manja u odnosu na vrijednosti na dijagonali, a navedeno bi značilo da svaki konstrukt (faktor) bolje objašnjava varijancu svojih indikatora (mjernih čestica) naspram indikatora drugog konstrukta. Uvidom u rezultate analize prema unakrsnim opterećenjima, zaključuje se da je navedeno postignuto.

Tablica 50. Rezultati analize diskriminantne valjanosti prema unakrsnim opterećenjima – analiza modela prvog reda

	PROB	SEV	SEFF	INT	FEA	REG	OPBI	REC
PROB1	**0,806**	0,439	0,133	0,247	0,345	0,261	-0,179	0,253
PROB2_1	**0,851**	0,452	0,025	0,195	0,382	0,263	-0,105	0,265
PROB2_2	**0,781**	0,436	0,047	0,172	0,366	0,209	-0,134	0,239
PROB2_3	**0,817**	0,494	-0,013	0,131	0,378	0,205	-0,081	0,261
PROB2_4	**0,772**	0,581	0,007	0,177	0,451	0,240	-0,120	0,243
SEV1	0,470	**0,712**	0,010	0,165	0,366	0,324	-0,044	0,165
SEV2_1	0,479	**0,857**	0,103	0,253	0,527	0,393	-0,052	0,261
SEV2_2	0,468	**0,819**	0,038	0,190	0,443	0,369	-0,118	0,207
SEV2_3	0,505	**0,863**	0,044	0,226	0,488	0,368	-0,048	0,228
SEV2_4	0,538	**0,845**	0,055	0,239	0,536	0,371	-0,059	0,271
SEFF1_1	0,105	0,120	**0,733**	0,409	0,129	0,162	0,052	0,142
SEFF1_2	0,034	0,040	**0,846**	0,456	0,073	0,076	0,099	0,136

	PROB	SEV	SEFF	INT	FEA	REG	OPBI	REC
SEFF1_3	0,017	0,039	**0,914**	0,470	0,031	0,011	0,132	0,107
SEFF1_4	0,019	0,028	**0,919**	0,459	0,018	0,016	0,112	0,118
INT1_4	0,178	0,225	0,551	**0,940**	0,284	0,263	0,053	0,215
INT1_5	0,233	0,278	0,468	**0,934**	0,350	0,300	0,044	0,228
INT1_6	0,231	0,233	0,436	**0,909**	0,305	0,295	-0,013	0,190
FEA1_1	0,470	0,540	0,067	0,320	**0,950**	0,499	-0,043	0,316
FEA1_3	0,442	0,565	0,068	0,321	**0,952**	0,501	-0,062	0,302
REG1_1	0,268	0,409	0,008	0,243	0,491	**0,877**	-0,040	0,134
REG1_2	0,298	0,442	0,103	0,301	0,484	**0,902**	-0,044	0,156
REG1_3	0,251	0,358	0,061	0,259	0,444	**0,921**	-0,031	0,133
REG1_4	0,231	0,383	0,088	0,295	0,465	**0,891**	0,024	0,136
OPBI1_2	-0,097	-0,011	0,128	0,061	-0,002	0,041	**0,747**	0,001
OPBI1_3	-0,078	-0,060	0,143	0,076	-0,028	-0,002	**0,763**	0,017
OPBI1_4	-0,114	-0,084	0,113	0,009	-0,089	-0,074	**0,817**	-0,005
OPBI2_1	-0,095	-0,009	0,064	0,046	-0,001	0,010	**0,740**	0,055
OPBI2_3	-0,170	-0,092	0,047	-0,015	-0,057	-0,033	**0,812**	-0,006
REC1_1	0,230	0,174	0,022	0,058	0,177	0,018	0,017	**0,778**
REC1_2	0,233	0,193	0,059	0,089	0,225	0,023	0,002	**0,780**
REC1_3	0,240	0,197	0,050	0,097	0,206	0,020	0,000	**0,784**
REC2_1	0,151	0,176	0,040	0,165	0,267	0,229	0,007	**0,556**
REC2_2	0,198	0,218	0,188	0,273	0,245	0,182	0,040	**0,613**
REC2_3	0,212	0,183	0,234	0,261	0,219	0,203	-0,025	**0,538**

Izvor: Izrada autora

U *Tablici 51* prezentirana je korelacijska matrica među konstruktima pri čemu se na dijagonali nalaze vrijednosti drugog korijena prosječno izlučene varijance (AVE). Kako bi se potvrdila odgovarajuća diskriminantna valjanost, AVE bi trebao biti veći od korelacijskih koeficijenata u odgovarajućim redcima i stupcima. Navedeno označava kako svaki konstrukt (latentna varijabla) bolje objašnjava varijancu svojih indikatora u odnosu na indikatore ostalih konstrukata te da je svaki promatrani konstrukt različit u odnosu na ostale konstrukte predviđene modelom. Budući da je navedeni uvjet ispunjen, zaključuje se kako je postignuta diskriminantna valjanost konstrukata.

Tablica 51. Rezultati analize diskriminantne valjanosti prema Fornell-Larcker kriteriju – analiza modela prvog reda

	PROB	SEV	SEFF	INT	FEA	REG	OPBI	REC
PROB	**0,806**							
SEV	0,599	**0,821**						
SEFF	0,049	0,064	**0,856**					
INT	0,229	0,264	0,525	**0,928**				
FEA	0,479	0,581	0,071	0,337	**0,951**			
REG	0,293	0,446	0,074	0,307	0,526	**0,898**		
OPBI	-0,154	-0,078	0,117	0,032	-0,055	-0,026	**0,777**	
REC	0,313	0,280	0,146	0,228	0,325	0,156	0,010	**0,683**

Izvor: Izrada autora

Konačno, diskriminantna valjanost se prosuđuje temeljem HTMT omjera koji se u usporedbi s ostalim razmotrenim metodama provjere diskriminantne valjanosti, smatra efikasnijim pristupom provjere (Henseler et al., 2015). S obzirom da tablica prezentira korelacije između indikatora koje mjere različite konstrukte u odnosu na korelacije između indikatora koji mjere isti konstrukt, cilj je imati što niže vrijednosti, a kao granična vrijednost postavlja se 0,85 (Hair et al., 2021; Kline, 2011). Rezultati potvrđuju kako su sve vrijednosti unutar *Tablice 52* ispod granične vrijednosti te se zaključuje kako je postignuta diskriminantna valjanost konstrukata, što je sukladno prethodnim dvjema metodama.

Tablica 52. Rezultati analize diskriminantne valjanosti prema HTMT pokazatelju – analiza modela prvog reda

	PROB	SEV	SEFF	INT	FEA	REG	OPBI	REC
PROB								
SEV	0,686							
SEFF	0,083	0,076						
INT	0,258	0,292	0,584					
FEA	0,543	0,650	0,083	0,372				
REG	0,326	0,493	0,103	0,334	0,578			
OPBI	0,166	0,085	0,146	0,064	0,061	0,062		
REC	0,384	0,339	0,185	0,277	0,400	0,198	0,090	

Izvor: Izrada autora

Nakon zaključene faze analize mjernog modela, u nastavku se razmatra analiza strukturalnog modela. Strukturalni model predstavljen je vezama između konstrukata. Model se sastoji od 8 konstrukata (latentnih varijabli) i 4 kontrolne varijable, od kojih su 3 egzogena konstrukta, a 5 endogenih konstrukata. U nastavku je opisana analiza strukturalnog modela u okviru glavnog istraživanja. Stoga se provjerava vrijednost dobivenih parametara u smislu smjera utjecaja, jakosti utjecaja, njihove značajnosti te adekvatnost modela.

Prvi korak u analizi strukturalnog modela je procjena kolinearnosti konstrukata koja se provodi pomoću analize VIF vrijednosti strukturalnog modela. S obzirom da vrijednosti ne prelaze referentnu vrijednost od 5 te strožu referentnu vrijednost od 3.3, zaključuje se da problem multikolinearnosti nije prisutan (*Tablica 53*).

Tablica 53. Rezultati analize multikolinearnosti unutarnjeg modela – analiza modela prvog reda

	VIF
PROB -> FEA	1,559
PROB -> REG	1,559
SEV -> FEA	1,559
SEV -> REG	1,559
SEFF -> INT	1,133
FEA -> INT	1,391
REG -> INT	1,394
OPBI -> PROB	1,000
OPBI -> SEV	1,000
REC -> PROB	1,000
Kontrolne varijable	
REC -> SEV	1,000
EMP -> INT	1,015
IT_EXP_1 -> INT	1,080
SEC_1 -> INT	1,062
DMAT_1 -> INT	1,072

Izvor: Izrada autora

Sljedeći korak u analizi strukturalnog modela je procjena statističke značajnosti procijenjenih koeficijenata puta. Statistička značajnost je izračunata putem „bootstraping“ procedure.

Tablica 54. Rezultati strukturalnog modela – analiza modela prvog reda

Pretpostavljena veza	Koeficijent puta (β)	Sredina uzorka	Standardna devijacija (STDEV)	Pokazatelj T-vrijednosti	Pokazatelj P-vrijednosti
PROB -> FEA	0,205	0,206	0,039	3,824	0,000
PROB -> REG	0,042	0,044	0,042	0,591	0,320
SEV -> FEA	0,458	0,459	0,038	6,175	0,000
SEV -> REG	0,421	0,421	0,038	1,503	0,000
FEA -> INT	0,212	0,213	0,034	4,651	0,000
REG -> INT	0,151	0,151	0,038	1,964	0,000
SEFF -> INT	0,452	0,452	0,036	5,229	0,000
OPBI -> PROB	-0,157	-0,163	0,034	0,994	0,000
OPBI -> SEV	-0,081	-0,086	0,041	7,881	0,050
REC -> PROB	0,315	0,318	0,040	7,752	0,000
REC -> SEV	0,281	0,283	0,036	3,992	0,000
EMP -> INT	0,012	0,017	0,021	1,130	0,555
IT_EXP_1 -> INT	0,094	0,094	0,063	12,616	0,133
SEC_1 -> INT	0,089	0,088	0,079	12,155	0,259
DMAT_1 -> INT	0,257	0,256	0,067	11,104	0,000

Izvor: Izrada autora

Temeljem *Tablice 54* koja sadržava rezultate testa statističke značajnosti pretpostavljenih veza unutar modela, moguće je donijeti prosudbu o prihvaćanju ili odbacivanju postavljenih hipoteza. Potvrđuje se kako pristranost optimizma značajno i negativno utječe na percepciju kibernetičke prijetnje kojom je izložena poslovna organizacija (H1a) te se potvrđuje u oba slučaja bez obzira na dimenziju percepcije prijetnje (OPBI -> PROB; β=-0,157, p=0,000 i OPBI -> SEV; β=-0,081, p=0,050). Potvrđuje se kako pristranost dostupnosti značajno pozitivno utječe na percepciju kibernetičke prijetnje kojom je izložena poslovna organizacija (H1b) te se potvrđuje u oba slučaja bez obzira na dimenziju percepcije prijetnje (REC -> PROB; β=0,315, p=0,000 i REC -> SEV; β=0,281, p=0,000). **Stoga se prihvaća hipoteza prema kojoj kognitivne pristranosti glavnih izvršnih menadžera značajno utječu na percepciju kibernetičke prijetnje kojoj je izložena poslovna organizacija (H1).**

Hipoteza H2 odnosi se na medijacijski utjecaj emocija, stoga je uputno prikazati *Tablicu 55* koja pruža uvid u produkt putanja predviđenih veza postavljene medijacije.

Tablica 55. Rezultati strukturalnog modela – Specifični i ukupni indirektni utjecaj – analiza modela prvog reda

Specifični indirektni utjecaj					
	Koeficijent puta	**Sredina uzorka**	**Standardna devijacija**	**Pokazatelj T-vrijednosti**	**Pokazatelj P-vrijednosti**
PROB -> FEA -> INT	0,043	0,044	0,011	4,040	0,000
PROB -> REG -> INT	0,006	0,007	0,007	0,916	0,360
SEV -> FEA -> INT	0,097	0,098	0,019	5,221	0,000
SEV -> REG -> INT	0,064	0,063	0,017	3,693	0,000
Ukupni indirektni utjecaj					
	Koeficijent puta	**Sredina uzorka**	**Standardna devijacija**	**Pokazatelj T-vrijednosti**	**Pokazatelj P-vrijednosti**
PROB -> INT	0,050	0,050	0,014	3,616	0,000
SEV -> INT	0,161	0,161	0,020	8,095	0,000

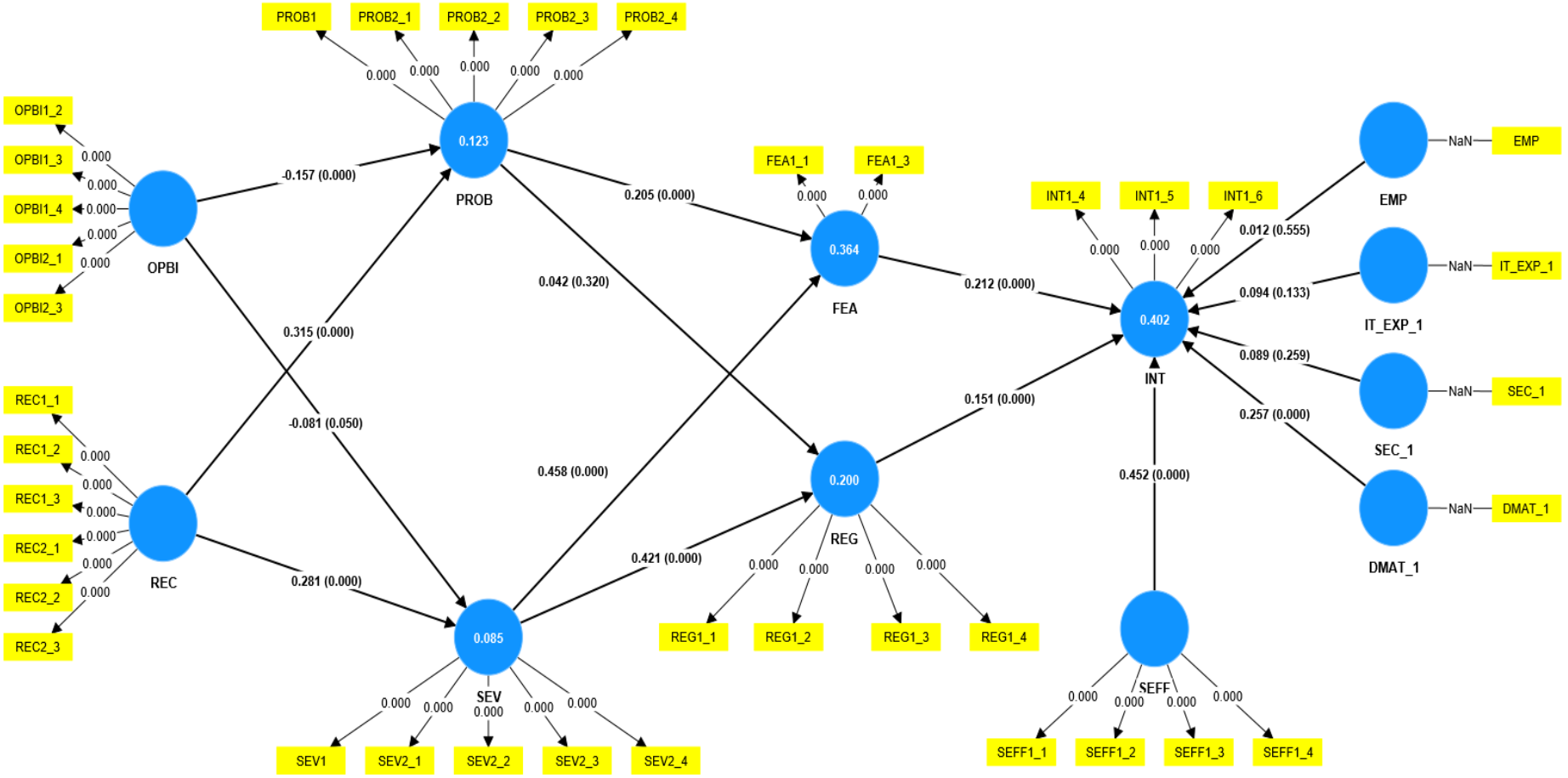
Izvor: Izrada autora

Potvrđuje se kako je utjecaj percepcije prijetnje na namjeru upravljanja kibernetičkim rizicima posredovan emocijama (H2). Navedeno se potvrđuje bez obzira na odabir dimenzije percepcije prijetnje (PROB -> INT; β=0,050, p=0,000 i SEV -> INT; β=0,161, p=0,000). Uvidom u specifični indirektni utjecaj, daje se razlučiti kako medijacijsku ulogu potvrđuje emocija straha (H2a) i to bez obzira na korištenu mjeru percepcije prijetnje (PROB -> FEA -> INT; β=0,043, p=0,000 i SEV -> FEA -> INT; β=0,097, p=0,000) te emocija žaljenje (H2b) pri čemu se statistički značajnim potvrđuje u slučaju kada se percepcija prijetnje mjeri pomoću dimenzije intenzitet utjecaja (SEV) (PROB -> REG -> INT; β=0,006, p=0,360 i SEV -> REG -> INT; β=0,064, p=0,000).

Temeljem rezultata strukturalnog modela, **vidljivo je kako percepcija glavnog izvršnog menadžera o sposobnosti suočavanja organizacije s kibernetičkim rizicima pozitivno utječe na namjeru upravljanja kibernetičkim rizicima (H3)** (SEFF -> INT; β=0,452, p=0,000).

Rezultati strukturalnog modela prvog reda grafički su prezentirani na *Slici 10*. Prikazane su značajnosti standardiziranih vanjskih faktorskih opterećenja, koeficijenti putanje strukturalnog modela i njihova značajnost te koeficijenti determinacije (R^2) za sve endogene konstrukte (faktore). Koeficijent determinacije odnosi se na postotak varijance endogenog konstrukta koji je objašnjen pretpostavljenim prediktorima. Uobičajeno je smatrati kako vrijednosti R^2 između 0,25 i 0,50 ukazuju na slabu, između 0,50 i 0,75 na umjerenu, a preko 0,75 na jaku

eksplanatornu snagu modela. Međutim, prema Hair et al. (2021) vrijednosti treba razmatrati ovisno o kontekstu istraživanja pri čemu se vrijednosti niže od 0,10 smatraju zadovoljavajućim. Prema Vuković (2022), Sarstedt et al. (2017) Ringle et al. (2014) i Cohen (2013) u istraživanjima u području društvenih i uže bihevioralnih znanosti, kao referentne granice postavljene su izdvojene vrijednosti koeficijenta determinacije, tako između 0,02 i 0,13 ukazuje na slabu, između 0,13 i 0,26 na umjerenu, a preko 0,26 na jaku eksplanatornu snagu modela. Uspoređivanje raznih modela temeljem koeficijenta determinacije može biti kompliciranо, s obzirom da uključivanje novih konstrukata u model može utjecati na povećanje R^2 vrijednosti. Stoga, kako bi se izbjegla pristranost prema kompleksnijim modelima, koristi se prilagođeni koeficijent determinacije (prilagođeni R^2) (Hair et al., 2021).



Slika 10. Dijagram putanje uz prikaz strukturalnih koeficijenata i njihove značajnosti – analiza modela prvog reda

Izvor: Izrada autora uz pomoć programa SmartPLS

Koeficijentom determinacije daje se uvid, koliko model dobro objašnjava varijabilnost endogenih varijabli. S druge strane, Stone-Geisser Q^2 pokazatelj pruža uvid u produktivnu relevantnost modela. Riječ je o metodi koja tehnikom uzorkovanja izostavlja dijelove podataka tijekom procijene i zatim, temeljem modela, pokušava predvidjeti izostavljene podatke (procedura „*blindfolding*“). Ukoliko Stone-Geisser Q^2 vrijednosti premašuju 0, smatra se da model ima prediktivnu relevantnost (Hair et al., 2014).

Temeljem vrijednosti koeficijenta determinacije, prilagođenog koeficijenta determinacije i Stone-Geisser Q^2 pokazatelja provedena je procjena strukturalnog modela.

Tablica 56. Vrijednost za koeficijent determinacije, prilagođeni koeficijent determinacije i Q2 pokazatelj – analiza modela prvog reda

Endogeni konstrukti	R^2	Prilagođeni R^2	Q^2
PROB	0,123	0,120	0,112
SEV	0,085	0,082	0,075
FEA	0,364	0,362	0,088
REG	0,200	0,197	0,022
INT	0,403	0,396	0,274

Izvor: Izrada autora

Sukladno *Tablici 56*, uočava se kako konstrukti strah (FEA) i namjera upravljanja kibernetičkim rizicima (INT) ističu se s najdominantnijim R^2 vrijednostima. Ovo sugerira da odabrani prediktori u modelu efikasno objašnjavaju varijabilnost ovih konstrukata, čime se postiže robusna eksplanatorna snaga u kontekstu ovih varijabli.

S druge strane, konstrukti percepcija ozbiljnosti utjecaja kibernetičkog rizika na poslovanje organizacije (SEV) i percepcija vjerojatnosti nastupa kibernetičkog rizika (PROB) demonstriraju relativno niže R^2 vrijednosti, što može sugerirati manju eksplanatornu moć modela za ove varijable. Međutim, njihovi Q^2 pokazatelji i dalje postižu pozitivne vrijednosti. Navedeno ukazuje na činjenicu da, unatoč potencijalno nižoj eksplanatornoj moći, model zadržava prediktivnu relevantnost za ove konstrukte.

Pored provedene analize strukturalnog modela, za potrebe dubljeg razumijevanja predloženog modela, nužno je pažljivo razmatranje koeficijenata utjecaja u smislu njihove jačine. Stoga se u sljedećoj tablici pruža uvid u jačinu utjecaja pojedinih koeficijenata pomoću izračuna Cohenovog koeficijenta (f^2) puta strukturalnog modela ukupnih efekata unutar modela. Sukladno Hair et al. (2021), slaba jačina utjecaja je prisutna za pretpostavljenu vezu čiji

koeficijent f^2 iznosi između 0,02 i 0,15, srednje jaki utjecaj je prisutan za pretpostavljenu vezu čiji koeficijent iznosi između 0,15 i 0,35 te jak utjecaj čiji koeficijent premašuje f^2 koeficijent od 0,35.

Kako se u razmatranom istraživanju analizira medijacijski utjecaj, odnosno cilj je odrediti snagu specifičnog neizravnog utjecaja, preporuka je prema Lachowicz et al. (2018) jačinu neizravnog učinka kvadrirati te vrijednost usporediti u odnosu na prilagođenu Cohenove vrijednost koja je prepolovljena za analizu jačine direktnog utjecaja (Ogbeibu et al. 2021). Stoga nove granične vrijednosti za prosudbu jačine utjecaja su; veliki utjecaj >0,175, srednje jaki utjecaj >0,075 i mali učinak >0,01.

Tablica 57. Snaga utjecaja predviđenih veza između konstrukata unutar modela – analiza modela prvog reda

Pretpostavljene veze	f^2	v^2	Snaga utjecaja
PROB -> FEA	0,042	/	Mali utjecaj
PROB -> REG	0,001	/	< Mali utjecaj
SEV -> FEA	0,212	/	Srednje jaki utjecaj
SEV -> REG	0,142	/	Mali utjecaj
PROB -> INT*		0,003	< Mali utjecaj
SEV -> INT*		0,026	Mali utjecaj
SEFF -> INT	0,302	/	Srednje jaki utjecaj
FEA -> INT	0,054	/	Mali utjecaj
REG -> INT	0,027	/	Mali utjecaj
OPBI -> PROB	0,028	/	Mali utjecaj
OPBI -> SEV	0,007	/	< Mali utjecaj
REC -> PROB	0,113	/	Mali utjecaj
REC -> SEV	0,086	/	Mali utjecaj
Kontrolne varijable			
EMP -> INT	0,000	/	< Mali utjecaj
IT_EXP_1 -> INT	0,003	/	< Mali utjecaj
SEC_1 -> INT	0,002	/	< Mali utjecaj
DMAT_1 -> INT	0,024	/	Mali utjecaj

Napomena: * označava primjenu prilagođenog Cohenovog kriterija za procjenu jačine neizravne veze.

Izvor: Izrada autora

Analiza snage utjecaja predviđenih veza unutar modela, temeljena na Cohenovom koeficijentu f^2 za izravne veze te prilagođenom Cohenovom koeficijentu v^2 za neizravne veze, pruža uvid u praktičnu važnost odnosa između pojedinih konstrukata (*Tablica 57*). Između razmatranih direktnih veza, s obzirom na jačinu utjecaja, izdvaja se veza između varijable percepcija ozbiljnosti utjecaja kibernetičkog rizika kao prijetnje (SEV) i varijable strah (FEA) te veza između varijable percepcija o sposobnosti suočavanja s kibernetičkim rizicima organizacije (SEFF) i namjere upravljanja kibernetičkim rizicima na razini organizacije (INT). U oba navedena slučaja, veze su srednje jakosti, što ukazuje na to da su varijabilnosti endogenih konstrukata (FEA i INT) u najvećoj mjeri određene spomenutim relacijama

Ostale direktne veze uglavnom su kategorizirane kao veze s malim utjecajem. Nadalje, što se tiče analize jakosti utjecaja neizravnih veza, za razmatrane veze utjecaj je generalno slab ili njegova jakost ne prelazi granicu postojanja slabog utjecaja. Kod razmatranih kontrolnih varijabli u modelu (veličina poslovne organizacije - EMP, iskustvo rada na IT poslovima - IT_EXP_1, djelatnost - SEC_1, stupanj digitalne zrelosti - DMAT_1), samo razina digitalne zrelosti poslovne organizacije iskazuje mali utjecaj, za ostale kontrolne varijable utjecaj je niži od razine koju ocjenjujemo kao slab utjecaj.

5.2.5. Analiza modela drugog reda u okviru glavnog istraživanja

Prethodno razmotren model predstavlja model prvog reda gdje se svaki konstrukt definira putem skupa indikatora. Slijedi analiza modela višeg reda (*engl. Higher Order Construct – HOC*) kojeg karakterizira veći stupanj složenosti s obzirom da predviđa više razina latentnih konstrukata (Hair et al., 2019). U okviru predstavljenog istraživanja, razmotren je model drugog reda, pri čemu se razmatra jedan konstrukt koji se sastoje od dvije latentne razine. U njima, konstrukt višeg reda (glavni konstrukt), postaje uzrok niza konstrukata prvog reda. Primjenom modela drugog reda, faktori prvog reda postaju sastavni dijelovi ili komponente faktora drugog reda (Hair et al., 2019).

S obzirom da je u središtu istraživanja percepcija prijetnje te da se prihvaća stajalište kako je percepcija prijetnje odraz percepcije učestalosti (PROB) i intenziteta (ozbiljnosti utjecaja) potencijalne prijetnje kakvu predstavlja kibernetički rizik (SEV), u nastavku se odabire pristup izrade konstrukta višeg reda za varijablu percepcija prijetnje, istodobno se uvođenjem konstrukta višeg reda potvrđuje robusnost procjene (Hair et al. 2021; Sarstedt et al., 2019).

Po uzoru na prethodno poglavlje, analizira se mjerni (vanjski) model koji mora ispuniti dva kriterija. Prvi kriterij odnosi se na mjerne modele komponenti nižeg reda, navedeno je potvrđeno uvidom u poglavlje 5.2.4. te drugi kriterij koji će se razmotriti u okviru ovog poglavlja, a odnosi se na test konvergentne i diskriminantne valjanosti. S obzirom da je prilikom procjene postavljeno kako je konstrukt prvog reda i konstrukt drugog reda reflektivan, korišten je reflektivno-reflektivan mjerni model.

U cilju testiranja pouzdanosti te konvergentne valjanosti, prezentirana je *Tablica 58* koja sadržava pokazatelj faktorskog opterećenja i njihovu statističku značajnost, Cronbach alpha koeficijent, CR pokazatelj te AVE pokazatelj.

Nastavljajući se na analizu prvog reda, indikatori u konačnom modelu prikazani su u *Tablici 58*. U formuliranju konstrukta višeg reda, sukladno Becker et al. (2012) korištena je metoda u dvije faze (*engl. disjoint two stage approach*).

Tablica 58. Rezultati analize pouzdanosti i konvergentne valjanosti PLS-SEM modela – analiza modela drugog reda

Konstrukt višeg reda	Konstrukt nižeg reda	Vanjsko opterećenje	Cronbach alpha	CR	AVE
PERCEPCIJA PRIJETNJE	PROB	0,874***	0,750	0,888	0,799
	SEV	0,913***			

Napomena: *p<0,05; **p<0,01; ***p<0,001

Rezultati analize konvergentne pouzdanosti i valjanosti za varijable prvog reda su neprimijenjene u odnosu na analizu provedenu u poglavlju 5.2.4. (Tablica 49).

Izvor: Prikaz autora

Vrijednosti standardiziranog vanjskog opterećenja ukazuju koliko dobro svaki konstrukt nižeg reda (*engl. Lower order construct - LOC*) u konkretnom slučaju konstrukt prvog reda, predstavlja latentnu konstrukciju višeg reda. S obzirom na vanjska opterećenja koja iznose 0,874 za percepciju učestalosti pojavljivanja kibernetičkih rizika (PROB) i 0,913 za percepciju ozbiljnosti utjecaja kibernetičkih rizika kao prijetnje na poslovanje organizacije (SEV), zaključuje se kako faktori prvog reda dobro odražavaju faktor drugog reda. Temeljem uvida u vrijednosti Cronbach alpha pokazatelj, koji mjeri unutarnju pouzdanost te CR pokazatelja koji mjeri ukupnu pouzdanost (kompozitna pouzdanost), s obzirom na vrijednosti veće od 0,7, zaključuje se kako konstrukti nižeg reda dobro odražavaju (predstavljaju) isti latentni konstrukt višeg reda. Razmatra se konvergentna valjanost pomoću AVE pokazatelja, te je za konstrukt

drugog reda vrijednost zadovoljavajuća i premašuje granicu od 0,5. Navedeno ukazuje kako korištene mjere za konstrukt višeg reda, riječ je o konstruktima prvog reda, pozitivno koreliraju među sobom, a konstrukt višeg reda objašnjava 0,799 varijance konstrukata prvog reda.

S obzirom na činjenicu da konstrukti nižeg reda postižu zadovoljavajuće vrijednosti standardiziranih vanjskih opterećenja te činjenicu da Cronbach alpha pokazatelj, CR pokazatelj te AVE pokazatelj premašuju preporučene pragove, smatra se kako je određen pouzdan mjerni model.

U nastavku se analizira diskriminantna valjanost procijenjenog modela prema trima kriterijima; unakrsno opterećenje, Fornell-Larcker kriteriju te HTMT-u.

Tablica 59 prezentira rezultate diskriminantne valjanosti pomoću unakrsnih opterećenja. Rezultati ukazuju kako je faktorsko opterećenje svih korištenih mjera, jače na osnovnom konstruktu (konstruktu kojeg mjere ili kojem pripadaju) umjesto na drugim konstruktima. Temeljem procjene unakrsnih opterećenja, zaključuje se kako je postignuta diskriminantna valjanost.

Tablica 59. Rezultati analize diskriminantne valjanosti prema unakrsnim opterećenjima – analiza modela drugog reda

	PERCEPCIJA PRIJETNJE	SEFF	INT	FEA	REG	OPBI	REC
PROB	**0,874**	0,047	0,228	0,479	0,292	-0,153	0,313
SEV	**0,913**	0,062	0,263	0,578	0,445	-0,081	0,278
SEFF1_1	0,124	**0,733**	0,409	0,129	0,162	0,052	0,143
SEFF1_2	0,040	**0,846**	0,456	0,073	0,076	0,099	0,136
SEFF1_3	0,030	**0,914**	0,470	0,031	0,011	0,133	0,107
SEFF1_4	0,025	**0,919**	0,459	0,018	0,016	0,112	0,118
INT1_4	0,226	0,551	**0,939**	0,284	0,263	0,053	0,216
INT1_5	0,286	0,468	**0,934**	0,350	0,299	0,042	0,228
INT1_6	0,258	0,436	**0,910**	0,305	0,295	-0,014	0,191
FEA1_1	0,566	0,067	0,320	**0,951**	0,499	-0,046	0,317
FEA1_3	0,566	0,068	0,321	**0,951**	0,501	-0,065	0,302
REG1_1	0,385	0,008	0,244	0,491	**0,877**	-0,044	0,134
REG1_2	0,420	0,103	0,301	0,484	**0,902**	-0,045	0,157
REG1_3	0,345	0,061	0,259	0,444	**0,922**	-0,035	0,134
REG1_4	0,348	0,088	0,296	0,465	**0,890**	0,020	0,137

	PERCEPCIJA PRIJETNJE	SEFF	INT	FEA	REG	OPBI	REC
OPBI1_2	-0,056	0,128	0,060	-0,002	0,041	**0,745**	0,001
OPBI1_3	-0,076	0,143	0,076	-0,028	-0,002	**0,773**	0,017
OPBI1_4	-0,108	0,113	0,009	-0,089	-0,074	**0,828**	-0,004
OPBI2_1	-0,054	0,064	0,046	-0,002	0,010	**0,726**	0,055
OPBI2_3	-0,142	0,047	-0,015	-0,057	-0,034	**0,805**	-0,006
REC1_1	0,223	0,022	0,058	0,177	0,018	0,015	**0,774**
REC1_2	0,236	0,059	0,089	0,225	0,024	0,000	**0,777**
REC1_3	0,241	0,050	0,097	0,206	0,020	-0,003	**0,781**
REC2_1	0,182	0,040	0,165	0,267	0,229	0,005	**0,560**
REC2_2	0,232	0,188	0,273	0,245	0,182	0,040	**0,618**
REC2_3	0,218	0,234	0,260	0,219	0,204	-0,024	**0,540**

Izvor: Izrada autora

U *Tablici 60* prezentirana je korelacijska matrica među konstruktima pri čemu se na dijagonali nalaze vrijednosti drugog korijena prosječne izlučene varijance (AVE). S obzirom da su vrijednosti na dijagonali veće od svih koeficijenata korelacije promatranog konstrukta s ostalim konstruktima, svaki konstrukt (latentna varijabla) bolje objašnjava varijancu svojih indikatora u odnosu na indikatore ostalih konstrukata. Time se potvrđuje kako je svaki promatrani konstrukt različit u odnosu na ostale konstrukte predviđene modelom, a zaključuje se kako je postignuta diskriminantna valjanost konstrukata.

Tablica 60. Rezultati analize diskriminantne valjanosti prema Fornell-Larcker kriteriju – analiza modela drugog reda

	PERCEPCIJA PRIJETNJE	SEFF	INT	FEA	REG	OPBI	REC
PERCEPCIJA PRIJETNJE	0,894						
SEFF	0,062	0,856					
INT	0,276	0,525	0,928				
FEA	0,595	0,071	0,337	0,951			
REG	0,420	0,074	0,307	0,526	0,898		
OPBI	-0,127	0,117	0,030	-0,058	-0,030	0,776	
REC	0,329	0,146	0,229	0,326	0,157	0,009	0,683

Izvor: Izrada autora

Konačno, diskriminantna valjanost se prosuđuje temeljem HTMT omjera. Rezultati potvrđuju kako su sve vrijednosti u *Tablici 61* ispod granične vrijednosti koja iznosi 0,85 te se izdvaja zaključak analize, sukladno prethodnim dvjema metodama, kako nije prisutan problem izostanka diskriminantne valjanosti.

Tablica 61. Rezultati analize diskriminantne valjanosti prema HTMT pokazatelju – analiza modela drugog reda

	PERCEPCIJA PRIJETNJE	SEFF	INT	FEA	REG	OPBI	REC
PERCEPCIJA PRIJETNJE							
SEFF	0,079						
INT	0,332	0,584					
FEA	0,722	0,083	0,372				
REG	0,494	0,103	0,334	0,578			
OPBI	0,146	0,146	0,064	0,061	0,062		
REC	0,437	0,185	0,277	0,400	0,198	0,090	
EMP	0,077	0,085	0,079	0,067	0,035	0,038	0,070

Izvor: Izrada autora

Nakon zaključene faze analize mjernog modela, u nastavku se razmatra analiza strukturalnog modela. Strukturalni model predstavljen je vezama između konstrukata. Model se sastoji od 7 konstrukata (latentnih varijabli), od kojih su 3 egzogena konstrukta, a 4 endogena konstrukata, te 4 kontrolne varijable. Stoga se provjerava vrijednost dobivenih parametara u smislu smjera utjecaja, jakosti utjecaja, njihove značajnosti te adekvatnost modela.

Prvi korak u analizi strukturalnog modela je procjena kolinearnosti konstrukata što se provodi pomoću analize VIF vrijednosti strukturalnog modela. S obzirom da vrijednosti ne prelaze referentnu vrijednost od 5 te strožu referentnu vrijednost od 3,3, zaključuje se da problem multikolinearnosti nije prisutan (*Tablica 62*).

Tablica 62. Rezultati analize multikolinearnosti unutarnjeg modela – analiza modela drugog reda

	VIF
PERCEPCIJA PRIJETNJE -> FEA	1,000
PERCEPCIJA PRIJETNJE -> REG	1,000
SEFF -> INT	1,133

	VIF
FEA -> INT	1,391
REG -> INT	1,393
OPBI -> PERCEPCIJA PRIJETNJE	1,000
REC -> PERCEPCIJA PRIJETNJE	1,000
Kontrolne varijable	
EMP -> INT	1,015
IT_EXP_1 -> INT	1,080
SEC_1 -> INT	1,061
DMAT_1 -> INT	1,072

Izvor: Izrada autora

Sljedeći korak u analizi strukturalnog modela obuhvaća procjenu statističke signifikantnosti i snage utjecaja procijenjenih koeficijenata puta. Statistička značajnost je izračunata putem „*bootstraping*“ procedure.

Tablica 63. Rezultati strukturalnog modela – analiza modela drugog reda

Pretpostavljena veza	Koeficijent puta (β)	Sredina uzorka	Standardna devijacija (STDEV)	Pokazatelj T-vrijednosti	Pokazatelj P-vrijednosti
PERCEPCIJA PRIJETNJE -> FEA	0,595	0,596	0,025	23,407	0,000
PERCEPCIJA PRIJETNJE -> REG	0,420	0,421	0,033	12,566	0,000
SEFF -> INT	0,452	0,452	0,036	12,614	0,000
FEA -> INT	0,212	0,213	0,034	6,177	0,000
REG -> INT	0,151	0,151	0,038	3,993	0,000
OPBI -> PERCEPCIJA PRIJETNJE	-0,130	-0,139	0,035	3,757	0,000
REC -> PERCEPCIJA PRIJETNJE	0,330	0,333	0,037	9,013	0,000
EMP -> INT	0,012	0,017	0,021	0,591	0,555
IT_EXP_1 -> INT	0,094	0,094	0,063	1,503	0,133
SEC_1 -> INT	0,089	0,088	0,079	1,130	0,259
DMAT_1 -> INT	0,257	0,256	0,067	3,824	0,000

Izvor: Izrada autora

Temeljem *Tablice 64* koja sadržava rezultate testa statističke značajnosti pretpostavljenih veza unutar modela, moguće je donijeti prosudbu o prihvaćanju ili odbacivanju postavljenih hipoteza. Potvrđuje se kako pristranost optimizma značajno i negativno utječe na percepciju kibernetičke prijetnje kojom je izložena poslovna organizacija (H1a) (OPBI -> PERCEPCIJA PRIJETNJE; β=-0,130, p=0,000). Potvrđuje se kako pristranost dostupnosti značajno pozitivno utječe na percepciju kibernetičke prijetnje kojom je izložena poslovna organizacija (H1b) (REC -> PERCEPCIJA PRIJETNJE; β=0,330, p=0,000). **Stoga se prihvaća hipoteza H1 kojom se tvrdi kako kognitivne pristranosti glavnih izvršnih menadžera značajno utječu na percepciju kibernetičke prijetnje kojoj je izložena poslovna organizacija.**

Hipoteza H2 pretpostavlja medijacijski utjecaj emocija, stoga je uputno prikazati *Tablicu 64* koja pruža uvid u produkt putanja predviđenih veza postavljene medijacije.

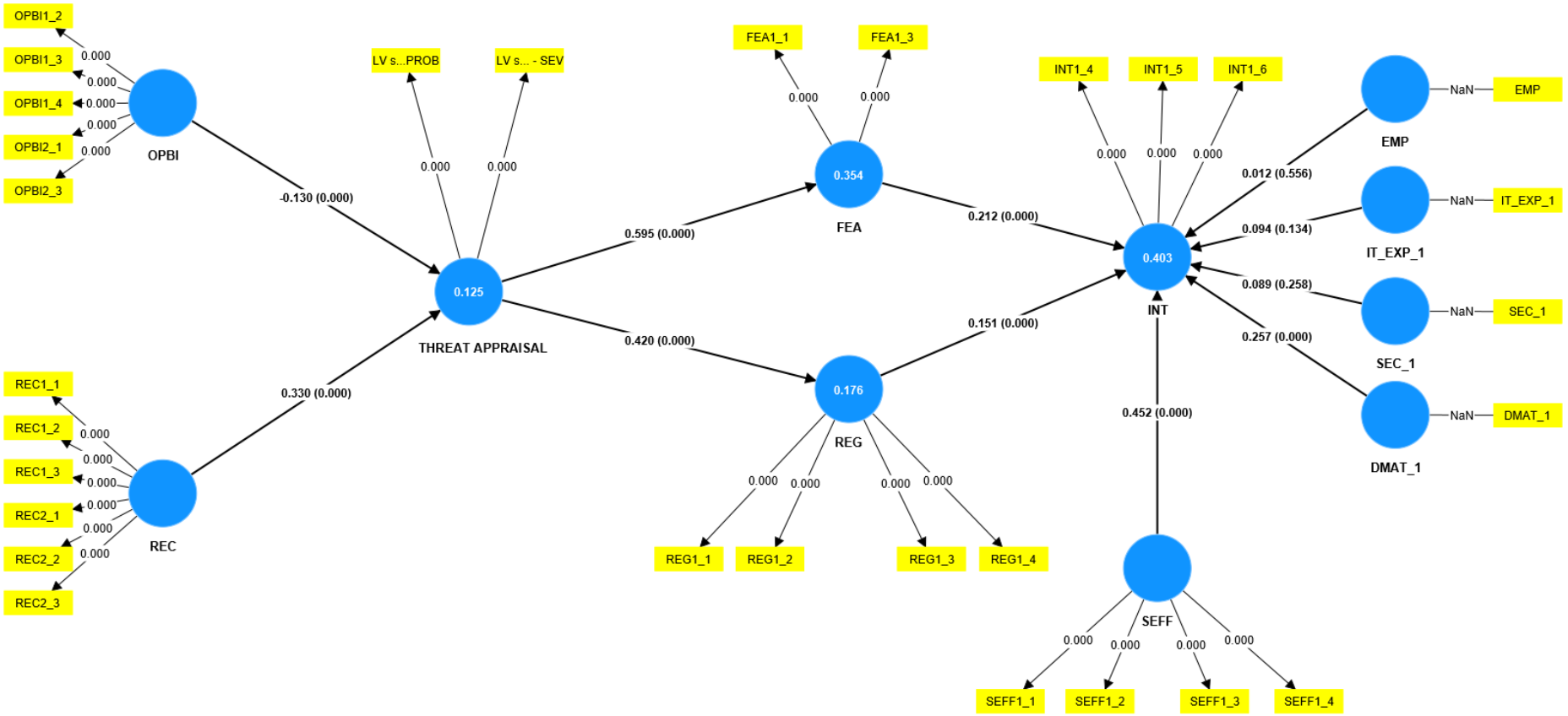
Tablica 64. Rezultati strukturalnog modela – Specifični i ukupni indirektni utjecaj – analiza modela drugog reda

Specifični indirektni utjecaj					
	Koeficijent puta	**Sredina uzorka**	**Standardna devijacija**	**Pokazatelj T-vrijednosti**	**Pokazatelj P-vrijednosti**
PERCEPCIJA PRIJETNJE -> FEA -> INT	0,126	0,127	0,022	5,819	0,000
PERCEPCIJA PRIJETNJE -> REG -> INT	0,063	0,064	0,017	3,656	0,000
Ukupni indirektni utjecaj					
	Koeficijent puta	**Sredina uzorka**	**Standardna devijacija**	**Pokazatelj T-vrijednosti**	**Pokazatelj P-vrijednosti**
PERCEPCIJA PRIJETNJE -> INT	0,190	0,191	0,021	8,845	0,000

Izvor: Izrada autora

Potvrđuje se kako je utjecaj percepcije prijetnje na namjeru upravljanja kibernetičkim rizicima posredovan emocijama (H2) (PERCEPCIJA PRIJETNJE -> INT; β=0,190, p=0,000). Uvidom u specifični indirektni utjecaj, daje se razlučiti kako medijacijsku ulogu potvrđuje emocija strah (H2a) (PERCEPCIJA PRIJETNJE -> FEA -> INT; β=0,126, p=0,000) te emocija žaljenje (H2b) (PERCEPCIJA PRIJETNJE -> REG -> INT; β=0,063, p=0,000).

Temeljem rezultata strukturalnog modela, **vidljivo je kako percepcija glavnog izvršnog menadžera o sposobnosti suočavanja organizacije s kibernetičkim rizicima pozitivno utječe na namjeru upravljanja kibernetičkim rizicima (H3)** (SEFF -> INT; β=0,452, p=0,000).



Slika 11. Dijagram putanje uz prikaz strukturalnih koeficijenata i njihove značajnosti – analiza modela drugog reda

Izvor: Izrada autora uz pomoć programa SmartPLS

Rezultati strukturalnog modela drugog reda grafički su prezentirani na *Slici 11*. Prikazane su značajnosti standardiziranih vanjskih faktorskih opterećenja, koeficijenti putanje strukturalnog modela i njihova značajnost te koeficijenti determinacije (R^2) za sve endogene konstrukte (faktore).

Temeljem vrijednosti koeficijenta determinacije, prilagođenog koeficijenta determinacije i Stone-Geisser Q^2 pokazatelja provedena je procjena strukturalnog modela.

Tablica 65. Vrijednost za koeficijent determinacije, prilagođeni koeficijent determinacije i Q^2 pokazatelj – analiza modela drugog reda

Endogeni konstrukti	R^2	Prilagođeni R^2	Q^2
PERCEPCIJA PRIJETNJE	0,125	0,122	0,114
FEA	0,354	0,353	0,089
REG	0,176	0,175	0,023
INT	0,403	0,396	0,275

Izvor: Izrada autora

Sukladno *Tablici 65*, konstrukti FEA i INT ističu se s najdominantnijim R^2 vrijednostima. Ovo sugerira da odabrani prediktori u modelu efikasno objašnjavaju varijabilnost ovih konstrukata, čime se postiže robusna eksplanatorna snaga u kontekstu ovih varijabli.

S druge strane, konstrukti PERCPECIJA PRIJETNJE i REG demonstriraju relativno niže R^2 vrijednosti, što može sugerirati manju eksplanatornu moć modela za ove varijable. Međutim, njihovi Q^2 pokazatelji i dalje postižu pozitivne vrijednosti. To ukazuje na činjenicu da, unatoč potencijalno nižoj eksplanatornoj moći, model zadržava prediktivnu relevantnost za ove konstrukte.

Pored provedene analize strukturalnog modela, za potrebe dubljeg razumijevanja predloženog modela, nužno je pažljivo razmatranje koeficijenata utjecaja u smislu njihove jačine. Stoga se u *Tablici 66* pruža uvid u jačinu utjecaja pojedinih koeficijenata pomoću izračuna Cohenovog koeficijenta (f^2) puta strukturalnog modela ukupnih efekata unutar modela.

Tablica 66. Snaga utjecaja predviđenih veza između konstrukata unutar modela – analiza modela drugog reda

Pretpostavljene veze	f^2	v^2	Snaga utjecaja
PERCEPCIJA PRIJETNJE -> FEA	0,548	/	Jaki utjecaj
PERCEPCIJA PRIJETNJE -> REG	0,214	/	Srednje jaki utjecaj
PERCEPCIJA PRIJETNJE -> INT*	/	0,036	Mali utjecaj
SEFF -> INT	0,302	/	Srednje jaki utjecaj
FEA -> INT	0,054	/	Mali utjecaj
REG -> INT	0,027	/	Mali utjecaj
OPBI -> PERCEPCIJA PRIJETNJE	0,019	/	Mali utjecaj
REC -> PERCEPCIJA PRIJETNJE	0,124	/	Mali utjecaj
Kontrolne varijable			
EMP -> INT	0	/	< Mali utjecaj
IT_EXP_1 -> INT	0,003	/	< Mali utjecaj
SEC_1 -> INT	0,002	/	< Mali utjecaj
DMAT_1 -> INT	0,024	/	Mali utjecaj

Napomena: * označava primjenu prilagođenog Cohenovog kriterija za procjenu jačine neizravne veze.

Izvor: Izrada autora

Analiza snage utjecaja predviđenih veza unutar modela, temeljena na Cohenovom koeficijentu f^2 za izravne veze te prilagođenom Cohenovom koeficijentu v^2 za neizravne veze, pruža uvid u praktičnu važnost odnosa između pojedinih konstrukata. Između razmatranih direktnih veza, s obzirom na jačinu utjecaja, izdvaja se veza između varijable (konstrukta) percepcija prijetnje i varijable strah (FEA) za koju je utvrđena jaka snaga utjecaja. Srednje jaki utjecaj uočava se između percepcije prijetnje i emocije žaljenje (REG) te između percepcije sposobnosti suočavanja s prijetnjom (SEFF) i namjere upravljanja kibernetičkim rizicima na razini organizacije (INT). Ostale direktne veze kategorizirane su kao veze s malim utjecajem.

Nadalje, što se tiče analize jakosti utjecaja neizravne veze pretpostavljene utjecajem percepcije prijetnje na namjeru upravljanja kibernetičkim rizicima na razini organizacije posredstvom emocija, utvrđen je mali utjecaj.

Kod razmatranih kontrolnih varijabli u modelu (EMP, IT_EXP_1, SEC_1, DMAT_1), samo razina digitalne zrelosti poslovne organizacije iskazuje mali utjecaj, za ostale kontrolne varijable utjecaj je niži od razine koju ocjenjujemo kao mali utjecaj.

Komparirajući dobivene rezultate provedene analize za model prvog i drugog reda uočava se konzistentnost u rezultatima odnosno procjeni modela te su zaključci u vezi postavljenih hipoteza konzistentni. Kako bi se dodatno potvrdila konzistentnost procjene sukladno Lu i White (2014) daje se uvid u promjene procijenjenih koeficijenata kada se specifikacija modela modificira na način da se postupno dodaju kontrolne varijable.

Tablica 67. Rezultati strukturalnog modela prvog reda – procjena konzistentnosti postupnim dodavanjem kontrolnih varijabli

Pretposta-vljena veza	Koeficijent puta (Beta)				
	Model bez kontrolnih varijabli	Model s jednom kontrolnom varijablom	Model s dvije kontrolne varijable	Model s tri kontrolne varijable	Model s četiri kontrolne varijable
PROB -> FEA	0,205***	0,205***	0,205***	0,205***	0,205***
PROB -> REG	0,042	0,042	0,042	0,042	0,042
SEV -> FEA	0,458***	0,458***	0,458***	0,458***	0,458***
SEV -> REG	0,421***	0,421***	0,421***	0,421***	0,421***
FEA -> INT	0,221***	0,220***	0,218***	0,216***	0,212***
REG -> INT	0,155***	0,155***	0,158***	0,159***	0,151***
SEFF -> INT	0,498***	0,496***	0,484***	0,479***	0,452***
OPBI -> PROB	-0,157***	-0,157***	-0,157***	-0,157***	-0,157***
OPBI -> SEV	-0,081*	-0,081*	-0,081*	-0,081*	-0,081*
REC -> PROB	0,315***	0,315***	0,315***	0,315***	0,315***
REC -> SEV	0,281***	0,281***	0,281***	0,281***	0,281***
EMP -> INT	/	0,017	0,016	0,013	0,012
IT_EXP_1 -> INT	/	/	0,113	0,101	0,094
SEC_1 -> INT	/	/	/	0,101	0,089
DMAT_1 -> INT	/	/	/	/	0,257***

Napomena: *p<0,05; **p<0,01; ***p<0,001

Izvor: Izrada autora

U *Tablicama 67 i 68* je razmotren model prvog reda koji se postupno proširuje za kontrolne varijable. Temeljem usporedbe rezultata osnovnog i postupno proširenih modela zaključuje se kako procijenjeni koeficijenti (pokazatelji puta) te procijenjena statistička značajnost pokazuju

minimalne promjene s dodavanjem kontrolnih varijabli. Stoga se potvrđuje robusnost procjene izravnih i neizravnih veza.

Tablica 68. Rezultati strukturalnog modela prvog reda – Specifični i ukupni indirektni utjecaj - procjena konzistentnosti postupnim dodavanjem kontrolnih varijabli

Specifični indirektni utjecaj					
Pretpostavljena veza	**Model bez kontrolnih varijabli**	**Model s jednom kontrolnom varijablom**	**Model s dvije kontrolne varijable**	**Model s tri kontrolne varijable**	**Model s četiri kontrolne varijable**
PROB -> FEA -> INT	0,045***	0,045***	0,045***	0,044***	0,043***
PROB -> REG -> INT	0,006	0,006	0,007	0,007	0,006
SEV -> FEA -> INT	0,101***	0,101***	0,100***	0,099***	0,097***
SEV -> REG -> INT	0,065***	0,065***	0,066***	0,067***	0,064***
Ukupni indirektni utjecaj					
PROB -> INT	0,052***	0,051***	0,051***	0,051***	0,050***
SEV -> INT	0,166***	0,166***	0,166***	0,166***	0,161***

Napomena: *p<0,05; **p<0,01; ***p<0,001

Izvor: Izrada autora

U *Tablicama 69 i 70* je razmotren model drugog reda koji se postupno proširuje za kontrolne varijable. Temeljem usporedbe rezultata osnovnog i postupno proširenih modela zaključuje se kako procijenjeni koeficijenti (pokazatelji puta) te procijenjena statistička značajnost pokazuju minimalne promjene s dodavanjem kontrolnih varijabli. Stoga se potvrđuje robusnost procjene izravnih i neizravnih veza.

Tablica 69. Rezultati strukturalnog modela drugog reda – procjena konzistentnosti postupnim dodavanjem kontrolnih varijabli

	Koeficijent puta (Beta)				
	Model bez kontrolnih varijabli	**Model s jednom kontrolnom varijablom**	**Model s dvije kontrolne varijable**	**Model s tri kontrolne varijable**	**Model s četiri kontrolne varijable**
PERCEPCIJA PRIJETNJE -> FEA	0,595***	0,595***	0,595***	0,595***	0,595***
PERCEPCIJA PRIJETNJE -> REG	0,420***	0,420***	0,420***	0,420***	0,420***
SEFF -> INT	0,498***	0,497***	0,485***	0,480***	0,452***
FEA -> INT	0,220***	0,219***	0,217***	0,216***	0,212***
REG -> INT	0,155***	0,155***	0,158***	0,159***	0,151***
OPBI -> PERCEPCIJA PRIJETNJE	-0,137***	-0,137***	-0,137***	-0,137***	-0,130***
REC -> PERCEPCIJA PRIJETNJE	0,330***	0,330***	0,330***	0,330***	0,330***

	Koeficijent puta (Beta)				
	Model bez kontrolnih varijabli	**Model s jednom kontrolnom varijablom**	**Model s dvije kontrolne varijable**	**Model s tri kontrolne varijable**	**Model s četiri kontrolne varijable**
EMP -> INT	/	0,021	0,016	0,013	0,012
IT_EXP_1 -> INT	/	/	0,113*	0,101	0,094
SEC_1 -> INT	/	/	/	0,101	0,089
DMAT_1 -> INT	/	/	/	/	0,257***

Napomena: *p<0,05; **p<0,01; ***p<0,001

Izvor: Izrada autora

Tablica 70. Rezultati strukturalnog modela drugog reda – Specifični i ukupni indirektni utjecaj - procjena konzistentnosti postupnim dodavanjem kontrolnih varijabli

Specifični indirektni utjecaj					
Pretpostavljena veza	**Model bez kontrolnih varijabli**	**Model s jednom kontrolnom varijablom**	**Model s dvije kontrolne varijable**	**Model s tri kontrolne varijable**	**Model s četiri kontrolne varijable**
PERCEPCIJA PRIJETNJE -> FEA -> INT	0,131***	0,130***	0,129***	0,128***	0,126***
PERCEPCIJA PRIJETNJE -> REG -> INT	0,065***	0,065***	0,066***	0,067***	0,063***
Ukupni indirektni utjecaj					
Pretpostavljena veza	**Model bez kontrolnih varijabli**	**Model s jednom kontrolnom varijablom**	**Model s dvije kontrolne varijable**	**Model s tri kontrolne varijable**	**Model s 4 kontrolne varijable**
PERCEPCIJA PRIJETNJE -> INT	0,196***	0,195***	0,195***	0,195***	0,190***

Napomena: *p<0,05; **p<0,01; ***p<0,001

Izvor: Izrada autora

6. ZAKLJUČNA RAZMATRANJA

U ovom dijelu rada objašnjavaju se i analiziraju glavni rezultati istraživanja i povezuje ih se s teorijskim okvirom koji je korišten u radu, potom se predstavljaju ograničenja provedenog istraživanja. U okviru zaključnog razmatranja nude se preporuke za buduća istraživanja s ciljem nadopune i produbljenja saznanja koje pruža ovo istraživanje. Konačno, poglavlje se zaključuje osvrtom na implikacije rezultata istraživanja za primjenu u praksi.

6.1. Rasprava o rezultatima istraživanja

Empirijsko istraživanje je provedeno na uzorku od 673 glavna izvršna menadžera koji upravljaju poslovnim organizacijama (trgovačkim društvima) na prostoru RH.

U svrhu razumijevanja karakteristika poslovnih organizacija unutar uzorka, analizirane su varijable: sektorska distribucija i distribucija prema broju zaposlenih kao pokazatelj veličine poslovne organizacije, i razina digitalne zrelosti te stvarna iskustva s djelovanjem kibernetičkih rizika u okviru poslovanja organizacije. Ove informacije omogućuju detaljniji uvid u obilježja uzorka i njegovu reprezentativnost u odnosu na populaciju. Naime, uočeno je odstupanje u sektorskoj zastupljenosti između uzorka i populacije u slučaju sektora M i J koji su zastupljeni u okviru uzorka u većoj mjeri, no što je to slučaj s populacijom. S druge strane, sektori F i I su značajnije podzastupljeni u uzorku u usporedbi s populacijom. U slučaju ostalih sektora razlike u zastupljenosti unutar uzorka i populacije su manje izražene. U pogledu veličine poduzeća, uzorak postiže reprezentativnost, pri čemu dominiraju manje organizacije koje zapošljavaju između 5 i 10 zaposlenih. Financijski pokazatelji razmatrani kroz prihod i rezultat poslovanja organizacija unutar uzorka upućuju na visoku asimetriju unutar populacije, s većim brojem manjih organizacija koje ostvaruju niže prihode i skromne poslovne rezultate.

Sukladno očekivanjima, digitalna zrelost ispitanika varira među industrijama. Industrije, poput K i S, bilježe visoku digitalnu zrelost, druge, kao što su C i I, imaju nižu zastupljenost organizacija koje obilježava viši stupanj digitalne zrelosti. Ovi nalazi ukazuju na različite pristupe integraciji digitalnih tehnologija unutar poslovnih procesa različitih sektora.

Stavljajući fokus na iskustva s negativnim djelovanjem kibernetičkih rizika na poslovanje organizacije, dominantna većina glavnih izvršnih menadžera (83,66 %), smatra da kibernetički rizik do sada nije značajno negativno utjecao na poslovanje organizacije koju predstavljaju. U

svezi s time, a s obzirom na umjereno izražene namjere upravljanja kibernetičkim rizicima u sljedećih 12 mjeseci, zaključuje se kako je navedeno vjerojatnije rezultat izostanka kibernetičkih rizika, no što je rezultat adekvatne pripremljenosti na kibernetičke rizike i njihovo upravljanje. S druge strane, 9,96 % menadžera potvrđuje da je njihova organizacija doživjela značajne negativne posljedice uslijed nastupa kibernetičkih rizika.

Analiza iskustva poslovnih organizacija iz uzorka, s kibernetičkim rizicima prema sektorima, ukazuje kako su industrije K i S naročito osjetljive na kibernetičke prijetnje s čak trećinom menadžera koji potvrđuju negativne posljedice u okviru dosadašnjeg poslovanja. Financijski sektor K, s obzirom na prirodu svoga poslovanja, često je meta kibernetičkih napada zbog potencijalnih financijskih koristi za pojedince koji ih uzrokuju. Slično navedenome, ostale uslužne djelatnosti, poput onih u sektor S, često uključuju obradu osobnih podataka klijenata, što ih čini atraktivnom metom za kibernetičke prijetnje.

U svrhu razumijevanja karakteristika glavnih izvršnih menadžera kao ključnih predstavnika poslovne organizacije, analizirane su sljedeće varijable; *obrazovanje, iskustvo vođenja poslovne organizacije* te *rada na IT poslovima* i *zadacima upravljanja rizicima*.

Uzevši u obzir obrazovanje ispitanika, dominira visoko obrazovanje, što sugerira da je formalno obrazovanje važan prediktor za ulogu glavnog izvršnog menadžera u organizacijama unutar uzorka. Velika većina ispitanika ima dugogodišnje iskustvo na poziciji glavnog izvršnog menadžera što sugerira da je uzorak sastavljen od iskusnih menadžera. Unutar uzorka dominiraju ispitanici s višegodišnjim iskustvom (5 i više godina) u barem jednom od dva razmatrana područja (iskustvo na poslovima IT-a i upravljanja rizicima), pri čemu gotovo 30 % ispitanika ima ekspertizu u obje domene.

Među populacijom glavnih izvršnih menadžera prevladava stajalište kako je pojava kibernetičkih rizika u poslovanju niska do umjerena, pri čemu je nastup kibernetičkog rizika s utjecajem na financijski gubitak ili gubitak ugleda razmatran kao nešto manje vjerojatan u usporedbi s krađom informacija ili oštećenjem ICT infrastrukture. Razmatrajući percepciju ozbiljnosti utjecaja kibernetičkih rizika na poslovanje organizacije kao dodatnu dimenziju percepcije prijetnje, uočava se kako prosječni ispitanik percipira da bi realizacija kibernetičkog rizika rezultirala neznačajnim prekidom rada, te da bi nastupom kibernetičkog rizika, mala količina podataka bila ugrožena. Što se tiče stajališta o sposobnosti organizacije u vezi suočavanja s prijetnjom, glavni izvršni menadžeri prepoznaju važnost i doprinos upravljanja kibernetičkim rizicima, ali i izazove i troškove koji su s tim povezani.

Glavni izvršni menadžeri iskazuju umjerenu sklonost prema provođenju mjera upravljanja kibernetičkim rizicima u poslovnim organizacijama u narednih 12 mjeseci, pri čemu je upravljanje kibernetičkim rizicima u organizacijama najizraženije kroz segment jačanja svijesti kod zaposlenika.

Ispitanici iskazuju umjerenu sklonost pristranosti optimizma. Iskazuju blago do umjerenu pristranost dostupnosti koja proizlazi temeljem informacija iz okoline (*izvještaji u medijima, industrijski izvještaji, iskustva drugih organizacija* i *osobna iskustva*), budući da jako mali udio glavnih izvršnih menadžera potvrđuje postojanje nedavnog negativnog iskustva s kibernetičkim rizicima. Dodatno, među ispitanicima prepoznaje se prisutnost emocija, pri čemu postoji blagi do umjereni osjećaj straha te žaljenje koje je intenzivnije prisutno u odnosu na strah.

Pomoću PLS-SEM tehnike testiran je model koji predviđa kognitivne pristranosti (optimističnu pristranost, pristranost dostupnosti) te percepciju sposobnosti suočavanja, kao egzogene latentne varijable. Istovremeno se percepcija kibernetičkih rizika kao prijetnje, emocije (strah i žaljenje) i namjera upravljanja kibernetičkim rizicima razmatraju kao endogene latentne varijable. Kombiniran je model prve razine te model druge razine kako bi se dobili relevantni rezultati koji opisuju karakteristike mjernog modela te strukturalne veze predviđene modelom, što u konačnici osigurava testiranje postavljenih hipoteza.

Analiza mjernog modela u oba slučaja (*model prve* i *druge razine*) potvrđuje pouzdanost te konvergentnu valjanost konstrukata s obzirom da se vrijednosti Cronbach alphe, CR i AVE nalaze u okvirima prihvatljivih granica. Diskriminantna valjanost potvrđuje se primarno kroz HTMT pokazatelj, koji potvrđuje rezultate testa unakrsnog opterećenja, te Fornell Larcker kriterij. VIF test potvrđuje kako među konstruktima nije prisutan problem multikolinearnosti.

Temeljem dobivenih vrijednosti koeficijenta determinacije i korigiranog koeficijenta determinacije, koji iznose 0,403 i 0,396, može se zaključiti da predloženi te analizirani model ima snažnu eksplanatornu snagu. Navedeno sugerira kako model uspješno objašnjava varijabilnost u podacima, a shodno rezultatima Stone-Geisser Q^2 pokazatelja, potvrđuje i prediktivnu relevantnosti što znači da može poslužiti i u predviđanju ishoda. Izdvojeni pokazatelji otkrivaju da je model koristan te pouzdan alat za istraživanje u domeni odluka u vezi kibernetičkih rizika.

Robusnost procjene potvrđuje se kroz dimenziju detaljno razmotrenog modela prve razine nakon čega je uslijedila analiza modela druge razine, ali i kroz testiranje konzistentnosti u

procijeni parametara te njihovoj statističkoj značajnosti, na način da su se osnovnom modelu postupno pridodavale kontrolne varijable.

Svrha istraživanja jest doprinijeti razumijevanju namjera glavnih izvršnih menadžera prema upravljanju kibernetičkim rizicima, integrirajući kognitivne pristranosti i emocije unutar modela motivacije za zaštitom. Time se tradicionalno razmatran PMT koncept proširuje za pretpostavke bihevioralne ekonomije što osigurava dublju perspektivu u stvarne odrednice namjere, a u kontekstu ovog istraživanja, namjere glavnih izvršnih menadžera u pogledu upravljanja kibernetičkim rizicima poslovnih organizacija. Nastavno na svrhu istraživanja, testirana je temeljna istraživačka hipoteza:

Kognitivne pristranosti određuje razinu percepcije prijetnje koja posredstvom emocija utječe na namjeru upravljanja kibernetičkim rizicima

koja se sukladno konceptualnom modelu istraživanja detaljnije segmentira na hipoteze u nastavku.

H1 Kognitivne pristranosti glavnih izvršnih menadžera značajno utječu na percepciju kibernetičke prijetnje kojoj je izložena poslovna organizacija

Rezultati empirijske analize potvrđuju značajnu ulogu kognitivnih pristranosti, *pristranosti optimizma* i *pristranosti dostupnosti*, na percepciju kibernetičkih rizika kao prijetnje za poslovanje kod glavnih izvršnih menadžera. Rezultati dobivaju na težini, posebice kada se uvaži činjenica da među populacijom glavnih izvršnih menadžera iz uzorka prevladava višegodišnje iskustvo upravljanja poslovnom organizacijom i visok stupanj formalnog obrazovanja te da gotovo trećina menadžera u uzorku istodobno potvrđuje 5 i više godina iskustva na IT poslovima i poslovima upravljanja rizicima. Naime, premda sva obilježja uzorkovanih glavnih izvršnih menadžera sugeriraju racionalan pristup, s obzirom na uočenu umjerenu pojavu pristranosti optimizma, zaključuje se kako obilježja kibernetičkih rizika i kontekst vezan za odluke o upravljanju kibernetičkim rizicima podupiru pojavu kognitivnih pristranosti, odnosno pristup integriranja pristranosti optimizma unutar PMT modela.

U skladu s teorijom, empirijski rezultati jasno pokazuju kako pristranost optimizma uzrokuje smanjenje percepcije kibernetičke prijetnje kod glavnih izvršnih menadžera. Uz pristranost optimizma, rezultati istraživanja također ukazuju na značaj pristranosti dostupnosti. Sukladno teorijskim pretpostavkama da ovakva pristranost može pojačati percepciju prijetnje, empirijski rezultati potvrđuju navedenu tvrdnju. Rezultati sukladni ranijim istraživanjima (Kahneman et

al., 2019; Powell et al., 2011; Hodgkinson i Clarke, 2007; Malmendier i Tate, 2005; Hammond et al., 1998; Samuelson i Zeckhauser, 1988; Schwenk, 1984; Kahneman et al., 1982), doprinose tezi o utjecaju kognitivnih pristranosti na donošenje odluka i u menadžerskom kontekstu.

U kontekstu teorijskih implikacija, ovo istraživanje pridonosi postojećem znanju o integraciji kognitivnih pristranosti u PMT model, čime se omogućava bolje razumijevanje procesa oblikovanja percepcije kibernetičkog rizika kao prijetnje. Predloženi model omogućava sveobuhvatniji pogled na odluku glavnih izvršnih menadžera u vezi namjere upravljanja kibernetičkim rizicima. U nastavku je ponuđen detaljniji osvrt na pomoćne hipoteze te rezultate empirijske analize.

H1a Pristranost optimizma kod donositelja odluka značajno i negativno utječe na percepciju kibernetičke prijetnje kojom je izložena poslovna organizacija

Temeljem prezentiranih rezultata empirijske analize, uočeno je postojanje značajne veze između pristranosti optimizma i percepcije kibernetičke prijetnje kod glavnih izvršnih menadžera poslovne organizacije (OPBI -> PERCEPCIJA PRIJETNJE; β=-0,130, p=0,000). Smjer veze sukladan je teorijskoj pretpostavci, odnosno potvrđuje se negativno djelovanje pristranosti optimizma na percepciju kibernetičke prijetnje.

Usmjeravajući se na rezultate modela prvog reda, u kojemu se odvojeno razmatraju dimenzije kibernetičke prijetnje, percepcija učestalosti pojavljivanja i intenziteta utjecaja, uočava se kako pristranost optimizma statistički značajno utječe na percepciju učestalosti pojavljivanja kibernetičkih rizika (OPBI -> PROB; β=-0,157, p=0,000) i to izraženijim intenzitetom, no što je to slučaj kod, također statistički značajno potvrđenog, utjecaja pristranosti optimizma na percepciju ozbiljnosti utjecaja kibernetičkih rizika (OPBI -> SEV; β=-0,081, p=0,050).

Rezultati istraživanja usklađeni su s nalazima drugih autora poput Rhee et al. (2012) i Weinstein i Klein (1996) koji ističu izazove u kvantifikaciji vjerojatnosti budućih rizika, posebno kada objektivne procjene nisu lako dostupne, a sukladno Chen et al. (2021) i Oakley et al. (2020), integracija pristranosti optimizma u PMT model, s obzirom na statističku značajnost utjecaja, je opravdana.

Pristranost optimizma manifestira se kroz sklonost glavnih izvršnih menadžera uspoređivanju položaja organizacije kojom upravljaju i usporednih poslovnih organizacija, s obzirom na veličinu i industrijsku pripadnost. Dodatno, pristranost optimizma manifestira se i kroz sklonost preslikavanja povoljnih povijesnih ishoda u ranijem razdoblju na buduće razdoblje. Time se

pristranost optimizma problematizira kroz usporedbu s drugima, ali i samom organizacijom kojom menadžer upravlja u različitim vremenskim razdobljima.

Među populacijom glavnih izvršnih menadžera pojavljuje se umjerena pojava pristranosti optimizma, a uz potvrđenu značajnost utjecaja na percepciju prijetnje, potvrđuje se opravdanost pristupa koji integrira kognitivne pristranosti u okviru PMT teorije.

Ukoliko se razmotri postotak objašnjene varijance faktora percepcija prijetnje, s obzirom na kontekst istraživanja u kojem se razmatraju bihevioralne komponente modela, postignuta razina R^2 iznosi 0,125 te se zaključuje kako je varijabla slabo objašnjena. Razmatrajući jačinu veze pomoću izračuna Cohenovog koeficijenta (f^2), isti iznosi 0,019≈0,02, zaključuje se kako je riječ o malom utjecaju na percepciju prijetnje. Spomenuti rezultat ostavlja prostor propitivanju dodatnih faktora utjecaja, među njima i ostalih oblika kognitivnih pristranosti koji doprinose objašnjenju razine percepcije prijetnje.

H1b Pristranost dostupnosti kod donositelja odluka značajno pozitivno utječe na percepciju kibernetičke prijetnje kojom je izložena poslovna organizacija

Rezultati empirijske analize potvrđuju kako je prisutna statistički značajna veza između pristranosti dostupnosti i percepcije kibernetičkih rizika kao prijetnje kod glavnih izvršnih menadžera poslovne organizacije (REC -> PERCEPCIJA PRIJETNJE; β=0,330, p=0,000). Smjer veze je sukladan teorijskoj pretpostavci, odnosno potvrđuje se pozitivno djelovanje pristranosti dostupnosti na percepciju kibernetičke prijetnje.

Usmjeravajući se na rezultate modela prvog reda gdje se odvojeno razmatraju dimenzije kibernetičke prijetnje, percepcija učestalosti pojavljivanja i intenziteta utjecaja, uočava se da pristranost dostupnosti statistički značajno utječe na percepciju učestalosti pojavljivanja kibernetičkih rizika (REC -> PROB; β=0,315, p=0,000) i to izraženijim intenzitetom, no što je to slučaj kod, također statistički značajno potvrđenog, utjecaja pristranosti dostupnosti na percepciju ozbiljnosti utjecaja kibernetičkog rizika (REC -> SEV; β=0,281, p=0,000).

Potvrđena značajnost utjecaja pristranosti dostupnosti na percepciju prijetnje sugerira usklađenost s teorijskom pretpostavkom i to na način da nedavna negativna iskustva precjenjuje objektivnu vjerojatnost pojavljivanja kibernetičkih rizika (Ma et al., 2014). U kontekstu kibernetičkog rizika, ovaj fenomen proizlazi iz heuristike dostupnosti, unutar koje donositelji odluka temelje svoje procjene, ne na potpunim informacijama, već na lako dostupnim informacijama (Tversky i Kahneman, 1974).

U kontekstu predstavljenog istraživanja, pristranost dostupnosti ogleda se kroz nedavna vlastita iskustva s kibernetičkim rizicima u poslovanju organizacije i informacijama iz okoline koje uključuje izvještaje u medijima, industrijske izvještaje, iskustva drugih poslovnih organizacija te vlastita iskustva izvan poslovnog konteksta.

Među populacijom glavnih izvršnih menadžera pojavljuje se umjerena pojava pristranosti dostupnosti mjerena kroz aspekt utjecaja informacija iz okoline. Međutim, kada je riječ o nedavnim vlastitim iskustvima kao mjernoj čestici pristranost dostupnosti, uočavaju se distribucijska svojstva koja odstupaju od normalne distribucije, u smislu postojanja pozitivne asimetrije. Zbog toga se zaključuje da među populacijom dominiraju ispitanici koji upravljaju organizacijama kod kojih u nedavnom razdoblju (prethodnih 12 mjeseci) nije nastupilo negativno djelovanje kibernetičkih rizika. Sukladno teorijskom dijelu rada koji opisuje obilježja kibernetičkih rizika, valja naglasiti da se radi o recentnoj kategoriji rizika koja se sve učestalije pojavljuje. Međutim, zbog dodatnog obilježja nematerijalnosti, često je teško prepoznati kibernetičke rizike kao prijetnju s negativnim posljedicama na poslovanje. Na tragu navedenog, ograničeno osobno iskustvo s kibernetičkim rizicima čimbenik je koji doprinosi nižoj percepciji kibernetičkih rizika kao prijetnje.

Ukoliko se razmotri postotak objašnjene varijance faktora percepcija prijetnje, s obzirom na kontekst istraživanja u kojem se razmatraju bihevioralne komponente modela, postignuta razina R^2 iznosi 0,125 te se zaključuje kako je varijabla slabo objašnjena. Razmatrajući jačinu veze pomoću izračuna Cohenovog koeficijenta (f^2), isti iznosi 0,124, zaključuje se kako je riječ o malom utjecaju, što ukazuje kako pristranost dostupnosti samo u maloj mjeri doprinosi objašnjenju percepcije prijetnje. Ova činjenica ukazuje da još ima prostora za propitivanje ostalih faktora, među njima i ostalih oblika kognitivnih pristranosti koji doprinose objašnjenju razine percepcije prijetnje.

H2 Utjecaj percepcije prijetnje na namjeru upravljanja kibernetičkim rizicima posredovan je emocijama glavnog izvršnog menadžera

Istraživanje potvrđuje važnost uloge emocija straha i žaljenja. U kontekstu H2a, empirijski rezultati potvrđuju snažan medijacijski utjecaj straha između percepcije prijetnje i namjere upravljanja kibernetičkim rizicima, čime se naglašava koliko je kritičan osobni doživljaja prijetnje za upravljanje kibernetičkim rizicima među glavnim izvršnim menadžerima. S druge strane, H2b pretpostavlja značajnu ulogu žaljenja, sugerirajući kako donositelji odluka teže izbjegavaju osjećaj žaljenja, posebno u kontekstu potencijalno katastrofalnih kibernetičkih

prijetnji. Iako je žaljenje intenzivna emocija, njegova uloga kao medijatora slabije je izražena nego uloga straha.

Rezultati sukladni ranijim istraživanjima (Brundin et al., 2022; Brundin i Liu, 2015), doprinose tezi da se u kontekstu menadžerskih odluka uočava utjecaj kognitivnih pristranosti. Konkretno, istraživanje je potvrdilo da emocije djeluju kao medijator između percepcije prijetnje i namjere upravljanja kibernetičkim rizicima. Specifično, strah se pojavljuje kao dominantan medijator, motivirajući menadžere na upravljanje kibernetičkim rizicima. Rezultati istraživanja naglašavaju potrebu za uključivanjem emocija u tradicionalne modele odlučivanja, a razumijevanje uloge emocija u oblikovanju odluka glavnih izvršnih menadžera nudi važne implikacije za kreiranje učinkovitih odgovora poslovnih organizacija na kibernetičke prijetnje.

U kontekstu teorijskih implikacija, ovo istraživanje pruža doprinos razvoju PMT modela inkorporacijom aspekata bihevioralne ekonomije, posebno u pogledu uloge emocija u procesu donošenja odluka.

H2a Utjecaj percepcije prijetnje na namjeru upravljanja kibernetičkim rizicima posredovan je osjećajem straha kojeg iskazuje glavni izvršni menadžer

Temeljem rezultata empirijske analize potvrđuje se utjecaj percepcije prijetnje na namjeru upravljanja kibernetičkim rizicima posredstvom emocije strah (PERCEPCIJA PRIJETNJE -> FEA -> INT; β=0,126, p=0,000).

Usmjeravajući se na rezultate modela prvog reda u kojem se odvojeno razmatraju dimenzije kibernetičke prijetnje, percepcija učestalosti pojavljivanja i intenziteta utjecaja, uočava se specifični neizravni utjecaj kojim emocija straha potvrđuje svoju medijacijsku ulogu između percepcije prijetnje i namjere upravljanja kibernetičkim rizicima (PROB -> FEA -> INT; β=0,043, p=0,000 i SEV -> FEA -> INT; β=0,097, p=0,000). Uočava se kako je emocija strah izraženije određena percipiranim intenzitetom utjecaja kibernetičkih rizika na poslovanje organizacije u odnosu na percipiranu učestalost pojavljivanja kibernetičkih rizika.

Nalazi su sukladni teoriji iz koje proizlazi da strah može znatno utjecati na stavove, motivaciju i namjere ponašanja unutar organizacije (Posey et al., 2015). Rezultati podupiru argument da strah može djelovati kao medijator između procjene prijetnje i motivacije za zaštitom, što je sugerirano ranijim istraživanjima (Ogbanufe i Pavur, 2022, Vrhovec i Mihelič, 2021, Boss et al. 2015). Nalaze je posebno važno promotriti u kontekstu tvrdnji Moody et al. (2018) te Wall

i Buche (2017) koji su naglasili potencijalnu nepotpunost PMT modela bez integracije straha, što ukazuje na kritičnu ulogu koju strah ima u kontekstu percepcije i reakcije na prijetnje.

Razmatranje medijacijske uloge straha između percepcije prijetnje i namjere upravljanja kibernetičkim rizicima opravdava se činjenicom kako strah može objasniti ranije zabilježene nedosljednosti u vezi s utjecajem percepcije prijetnje na namjeru ponašanja (Cram et al., 2019). Strah se u kontekstu kibernetičkih prijetnji prepoznaje kao emocija s izraženim psihološkim manifestacijama, a spoznaja o izloženosti prijetnji inducira strah kao negativan emocionalni odgovor (Ma, 2022; Boss et al., 2015). Potvrđuje se da strah potiče motivaciju za zaštitom, čime se inicijalno predložena, ali ipak odbačena ideja Rogers (1983), potvrđuje kao ispravna, a dobiveni rezultati su usklađeni s Ma (2022) i Boss et al. (2015).

Važnost ovog istraživanja leži u razmatranju straha od kibernetičkih rizika u kontekstu odluka glavnih izvršnih menadžera. Uvažavajući njihovu značajnu osobnu izloženost organizaciji, u ovom se istraživanju prepoznaje da menadžeri mogu osjećati emociju straha, što može značajno oblikovati njihove namjere i ponašanje prema upravljanju kibernetičkim rizicima.

Rezultati ovog istraživanja pružaju doprinos razumijevanju kako emocija straha utječe na odluke vezane uz upravljanje kibernetičkim rizicima. Integrirajući teorijske postavke i empirijske dokaze, može se zaključiti kako donositelji odluka trebaju uzeti u obzir emocionalne aspekte kada razmatraju namjere u vezi upravljanja kibernetičkim rizicima.

H2b Utjecaj percepcije prijetnje na namjeru upravljanja kibernetičkim rizicima posredovan je osjećajem žaljenja kojega iskazuje glavni izvršni menadžer

Rezultati ukazuju na značajnu ulogu emocije žaljenja u procesu donošenja odluka vezanih uz upravljanje kibernetičkim rizicima. Točnije, empirijska analiza potvrdila je hipotezu H2b koja predviđa posredovanje emocije žaljenja između percepcije prijetnje i namjere upravljanja kibernetičkim rizicima (PERCEPCIJA PRIJETNJE -> REG -> INT; β=0,063, p=0,000).

Usmjeravajući se na rezultate modela prvog reda u kojemu se odvojeno razmatraju dimenzije kibernetičke prijetnje, percepcija učestalosti pojavljivanja i intenziteta utjecaja, uočava se da emocija žaljenja igra specifičnu medijacijsku ulogu između percepcije intenziteta prijetnje i namjere upravljanja kibernetičkim rizicima (PROB -> REG -> INT; β=0,006, p=0,360 i SEV -> REG -> INT; β=0,064, p=0,000). Uspoređujući utjecaj percipirane učestalosti i intenziteta utjecaja kibernetičkih rizika, uočava se kako je snažniji utjecaj potonjeg na namjeru upravljanja kibernetičkim rizicima posredstvom emocije žaljenje.

Istraživanje je potvrdilo kako osjećaj žaljenja ima pozitivan utjecaj na namjeru usvajanja adaptivnog odgovora, što je sukladno ranijim istraživanjima (Ogbanufe i Pavur 2022; Ogbanufe i Baham, 2022; Verkijika, 2019; 2018). Time ovo istraživanjem doprinosi tezi da je donositelj odluka motiviran poduzimati adaptivan odgovor u nastojanju da izbjegne osjećaj žaljenja (Wangzhou et al., 2021; Chen et al., 2018; Zeelenberga, 1999).

Rezultati ovog istraživanja pružaju doprinos razumijevanju kako emocija žaljenje utječe na odluke vezane uz upravljanje kibernetičkim rizicima. Integrirajući teorijske postavke i empirijske dokaze, može se zaključiti da donositelji odluka trebaju uzeti u obzir emocionalne aspekte kada razmatraju namjere u vezi upravljanja kibernetičkim rizicima.

H3 Percepcija glavnog izvršnog menadžera o sposobnosti suočavanja organizacije s kibernetičkim rizicima pozitivno utječe na namjeru upravljanja kibernetičkim rizicima

Temeljem rezultata empirijske analize, vidljivo je da postoji značajna veza između percepcije glavnih izvršnih menadžera o sposobnosti suočavanja organizacije s kibernetičkim rizicima i namjere upravljanja kibernetičkim rizicima (SEFF -> INT; β=0,452, p=0,000). Smjer veze sukladan je teorijskoj pretpostavci, odnosno potvrđuje se da u poslovnim organizacijama čiji glavni izvršni menadžeri procjenjuju veću sposobnost upravljanja kibernetičkim rizicima, namjera upravljanja kibernetičkim rizicima u poslovnim organizacijama u sljedećih 12 mjeseci, intenzivnije je iskazana.

S obzirom na postavljen nužni kriterij ispunjenosti mjernih svojstava, ali i konzistentnosti procjene modela u razini 1 i 2, percepcija sposobnosti suočavanja mjerena je ključnim konstruktom koji ukazuje na percepciju efikasnosti provedbe upravljanja kibernetičkim rizicima (samoučinkovitost). Time se konstrukti percepcija korisnosti te percepcija troškova upravljanja kibernetičkim rizicima ne razmatraju u okviru strukturalnog modela. Ipak, zbog toga što je fokus istraživanja potpunije razumijevanje uloge percepcije prijetnje i jer je u ranijim istraživanjima postignut veći stupanj konzistentnosti procjene statističke značajnosti utjecaja percepcije sposobnosti suočavanja s prijetnjom na namjeru njenog upravljanja te zbog toga što su, u konačnici, zabilježena istraživanja koja ne obuhvaćaju sve tri dimenzije percepcije sposobnosti suočavanja s prijetnjom (*percepcija samoučinkovitosti, percepcija učinkovitost i percepcija troškova*), međutim, zadržavaju dimenziju percepcije efikasnosti (Ma, 2022; Aurigemma i Mattson 2019; Hina et al., 2019; Tu et al. 2015; Ifinedo, 2014; 2012), prihvaća se navedeni pristup kao odgovarajući.

Ukoliko se razmotri postotak objašnjene varijance faktora namjere upravljanja kibernetičkim rizicima, s obzirom na kontekst istraživanja u kojem se razmatraju bihevioralne komponente modela, postignuta razina R^2 iznosi 0,403, zaključuje se da je varijabla dobro objašnjena, a s obzirom na utvrđenu snagu veze pomoću Cohenovog koeficijenta (f^2), jasno je da najveći doprinos objašnjenju varijance zavisne varijable proizlazi iz procjene sposobnosti suočavanja s prijetnjom. Utvrđeno je kako Cohenov koeficijent (f^2) iznosi 0,302 što upućuje na postojanje srednjeg jakog utjecaja percepcije sposobnosti suočavanja s kibernetičkim rizicima na namjeru upravljanja kibernetičkim rizicima. Navedeno upućuje da je među populacijom glavnih izvršnih menadžera namjera upravljanja kibernetičkim rizicima još uvijek dominantno određena percepcijom ekonomske provedivosti upravljanja kibernetičkim rizicima. Drugim riječima, percepcija učinkovitosti poslovne organizacije u namjeri provedbe aktivnosti upravljanja kibernetičkim rizicima je važnija u odnosu na percepciju prijetnje.

Iako se prema Sommested et al. (2014) moglo očekivati da će se u okviru poslovnog konteksta u kojemu organizacije postavljaju jasna pravila i politike postupanja prijetnje, percepcija prijetnje bilježiti veću važnost u oblikovanju odluke, navedeno se ne potvrđuje. Percepcija sposobnosti suočavanja važnija je odrednica namjere upravljanja kibernetičkim rizicima u odnosu na percepciju prijetnje, a rezultati su sukladni istraživanjima (Ma et al., 2022; Simonet i Teufel, 2019; Li et al., 2019; Barlette et al., 2015; Tu et al., 2015).

Konačno, zaključuje se da su empirijski rezultati istraživanja usklađeni s teorijskim okvirom koji ističe važnost percepcije suočavanja kao odrednice namjere upravljanja kibernetičkim rizicima.

Kontrolne varijable korištene u ovome istraživanju važne su za osiguranje valjanosti i vjerodostojnosti rezultata. Iako kontrolne varijable nisu bile primarni fokus istraživanja, uključenje specifičnih obilježja donositelja odluka i organizacije omogućilo je razumijevanje kompleksnih odnosa među glavnim varijablama istraživanja. Primjećuju se zanimljivi rezultati u vezi kontrolnih varijabli. Naime, stupanj digitalne zrelosti organizacije potvrđuje statistički značajan utjecaj na namjeru upravljanja kibernetičkim rizicima, pri čemu vrijedi kako je veći stupanj digitalne zrelosti povezan s izraženijom namjerom upravljanja kibernetičkim rizicima u sljedećih 12 mjeseci. U slučaju ostalih uključenih kontrolnih varijabli; *veličina poslovne organizacije, iskustvo rada na IT zadacima, sektorska pripadnost*, izostaje potvrda statističke značajnosti utjecaja na namjeru upravljanja kibernetičkim rizicima s kojima se suočava poslovna organizacija. Ova činjenica ukazuje na potencijalnu važnost digitalne zrelosti u kontekstu upravljanja kibernetičkim rizicima na razini organizacije.

Tablica 71. Sažetak procjene PLS-SEM modela

Hipoteze		Model prve razine					Model druge razine			
		LOC konstrukti HOC-a	Koeficijent puta (Beta)	Značajnost	Snaga utjecaja	Status	Koeficijent puta (Beta)	Značajnost	Snaga utjecaja	Status
H1	**Kognitivne pristranosti glavnih izvršnih menadžera značajno utječu na percepciju kibernetičke prijetnje kojoj je izložena poslovna organizacija**	/	/	/	/	**Potvrđena; mali utjecaj**	/	/	/	**Potvrđena; mali utjecaj**
H1a	Pristranost optimizma kod donositelja odluka značajno i negativno utječe na percepciju kibernetičke prijetnje kojom je izložena poslovna organizacija	PROB	-0,157	***	0,028	Potvrđena; mali utjecaj	-0,13	***	0,019	Potvrđena; mali utjecaj
		SEV	-0,081	*	0,007	Potvrđena; < mali utjecaj				
H1b	Pristranost dostupnosti kod donositelja odluka značajno pozitivno utječe na percepciju kibernetičke prijetnje kojom je izložena poslovna organizacija	PROB	0,315	***	0,113	Potvrđena; mali utjecaj	0,330	***	0,124	Potvrđena; mali utjecaj
		SEV	0,281	***	0,086	Potvrđena; mali utjecaj				
H2	**Utjecaj percepcije prijetnje na namjeru upravljanja kibernetičkim rizicima posredovan je emocijama glavnog izvršnog menadžera.**	**PROB**	**0,050**	***	**0,003** †	**Potvrđena; <mali utjecaj**	**0,190**	***	**0,036** †	**Potvrđena; mali utjecaj**
		SEV	**0,161**	***	**0,026** †	**Potvrđena; mali utjecaj**				
H2a	Utjecaj percepcije prijetnje na namjeru upravljanja kibernetičkim rizicima posredovan je osjećajem straha kojeg iskazuje glavni izvršni menadžer	PROB	0,043	***	0,002 †	Potvrđena; < mali utjecaj	0,126	***	0,016 †	Potvrđena; mali utjecaj
		SEV	0,097	***	0,01 †	Potvrđena; mali utjecaj				
H2b	Utjecaj percepcije prijetnje na namjeru upravljanja kibernetičkim rizicima posredovan je osjećajem žaljenja kojega iskazuje glavni izvršni menadžer	PROB	0,006	n.z.	0,000 †	Nije potvrđena; < mali utjecaj	0,063	***	0,004 †	Potvrđena; < mali utjecaj
		SEV	0,064	***	0,004 †	Potvrđena; < mali utjecaj				
H3	**Percepcija glavnog izvršnog menadžera o sposobnosti suočavanja organizacije s kibernetičkim rizicima pozitivno utječe na namjeru upravljanja kibernetičkim rizicima**	/	**0,452**	***	**0,302**	**Potvrđena; srednje jaki utjecaj**	**0,452**	***	**0,302**	**Potvrđena; srednje jaki utjecaj**

Napomena: *p<0,05; **p<0,01; ***p<0,001; n.z. – nije značajno; † - prepolovljena granica za procjenu jačine utjecaja

Izvor: Izrada autora

6.2. Ograničenja provedenog istraživanja

Unatoč doprinosu predstavljenog istraživanja u razumijevanju utjecaja kognitivnih pristranosti i emocija na upravljanje kibernetičkim rizicima, razmotren je ograničen broj kognitivnih pristranosti i emocija. Opravdanost zauzetog pristupa je ograničenje u provedivosti istraživanja. Svako dodavanje nove varijable u istraživanje donosi sa sobom dodatne izazove, kako u pogledu metodologije tako i u smislu resursa potrebnih za njegovo provođenje. Stoga, u okviru istraživanja nije bilo moguće uključiti širi skup kognitivni pristranosti i emocija. Proširenje istraživačkog fokusa na širi raspon kognitivnih pristranosti i emocija omogućilo bi sveobuhvatniju analizu i bolje razumijevanje odluka u vezi upravljanja kibernetičkim rizicima.

Podaci potrebni za glavno istraživanje prikupljeni su na prostoru Republike Hrvatske, što može zahtijevati potrebu za prilagodbom u drugim geografskim područjima. Važno se osvrnuti na ograničenje vremenskog konteksta. Istraživanje je provedeno u jedinstvenoj točki u vremenu uz izostanak razmatranja dinamičnosti koje bi bilo postignuto longitudinalnom studijom. S obzirom na ubrzani razvoj tehnologije, za očekivati je da će se percepcija kibernetičkih rizika kao prijetnje za poslovanje među populacijom glavnih izvršnih menadžera dodatno izgraditi.

Iako je korišten znanstveno prihvaćen i široko primijenjen pristup prikupljanja podataka putem anketnog upitnika u elektroničkoj formi te su podaci obrađeni modeliranjem putem strukturalnih jednadžbi, drugačija metodologija i proces prikupljanja podataka prilagođeni eksperimentalnom istraživanju pružili bi veću točnost prikupljenih podataka i veću pouzdanost procjene. Međutim, eksperimentalno istraživanje nije bilo provedivo. Stoga, odabranim pristupom koji predviđa oslanjanje na podatke temeljene na samoprocjeni, istraživanje suočava s izazovom dobivanja odgovora koji su percipirani kao društveno prihvatljivi i kojima se štiti ugled organizacije. Kako bi se umanjio značaj navedenog problema, jamčena je potpuna anonimnost kod sudjelovanja u istraživanju.

Prilikom prikupljanja odgovora nije bilo moguće kontrolirati jesu li dobiveni odgovori zaista odgovori glavnih izvršnih menadžera, međutim, kako bi se navedeni izazov suzbio u značajnijoj mjeri, prilikom odašiljanja ankete postavljene su jasne upute, pri čemu je naglašeno da je davanje odgovora predviđeno od strane glavnih izvršnih menadžera. Dodatno, vodilo se računa o tome da kontakt podaci budu u što manjoj mjeri generičke forme te da njihova kvaliteta osigura izravniji pristup glavnim izvršnim menadžerima.

Na tragu navedenih ograničenja, u nastavku se pružaju preporuke za buduća istraživanja.

6.3. Preporuke za buduća istraživanja

Kognitivne pristranosti u odlučivanju

Istraživanje je usredotočeno na pristranost optimizma i pristranost dostupnosti. Stoga, budući radovi mogu istražiti kako dodatni oblici kognitivnih pristranosti koji su moguća pojava s obzirom na obilježja kibernetičkih rizika, primjerice status quo (*engl. Status quo bias*) i efekt noja (*engl. Ostrich effect bias*), mogu oblikovati percepciju kibernetičkog rizika te reakciju na kibernetičke prijetnje. Dodatno, moguće je proučiti utjecaj kognitivnih pristranosti na percepciju sposobnosti suočavanja s prijetnjom. Proširenje istraživačkog fokusa na širi raspon kognitivnih pristranosti omogućit će sveobuhvatniju analizu i potpunije razumijevanje menadžerskih odluka u vezi upravljanja kibernetičkim rizicima.

Emocije u odlučivanju

Proučavanje namjera upravljanja kibernetičkim rizicima u okviru poslovne organizacije može biti nadopunjeno uključivanjem drugih oblika emocija, poput ljutnje i srama. Takav pristup pružio bi drugačiju perspektivu i doprinio razumijevanju namjera glavnih izvršnih menadžera u vezi upravljanja kibernetičkim rizicima.

Stav prema riziku te stvarno poduzimanje aktivnosti organizacije

Iako je istraživanje temeljeno na teoriji motivacije za zaštitom, u budućim istraživanjima postoji prostor za integraciju stava prema riziku unutar modela. Preporuka je proširiti korišten model na način da se razmotri utjecaj namjere na stvarno ponašanje glavnih izvršnih menadžera.

Konkretizacija oblika kibernetičkog rizika

Zavisna varijabla može biti konkretizirana na način da se heterogeni koncept kibernetičkih rizika usmjeri na konkretni oblik kibernetičkog rizika kao što je, primjerice, napad preko elektroničke pošte s ciljem krađe identiteta (*engl. Phishing*) i upravljanje istim.

Uvažavanje različitih kulturoloških okolnosti

S obzirom da se modelom razmatra postupanje glavnog izvršnog menadžera za koje je potvrđeno da su određeni pristranostima, percepcijom i emocijama, preporuka je istražiti primjenu modela u različitim kulturološkim kontekstima.

Odluke glavnih izvršnih menadžera u kontekstu upravljačkog odbora

Preporuka je razmotriti odluke glavnog izvršnog menadžera unutar šireg konteksta tima izvršnih menadžera.

Metodološka preporuka

Sugestija je primijeniti pristup longitudinalnog istraživanja, što bi pružilo uvid u dinamiku postavljenih relacija te njihovo potpunije razumijevanje, kao i eksperimentalni dizajn koji bi omogućio potpuniju razinu kontrole nad proučavanim relacijama. Sugestija je u budućim istraživanjima dati veću važnost kvalitativnom pristupu istraživanju te isti kombinirati s kvantitativnim pristupom.

6.4. Implikacije za primjenu u praksi

S obzirom na neprestane promjene unutar poslovnog konteksta i izazove donošenja odluka u uvjetima nepotpunih informacija, poslovne organizacije bi trebale redovito preispitivati i prilagođavati svoje strategije upravljanja rizicima, uzimajući u obzir kako objektivne tako i bihevioralne čimbenike.

Referirajući se na perspektivu prakse, istraživanje doprinosi razumijevanju uvjeta potrebnih za razvoj procesa upravljanja kibernetičkim rizicima i to primarno kroz obuhvatnije razumijevanje uloge glavnih izvršnih menadžera te načina na koji donose odluke u vezi upravljanja kibernetičkim rizicima. Temeljem provedenog istraživanja, vlasnici organizacija imaju uvid u to kakvu ulogu imaju kognitivne pristranosti i emocije u procjeni rizika i namjerama glavnih izvršnih menadžera u vezi upravljanja kibernetičkim rizicima. Integracija spoznaja predstavljenog istraživanja u razvoj strategije upravljanja organizacijskim rizicima potaknut će bolju pripremljenost poslovnih organizacija na suočavanje s izazovima digitalnog doba.

Istraživanje doprinosi proširenju spoznaja o odlučivanju u uvjetima neizvjesnosti kada se očekuju odstupanja od savršeno racionalne odluke. Naime, pristranost optimizma može smanjiti percepciju kibernetičkog rizika kao prijetnje, dok pristranost dostupnosti pojačava percepciju kibernetičkog rizika kao prijetnje. Temeljem navedenih spoznaja, vlasnici organizacija trebaju biti svjesni uloge pristranosti kada razmatraju pristup upravljanju kibernetičkim rizicima, a isto uvažiti kod razvoja programa informiranja i jačanja svijesti o kibernetičkim rizicima među glavnim izvršnim menadžerima. U okviru programa informiranja

i jačanja svijesti, nužno je uvažiti spoznaje o ulozi emocija koje mogu intenzivirati doživljenu prijetnju i doprinijeti adekvatnom odgovoru organizacije na kibernetičku prijetnju.

Osim vlasnicima, istraživanje može biti od koristi i krajnjim korisnicima usluga i proizvoda organizacija, odnosno poslovnim partnerima. Prepoznavanje intenziteta s kojim glavni izvršni menadžeri percipiraju kibernetički rizik kao prijetnju pomaže krajnjim korisnicima proizvoda i usluga te poslovnim partnerima da bolje shvate ozbiljnost s kojom organizacija pristupa kibernetičkim rizicima, što je uvjet sigurnije usluge, veće transparentnosti u komunikaciji te, u konačnici, izgradnji povjerenja u poslovnu organizaciju.

S obzirom na složenost odlučivanja u području kibernetičkih rizika, istraživanje naglašava važnost interdisciplinarnog pristupa u upravljanju kibernetičkim rizicima što podrazumijeva multidisciplinaran tim koji pokriva područje informacijskih i komunikacijskih tehnologija te ekonomije, u okviru čega je potrebno uvažiti spoznaje bihevioralne ekonomije. **Potonji pristup nije samo teorijski značajan, već ima i praktičnu primjenu te omogućava bolje razumijevanje načina na koji ljudski faktori i tehnološki aspekti doprinose kibernetičkim prijetnjama.** Formiranje interdisciplinarnog tima za donošenje odluka omogućuje integraciju različitih perspektiva i stručnosti, što je ključno za učinkovito suočavanje s kibernetičkim rizicima.

S obzirom na važnost uloge koju percepcija glavnog izvršnog menadžera o sposobnosti suočavanja organizacije s kibernetičkim rizicima ima na iskazivanje namjere upravljanja kibernetičkim rizicima, važno je u informiranju glavnih izvršnih menadžera od strane odjela podrške u odlučivanju, primarno odjela za upravljanje rizicima te IT odjela, inkorporirati podatke u vezi organizacijskih zahtjeva, mogućnosti, korisnosti, troškova i efikasnosti provedbe upravljanja kibernetičkim rizicima.

Ističući implikacije koje rezultati istraživanja imaju za poslovnu praksu, neizostavno je razmotriti utjecaj na javne politike. Razvoj javnih politika osnova je postizanja napretka u kibernetičkoj otpornosti poslovnih organizacija te društva u cjelini te ima presudan utjecaj na stvaranje adaptivnog odgovora na izloženost kibernetičkoj prijetnji. Povezivanje rezultata istraživanja s javnim politikama otvara prostor za unaprjeđenje regulatornog okvira te razvoj programa koji će učinkovito doprinijeti izazovu neadekvatne svijesti i nedovoljne angažiranosti ključnih donositelja odluka u razvoj i implementaciju prakse upravljanja kibernetičkim rizicima. Konačno, otvara prostor integraciji kibernetičkih rizika u upravljanje poslovnim rizicima organizacije.

S obzirom na to da istraživanje naglašava važnost uloge glavnih izvršnih menadžera u organizacijskoj promjeni i prihvaćanju adaptivnog pristupa, na način da se kibernetičkim rizicima upravlja, ova ključna uloga vodstva organizacije treba biti uzeta u obzir u javnim politikama. Učinkovite javne politike trebaju biti dizajnirane ne samo da potiču, već i da zahtijevaju aktivno uključivanje vodstva poslovnih organizacija u upravljanje kibernetičkim rizicima.

Važno je naglasiti ulogu integracije kibernetičkog rizika u sustav upravljanja poslovnim rizicima. Glavni izvršni menadžeri imaju presudan utjecaj u definiranju strateškog smjera organizacija kojima upravljaju i od ključne su važnosti za provođenje učinkovitih praksi upravljanja rizicima. Također, oni preuzimaju značajan dio odgovornosti u slučajevima gdje su kibernetički rizici zanemareni ili nisu adekvatno adresirani. Stoga, važnost njihove uloge u upravljanju rizicima, time i kibernetičkim rizicima, mora biti priznata i reflektirana kroz javne politike koje promiču odgovornost i proaktivnost na najvišim razinama upravljanja.

Nastavljajući se na sugestije, promjena javnih politika potaknula bi očekivanja u vezi potrebnih kompetencija vodstva organizacija, a regulatorne mjere mogle bi nametnuti obveznu edukaciju i/ili obuku. Cilj je stvoriti okruženje u kojem glavni izvršni menadžeri nisu samo svjesni složenosti kibernetičkih prijetnji, već su i obvezni proaktivno doprinositi upravljanju kibernetičkim rizicima kao integriranom dijelu svojih odgovornosti vezanih uz upravljanje ukupnim poslovnim rizicima. Integriranje rezultata istraživanja i javnih politika može znatno ojačati sveukupnu otpornost organizacija na kibernetičke prijetnje.

Nužno je jasno definiranje odgovornosti vodstva organizacije u slučaju propusta u vezi kibernetičke sigurnosti, ali i osigurati da vodstvo ima potrebnu podršku za razvoj upravljanja kibernetičkim rizicima poslovne organizacije. Predstavnici javnih institucija, prilikom dizajniranja kampanja i edukativnih programa kojima nastoje širiti svijest o kibernetičkim rizicima kao prijetnji te širiti važnost upravljanja kibernetičkim rizicima, mogu uvažiti spoznaje temeljene na predstavljenom istraživanju te usmjerenje postaviti na vodstvo poslovnih organizacija kao ključnih nositelja potrebnih promjena. Isto tako, mogu financirati programe edukacije o kognitivnim pristranostima, emocijama i njihovim posljedicama na donošenje odluka za glavne izvršne menadžere,, što može pridonijeti boljoj praksi upravljanja rizicima.

U konačnici, cilj ovih preporuka je osigurati da javne politike adekvatno prepoznaju i adresiraju ljudsku dimenziju kibernetičkih rizika.

POPIS LITERATURE

1) Abdalla, M., Jarrah, M., Abu-Khadrah, A., & bin Arshad, Y. (2021). Factors influencing the adoption of cyber security standards among public listed companies in Malaysia. *International Journal of Advanced Computer Science and Applications*, *12*(11).
2) Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. *ICIS 2006 proceedings*, 94. Dostupno na: https://aisel.aisnet.org/icis2006/94/, pristupljeno [20.11.2023.].
3) Addae, J. H., Sun, X., Towey, D., & Radenkovic, M. (2019). Exploring user behavioral data for adaptive cybersecurity. *User Modeling and User-Adapted Interaction*, *29*, 701-750.
4) Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1), tyy006.
5) Aiyer, B., Caso, J., Russell, P., & Sorel, M. (2022). New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers. McKinsey & Company. Dostupno na: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers, pristupljeno [20.11.2023.].
6) Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. U: Kuhl, J., Beckmann, J. (ur.) *Action control: From cognition to behavior*. Springer Berlin Heidelberg, 11-39.
7) Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes*, *50*(2), 179-211.
8) Ajzen, I. (2020). The theory of planned behavior: Frequently asked questions. *Human Behavior and Emerging Technologies*, *2*(4), 314-324.
9) Ajzen, I., & Fishbein, M. (1975). A Bayesian analysis of attribution processes. *Psychological bulletin*, *82*(2), 261-277.
10) Ajzen, I., & Madden, T. J. (1986). Prediction of goal-directed behavior: Attitudes, intentions, and perceived behavioral control. *Journal of experimental social psychology*, *22*(5), 453-474.

11) Alassaf, M., & Alkhalifah, A. (2021). Exploring the influence of direct and indirect factors on information security policy compliance: A systematic literature review. *IEEE Access*, *9*, 162687-162705.

12) Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2022). The drivers of cyber risk. *Journal of Financial Stability*, *60*, 100989.

13) Alharbi, S., & Drew, S. (2014). Using the technology acceptance model in understanding academics' behavioural intention to use learning management systems. *International Journal of Advanced Computer Science and Applications*, *5*(1), 143 –155.

14) Ali, S. E. A., Lai, F. W., Dominic, P. D. D., Brown, N. J., Lowry, P. B. B., & Ali, R. F. (2021a). Stock market reactions to favorable and unfavorable information security events: A systematic literature review. *Computers & Security*, *110*, 102451.

15) Ali, S. E. A., Lai, F. W., Hassan, R., & Shad, M. K. (2021b). The long-run impact of information security breach announcements on investors' confidence: The context of efficient market hypothesis. *Sustainability*, *13*(3), 1066.

16) Allianz. (2023). Allianz Risk Barometer - Identifying the Major Business Risks for 2023. Dostupno na: https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2023.pdf, pristupljeno [30.1.2023.].

17) Almansoori, A., Al-Emran, M., & Shaalan, K. (2023). Exploring the Frontiers of Cybersecurity Behavior: A Systematic Review of Studies and Theories. *Applied Sciences*, *13*(9), 5700.

18) Alohali, M., Clarke, N., Furnell, S., & Albakri, S. (2017, July). Information security behavior: Recognizing the influencers. In *2017 Computing Conference*, 844–853. IEEE. Dostupno na: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8252194, pristupljeno [20.11.2023.].

19) Alshammari, A., Benson, V., & Batista, L. C. (2023). *Emotional Cost of Cyber Crime and Cybersecurity Protection Motivation Behaviour: A Systematic Literature Review*. *PACIS 2023 Proceedings.* 133. Dostupno na: https://aisel.aisnet.org/pacis2023/133, pristupljeno [20.11.2023.].

20) Ameen, N., Tarhini, A., Shah, M. H., & Madichie, N. O. (2020). Employees' behavioural intention to smartphone security: A gender-based, cross-national study. *Computers in Human Behavior*, *104*, 106184.

21) Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies*, *23*, 1177-1206.

22) Angner, E., & Loewenstein, G. (2012). Behavioral Economics. U: Mäki, U. (ur.) *Handbook of the Philosophy of Science: Philosophy of Economics*. North-Holland. 641-689.

23) Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology*, *21*(1), 2-35.

24) Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, 437-443.

25) Arbanas, K. (2021). Radni okvir za procjenu i unapređenje kulture informacijske sigurnosti. Disertacija. Varaždin: Sveučilište u Zagrebu, Fakultet organizacije i informatike. Varaždin. Dostupno na: https://urn.nsk.hr/urn:nbn:hr:211:439511, pristupljeno [30.1.2023.].

26) Arcuri, M. C., Brogi, M., & Gandolfi, G. (2017). *How does cyber crime affect firms? The effect of information security breaches on stock returns.* First Italian Conference on Cybersecurity. Venice, Italy. Dostupno na: https://ceur-ws.org/Vol-1816/paper-18.pdf, pristupljeno [20.11.2023.].

27) Ardaya, A. B., Evers, M., & Ribbe, L. (2017). What influences disaster risk perception? Intervention measures, flood and landslide risk perception of the population living in flood risk areas in Rio de Janeiro state, Brazil. *International journal of disaster risk reduction*, *25*, 227-237.

28) Ariely, D., & Jones, S. (2008). *Predictably irrational*. New York: HarperCollins.

29) Ashby, S., Buck, T., Nöth-Zahn, S., & Peisl, T. (2018). Emerging IT risks: insights from German banking. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *43*(2), 180-207.

30) Aslam, M., Khan Abbasi, M. A., Khalid, T., Shan, R. U., Ullah, S., Ahmad, T., Saeed, S., Alabbad, D.A., & Ahmad, R. (2022). Getting Smarter about Smart Cities: Improving Data Security and Privacy through Compliance. *Sensors*, *22*(23), 9338.

31) Aurigemma, S., & Mattson, T. (2019). Generally speaking, context matters: Making the case for a change from universal to particular ISP research. *Journal of the Association for Information Systems*, *20*(12), 122-142.

32) Ayre, C., & Scally, A. J. (2014). Critical values for Lawshe's content validity ratio: revisiting the original methods of calculation. *Measurement and evaluation in counseling and development*, *47*(1), 79-86.

33) Badie, N., & Lashkari, A. H. (2012). A new evaluation criteria for effective security awareness in computer risk management based on AHP. *Journal of Basic and Applied Scientific Research*, *2*(9), 9331-9347.

34) Baer, W. S., & Parkinson, A. (2007). Cyberinsurance in it security management. *IEEE Security & Privacy*, *5*(3), 50-56.

35) Bagozzi, R. (2011). Measurement and Meaning in Information Systems and Organizational Research: Methodological and Philosophical Foundations. *MIS Quarterly, 35*(2), 261-292.

36) Barber, B. M., Odean, T., & Zheng, L. (2005). Out of sight, out of mind: The effects of expenses on mutual fund flows. *The Journal of Business*, *78*(6), 2095-2120.

37) Barlette, Y., Gundolf, K., & Jaouen, A. (2015). Toward a better understanding of SMB CEOs' information security behavior: Insights from threat or coping appraisal. *Journal of Intelligence Studies in Business*, *5*(1), 5-17.

38) Barlette, Y., Gundolf, K., & Jaouen, A. (2017). CEOs' information security behavior in SMEs: Does ownership matter?. *Systemes d'information management*, *22*(3), 7-45.

39) Barnes Jr, J. H. (1984). Cognitive biases and their impact on strategic planning. *Strategic Management Journal*, *5*(2), 129-137.

40) Baron, J. (2023). *Thinking and deciding*. 5 izd. Cambridge University Press.

41) Baruch, Y. (1999). Response rate in academic studies-A comparative analysis. *Human relations*, *52*(4), 421-438.

42) Beaudry, A., & Pinsonneault, A. (2010). The other side of acceptance: Studying the direct and indirect effects of emotions on information technology use. *MIS quarterly*, 689-710.

43) Beautement, A., Becker, I., Parkin, S., Krol, K., & Sasse, A. (2016). Productive security: A scalable methodology for analysing employee security behaviours. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, 253-270. Dostupno na: https://www.usenix.org/conference/soups2016/technical-sessions/presentation/beautement, pristupljeno [4.8.2023.].

44) Becker, J. M., Klein, K., & Wetzels, M. (2012). Hierarchical latent variable models in PLS-SEM: guidelines for using reflective-formative type models. *Long range planning*, 45(5-6), 359-394.

45) Bell, D. E. (1982). Regret in decision making under uncertainty. *Operations research*, *30*(5), 961-981.

46) Berghaus, S., & Back, A. (2016). Stages in digital business transformation: Results of an empirical maturity study. *MCIS 2016 Proceedings*. 22. Dostupno na: https://aisel.aisnet.org/mcis2016/22, pristupljeno [20.11.2023.].

47) Bergström, E., Lundgren, M., & Ericson, Å. (2019). Revisiting information security risk management challenges: a practice perspective. *Information & Computer Security*, *27*(3), 358-372.

48) Berthet, V. (2022). The impact of cognitive biases on professionals' decision-making: A review of four occupational areas. *Frontiers in psychology*, *12*, 802439.

49) Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *40*, 131-158.

50) Biener, C., Eling, M., & Wirfs, J. H. (2016). The determinants of efficiency and productivity in the Swiss insurance industry. *European Journal of Operational Research*, *248*(2), 703-714.

51) Blythe, J. M., & Coventry, L. (2018). Costly but effective: Comparing the factors that influence employee anti-malware behaviours. *Computers in Human Behavior*, *87*, 87-97.

52) Bode, C., Macdonald, J. R., & Merath, M. (2022). Supply disruptions and protection motivation: Why some managers act proactively (and others don't). *Journal of Business Logistics*, *43*(1), 92-115

53) Boehm, J., Dias, D., Lewis, C., Li, K., & Wallance, D. (2022). Cybersecurity trends: Looking over the horizon. *McKinsey & Company. March, 10.* Dostupno na: , https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon, pristupljeno [20.11.2023.].

54) Böhme, R. & Kataria, G. (2006) Models and measures for correlation in cyber-insurance, working paper, *Proceedings of the Fifth Workshop on the Economics of Information Security (WEIS)*, University of Cambridge. Dostupno na: https://www.econinfosec.org/archive/weis2006/docs/16.pdf [2.5.2023.]

55) Böhme, R., Laube, S., & Riek, M. (2019). A fundamental approach to cyber risk analysis. *Variance*, *12*(2), 161-185.

56) Bone, J. (2017). *Cognitive hack: the new battleground in cybersecurity... the human mind*. CRC Press Taylor & Francis Group.

57) Bose, I., & Leung, A. C. M. (2014). Do phishing alerts impact global corporations? A firm value analysis. *Decision Support Systems*, *64*, 67-78.

58) Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS quarterly*, *39*(4), 837-864.

59) Breakwell, G. (2014). *The Psychology of Risk*. Cambridge University Press.

60) Brewer, N. T., DeFrank, J. T., & Gilkey, M. B. (2016). Anticipated regret and health behavior: A meta-analysis. *Health Psychology, 35*(11), 1264–1275.

61) Brown, J. D. (2012). Understanding the better than average effect: Motives (still) matter. *Personality and Social Psychology Bulletin*, *38*(2), 209-219.

62) Brown, T. A. (2006). *Confirmatory factor analysis for astrlied research*. The Guilford Press.

63) Brundin, E., Liu, F., & Cyron, T. (2022). Emotion in strategic management: A review and future research agenda. *Long Range Planning*, *55*(4), 102144.

64) Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, *34*(3) 523-548.

65) Bureau van Dijk Electronic Publishing Ltd. (2023). Orbis database. Dostupno na: https://www.bvdinfo.com/en-gb/, pristupljeno [11.4.2023.].

66) Burns, A. J., Posey, C., Roberts, T. L., & Lowry, P. B. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior*, *68*, 190-209.

67) Burns, A. J., Roberts, T. L., Posey, C., & Lowry, P. B. (2019). The adaptive roles of positive and negative emotions in organizational insiders' security-based precaution taking. *Information Systems Research*, *30*(4), 1228-1247.

68) Busenitz, L. W., & Barney, J. B. (1997). Differences between entrepreneurs and managers in large organizations: Biases and heuristics in strategic decision-making. *Journal of business venturing*, *12*(1), 9-30.

69) Camerer, C. & Loewenstein, G. (2004). Behavioral Economics: Past, Present, Future, in Camerer, C., Loewenstein, G., and Rabin, M. (ur.) *Advances in Behavioral Economics*. Russell Sage Foundation, 3–51.

70) Campbell, J., Greenauer, N., Macaluso, K., & End, C. (2007). Unrealistic optimism in internet events. *Computers in human behavior*, *23*(3), 1273-1284.

71) Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer security*, *11*(3), 431-448.

72) Carfora, V., Caso, D., & Conner, M. (2017). Randomised controlled trial of a text messaging intervention for reducing processed meat consumption: The mediating roles of anticipated regret and intention. *Appetite*, *117*, 152-160.

73) Carver, C. S., Scheier, M. F., & Segerstrom, S. C. (2010). Optimism. *Clinical psychology review*, *30*(7), 879-889.

74) Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, *9*(1), 70-104.

75) Cebula, J. J., & Young, L. R. (2010). A taxonomy of operational cyber security risks. *Software Engineering Institute, Carnegie Mellon University*. Dostupno na: https://apps.dtic.mil/sti/citations/ADA537111, pristupljeno [20.11.2023.].

76) CERT. (2021). Nacionalna taksonomija računalno-sigurnosnih incidenata. Verzija 2.1. Dostupno na https://www.cert.hr/wp-content/uploads/2021/12/Nacionalna-taksonomija-racunalno-sigurnosnih-incidenata.pdf, pristupljeno [2.5.2023.].

77) Chambers, J. R., & Windschitl, P. D. (2004). Biases in social comparative judgments: The role of nonmotivated factors in above-average and comparative-optimism effects. *Psychological Bulletin*, *130*(5), 813–838.

78) Chaudhry, P. E., Chaudhry, S. S., Reese, R., & Jones, D. S. (2012). Enterprise information systems security: A conceptual framework. U: *Re-conceptualizing Enterprise Information Systems: 5th IFIP WG 8.9 Working Conference, CONFENIS 2011, Aalborg, Denmark, Revised Selected Papers*. Springer Berlin Heidelberg, 118-128. Dostupno na: https://link.springer.com/chapter/10.1007/978-3-642-28827-2_9, pristupljeno [1.8.2023.].

79) Chen, C., Ishfaq, M., Ashraf, F., Sarfaraz, A., & Wang, K. (2022a). Mediating Role of Optimism Bias and Risk Perception Between Emotional Intelligence and Decision-Making: A Serial Mediation Model. *Frontiers in Psychology*, *13*, 914649.

80) Chen, H., & Li, W. (2017). Mobile device users' privacy security assurance behavior: A technology threat avoidance perspective. *Information & Computer Security*, *25*(3), 330-344.

81) Chen, H., Turel, O., & Yuan, Y. (2021), E-waste information security protection motivation: the role of optimism bias, *Information Technology & People*, *35*(2), 600-620.

82) Chen, L., Xie, Z., Zhen, J., & Dong, K. (2022b). The Impact of Challenge Information Security Stress on Information Security Policy Compliance: The Mediating Roles of Emotions. *Psychology Research and Behavior Management*, *15,* 1177-1191.

83) Chen, P. Y., Kataria, G., & Krishnan, R. (2011). Correlated failures, diversification, and information security risk management. *MIS quarterly*, *35*(2), 397-422.

84) Chen, W., Goh, M., & Zou, Y. (2018). Logistics provider selection for omni-channel environment with fuzzy axiomatic design and extended regret theory. *Applied Soft Computing*, *71*, 353-363.

85) Cho, H., Lee, J. S., & Chung, S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior*, *26*(5), 987-995.

86) Cohen, J. (2013). *Statistical power analysis for the behavioral sciences*. Academic press.

87) Connelly, B. L., & Shi, W. (2022). Threats and responses in organizational research. *Journal of management*, *48*(6), 1366-1381.

88) Corradini, I. (2020). *Building a cybersecurity culture in organizations: How to bridge the gap between people and digital technology*. Springer Nature.

89) COSO. (Committee of Sponsoring Organizations of the Treadway Commission). (2009). Strengthening Enterprise Risk Management for Strategic Advantage. Dostupno na: https://us.aicpa.org/content/dam/aicpa/forthepublic/auditcommitteeeffectiveness/auditcommitteebrief/downloadabledocuments/strengthening-enterprise-risk.pdf, pristupljeno [20.11.2023.].

90) Costa-Font, J., Mossialos, E., & Rudisill, C. (2009). Optimism and the perceptions of new risks. *Journal of risk research*, *12*(1), 27-41.

91) Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology innovation management review*, *4*(10), 13-21.

92) Cram, W. A., D'arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly*, *43*(2), 525-554.

93) Creese, S., Saunders, J., Axon, L., & Dixon, W. (2020). Future Series: Cybersecurity, emerging technology and systemic risk. In *World Economic Forum*. Dostupno na: https://www3.weforum.org/docs/WEF_Future_Series_Cybersecurity_emerging_technology_and_systemic_risk_2020.pdf, pristupljeno [20.11.2023.].

94) CRO Forum. (2016). Concept Paper on a Proposed Categorisation Methodology for Cyber Risk. Dostupno na: https://www.thecroforum.org/wp-content/uploads/2016/06/ZRH-16-09033-P1_CRO_Forum_Cyber-Risk_web.pdf, pristupljeno [11.7.2020.].

95) Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *computers & security*, *32*, 90-101.

96) Crossler, R., & Bélanger, F. (2014). An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (USP) instrument. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *45*(4), 51-71.

97) Ćurak, M. (2019). Kibernetički rizici iz perspektive osiguranja. U: Rimac Smiljanić, A., Šimić Šarić, M. & Visković Josip (ur.) *Financijska kretanja - najnoviji događaji i perspektive*. Split, Sveučilište u Splitu, Ekonomski fakultet Split, 351-376.

98) Cycyota, C. S., & Harrison, D. A. (2002). Enhancing survey response rates at the executive level: Are employee-or consumer-level techniques effective?. *Journal of Management*, *28*(2), 151-176.

99) D'Arcy, J., & Teh, P. L. (2019). Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization. *Information & Management*, *56*(7), 103151.

100) Dane, E., & Pratt, M. G. (2007). Exploring intuition and its role in managerial decision making. *Academy of management review*, *32*(1), 33-54.

101) Das, S., Mukhopadhyay, A., & Anand, M. (2012). Stock market response to information security breach: A study using firm and attack characteristics. *Journal of Information Privacy and Security*, *8*(4), 27-55.

102) Das, T. K., & Teng, B. S. (1999). Cognitive biases and strategic decision processes: An integrative perspective. *Journal of management studies*, *36*(6), 757-778.

103) Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, *13*(3), 319-340.

104) Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management science*, *35*(8), 982-1003.

105) De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2022). What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. *Behaviour & Information Technology*, *41*(8), 1796-1808.

106) De Smidt, G., & Botzen, W. (2018). Perceptions of corporate cyber risks and insurance decision-making. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *43*(2), 239-274.

107) De Vaus, D. (2013). *Surveys in social research*. 6.izd. Routledge.

108) Deligonul, Z. S., Hult, G. T. M., & Cavusgil, S. T. (2008). Entrepreneuring as a puzzle: an attempt to its explanation with truncation of subjective probability distribution of prospects. *Strategic Entrepreneurship Journal*, *2*(2), 155-167.

109) DellaVigna, S. (2009). Psychology and economics: Evidence from the field. *Journal of Economic literature*, *47*(2), 315-372.

110) Deloitte. (2016). Cyber risk management challenges and solutions. The Deloitte Center for Financial Service. Dostupno na: https://www2.deloitte.com/content/dam/insights/us/multimedia/cyber-risk-management-financial-services-industry/DUP_3413_CyberInFSI_Infographic.pdf, pristupljeno [20.11.2023.].

111) Deloitte. (2023). 2023 Global Future of Cyber Survey. Dostupno na: https://www.deloitte.com/global/en/services/risk-advisory/content/future-of-cyber.html, pristupljeno [20.11.2023.].

112) Dhami, S., & al-Nowaihi, A. (2012). Behavioural Economics. U: *Encyclopedia of Human Behaviour*, 2.izd., Elsevier, *13*, 288-300. Dostupno na: https://figshare.le.ac.uk/articles/chapter/Behavioural_Economics/10175594, pristupljeno [15.11.2023.].

113) Dodel, M., & Mesch, G. (2019). An integrated model for assessing cyber-safety behaviors: How cognitive, socioeconomic and digital determinants affect diverse safety practices. *Computers & Security*, *86*, 75-91.

114) Doerr, S., Gambacorta, L., Leach, T., Legros, B., & Whyte, D. (2022). Cyber risk in central banking (BIS Working Papers No 1039), Bank for International Settlements

Monetary and Economic Department. Dostupno na: https://www.bis.org/publ/work1039.htm, pristupljeno [1.12.2022.]

115) Dong, L. (2008). Exploring the impact of top management support of enterprise systems implementations outcomes: Two cases. *Business Process Management Journal*, *14*(2), 204-218.

116) Dostupno na: https://onlinelibrary.wiley.com/doi/abs/10.1002/9781118445112.stat03762, pristupljeno [20.11.2023.].

117) Egelman, S., Sotirakopoulos, A., Muslukhov, I., Beznosov, K., & Herley, C. (2013). Does my password go up to eleven? The impact of password meters on password selection. U: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2379-2388. Dostupno na: https://dl.acm.org/doi/abs/10.1145/2470654.2481329, pristupljeno [1.8.2023.].

118) Eling, M. (2018). Cyber Risk and Cyber Risk Insurance: Status Quo and Future Research. The Geneva Papers on Risk and Insurance - Issues and Practice, *43*(2), 175–179.

119) Eling, M. (2020). Cyber risk research in business and actuarial science. *European Actuarial Journal*, *10*(2), 303-333.

120) Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance?. *The Journal of Risk Finance*, *17*(5), 474-491.

121) Eling, M., McShane, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, *24*(1), 93-125.

122) ENISA. (2012) Incentives and barriers of the cyber insurance market in Europe. Dostupno na: https://www.enisa.europa.eu/publications/incentives-and-barriers-of-the-cyber-insurance-market-in-europe, pristupljeno [15.9.2020.].

123) Enterprise Strategy Group. (2020). Cybersecurity in the C-suite and Boardroom. Dostupno na: https://www.bitsight.com/resources/cybersecurity-in-the-c-suite-and-boardroom, pristupljeno [2.5.2023.].

124) Eppler, M., & Muntwiler, C. (2021). BIASMAP–developing a visual typology and interface to explore and understand decision-making errors in management. U: *Human Interaction, Emerging Technologies and Future Applications IV: Proceedings of the 4th International Conference on Human Interaction and Emerging Technologies: Future*

Applications (IHIET–AI 2021), Strasbourg, France. Springer International Publishing, 670-677. Dostupno na: https://link.springer.com/chapter/10.1007/978-3-030-74009-2_85, pristupljeno [1.8.2023.].

125) Ernst & Young, Institute of Internal Auditors. (2021). *The risky six. Key questions to expose gaps in board understanding of organisational cyber resiliency*. Dostupno na: https://global.theiia.org/knowledge/Public%20Documents/EY-The-Risky-Six-Board-Disconnections.pdf, pristupljeno [30.1.2023.].

126) Ernst & Young. (2018). Is Cybersecurity about More than Protection? EY Global Information Security Survey 2018-2019. Dostupno na: https://assets.ey.com/content/dam/ey-sites/ey-com/en_ca/topics/advisory/ey-global-information-security-survey-2018-19.pdf, pristupljeno [1.9.2022.].

127) Ernst & Young. (2021). Cybersecurity: How do you rise above the waves of a perfect storm?. Dostupno na: https://assets.ey.com/content/dam/ey-sites/ey-com/es_cl/webcast/2021/09/ey-chile-global-information-security-survey-2021.pdf, pristupljeno [30.1.2023.].

128) European Union Law. (2016). Direktiva o sigurnosti mrežnih i informacijskih sustava. Europski parlament i Vijeće Europske Unije - Direktiva (EU) 2016/1148., Službeni List Europske Unije, 194, 1-30. Dostupno na: https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A32016L1148, pristupljeno [20.11.2023.].

129) European Union Law. (2016). Opća uredba o zaštiti podataka - Uredba (EU) 2016/679. Europski parlament i Vijeće Europske Unije, Službeni List Europske Unije, 119, 1-88. Dostupno na: https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32016R0679, pristupljeno [20.11.2023.].

130) European Union Law. (2019). Akt o kibersigurnosti - Direktiva (EU) 2019/881. Europski parlament i Vijeće Europske Unije, 151, 15-69. Dostupno na: https://eur-lex.europa.eu/legal-content/hr/ALL/?uri=CELEX%3A32019R0881, pristupljeno [20.11.2023.].

131) European Union Law. (2022). Europski akt o upravljanju podacima (2022/868). Europski parlament i Vijeće Europske Unije, 152, 1-44. Dostupno na: https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A52020PC0767, pristupljeno [20.11.2023.].

132) Europska komisija. (2023a). NIS2 Directive. Europska komisija. Dostupno na: https://digital-strategy.ec.europa.eu/en/node/10361/printable/pdf, pristupljeno [20.11.2023.].

133) Europska komisija. (2023b). Europski akt o upravljanju podacima. Europska komisija. Dostupno na: https://digital-strategy.ec.europa.eu/hr/policies/data-governance-act, pristupljeno [20.11.2023.].

134) Evans, J. S. B. (2003). In two minds: dual-process accounts of reasoning. *Trends in cognitive sciences*, *7*(10), 454-459.

135) Farshadkhah, S., Van Slyke, C., & Fuller, B. (2021). Onlooker effect and affective responses in information security violation mitigation. *Computers & Security*, *100*, 102082.

136) Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk management. *Information Management & Computer Security*, *22*(5), 410-430.

137) Financial Stability Board. (2023, April 13). Cyber Lexicon. Dostupno na: https://www.fsb.org/wp-content/uploads/P130423-3.pdf, pristupljeno [20.11.2023.].

138) Fininfo (2023). Fininfo baza podtaka. Dostupno na: https://www.fininfo.hr/, pristupljeno [11.4.2023.].

139) Fishbein, M., & Ajzen, I. (2011). *Predicting and changing behavior: The reasoned action approach*. Taylor & Francis.

140) Fishburn, P. C. 1982. Non-transitive measurable utility. *Journal of Mathematical Psychology, 26*(1), 31-67.

141) Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of applied social psychology*, *30*(2), 407-429.

142) Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research*, *18*(1), 39-50.

143) Fredrickson, B. L. (2001). The role of positive emotions in positive psychology: The broaden-and-build theory of positive emotions. *American psychologist*, *56*(3), 218-226.

144) Fullbrook, E. (2003). *The Crisis in Economics*. Routledge.

145) Furnell, S., & Thomson, K. L. (2009). Recognising and addressing 'security fatigue'. *Computer Fraud & Security*, *2009*(11), 7-11.

146) Gale, M., Bongiovanni, I., & Slapnicar, S. (2022). Governing cybersecurity from the boardroom: challenges, drivers, and ways ahead. *Computers & Security*, *121*, 102840.

147) Gassen, J., Nowak, T. J., Henderson, A. D., Weaver, S. P., Baker, E. J., & Muehlenbein, M. P. (2021). Unrealistic optimism and risk for COVID-19 disease. *Frontiers in psychology*, *12*, 647461.

148) Gatzert, N., & Martin, M. (2015). Determinants and value of enterprise risk management: Empirical evidence from the literature. *Risk Management and Insurance Review*, *18*(1), 29-53.

149) Gatzlaff, K. M., & McCullough, K. A. (2010). The effect of data breaches on shareholder wealth. *Risk Management and Insurance Review*, *13*(1), 61-83.

150) Gellman, M. D., Turner, J. R. (2013). *Encyclopedia of behavioral medicine*. Springer New York.

151) George, D., & Mallery, P. (2019). *IBM SPSS statistics 26 step by step: A simple guide and reference*. Routledge.

152) Gill, M., & VanBoskirk, S. (2016). The digital maturity model 4.0. Benchmarks: digital transformation playbook. Dostupno na: http://forrester.nitro-digital.com/pdf/Forrester-s%20Digital%20Maturity%20Model%204.0.pdf, pristupljeno [1.8.2023.].

153) Gomez, M. A., & Villar, E. B. (2018). Fear, uncertainty, and dread: Cognitive heuristics and cyber threats. *Politics and Governance*, *6*(2), 61-72.

154) Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM*, *46*(3), 81-85.

155) Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs?. *Journal of Computer Security*, *19*(1), 33-56.

156) Gordon, L. A., Loeb, M. P., & Zhou, L. (2015). The impact of information sharing on cybersecurity underinvestment: A real options perspective. Journal of Accounting and Public Policy, *34*(5), 509-519.

157) Gouveia, S. O., & Clarke, V. (2001). Optimistic bias for negative and positive events. *Health Education*, *101*(5), 228-234.

158) Grace, M. F., Leverty, J. T., Phillips, R. D., & Shimpi, P. (2015). The value of investing in enterprise risk management. *Journal of Risk and Insurance*, *82*(2), 289-316.

159) Gradinaru, A. (2014). The contribution of behavioral economics in explaining the decisional process. *Procedia Economics and Finance*, *16*, 417-426.

160) Greitzer, F. L., & Hohimer, R. E. (2011). Modeling human behavior to anticipate insider attacks. *Journal of Strategic Security*, *4*(2), 25-48.

161) Grewal, N.S., Sparks, J.A., Reiter, J., Moses, E. (2016). Behavioral Economics. U: *Encyclopedia of Mental Health, 2 izd.,* 143-149. Dostupno na: https://doi.org/10.1016/B978-0-12-397045-9.00201-9, pristupljeno [15.11.2023.].

162) Guhr, N., Lebek, B., & Breitner, M. H. (2018). The impact of leadership on employees' intended information security behaviour: An examination of the full-range leadership theory. *Information Systems Journal*, *29*(2), 340-362.

163) Gulenko, I. (2014). Improving passwords: Influence of emotions on security behaviour. *Information Management & Computer Security*, *22*(2), 167-178.

164) Haag, S., Siponen, M., & Liu, F. (2021). Protection motivation theory in information systems security research: A review of the past and a road map for the future. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *52*(2), 25-67.

165) Hadlington, L. J. (2018). Employees' attitudes towards cyber security and risky online behaviours: An empirical assessment in the United Kingdom. *International Journal of Cyber Criminology*, *12*, 262–277.

166) Hagen, J. M., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*, *16*(4), 377-397.

167) Hair Jr, J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., Danks, N. P., & Ray, S. (2021). *Partial least squares structural equation modeling (PLS-SEM) using R: A workbook*. Springer Nature.

168) Hair Jr, J. F., Matthews, L. M., Matthews, R. L., & Sarstedt, M. (2017b). PLS-SEM or CB-SEM: updated guidelines on which method to use. *International Journal of Multivariate Data Analysis*, *1*(2), 107-123.

169) Hair Jr, J. F., Sarstedt, M., Hopkins, L., & Kuppelwieser, V. G. (2014). Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. *European business review*, *26*(2), 106-121.

170) Hair, J. F., Black, W. C., Babin, B. J. i Anderson, R. E. (2010). *Multivariate Data Analysis.* 7.izd. New York: Pearson.

171) Hair, J. F., Hult, G. T. M., Ringle, C. M. and Sarstedt, M. (2017a). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. 2.izd. Sage Publications.

172) Hair, J. F., Risher, J. J., Sarstedt, M. i Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2-24.

173) Hair, J. F., Sarstedt, M., Pieper, T. M., & Ringle, C. M. (2012). The use of partial least squares structural equation modeling in strategic management research: a review of past

practices and recommendations for future applications. *Long range planning*, *45*(5-6), 320-340.

174) Hakami, M., & Alshaikh, M. (2022). Identifying Strategies to Address Human Cybersecurity Behavior: A Review Study. *International Journal of Computer Science & Network Security*, *22*(4), 299-309.

175) Haltinner, K., Sarathchandra, D., & Lichtenberg, N. (2016). Can I Live? College Student Perceptions of Risks, Security, and Privacy in Online Spaces. U: *Cyber Security: Second International Symposium, CSS 2015, Coeur d'Alene, ID, Revised Selected Papers 2*. Springer International Publishing, 69-81. Dostupno na: https://link.springer.com/chapter/10.1007/978-3-319-28313-5_6, pristupljeno [3.8.2023.].

176) Hammond, J. S., Keeney, R. L., & Raiffa, H. (1998). The hidden traps in decision making. *Harvard business review*, *76*(5), 47-58.

177) Hanus, B., Windsor, J. C., & Wu, Y. (2018). Definition and multidimensionality of security awareness: Close encounters of the second order. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *49*(SI), 103-133.

178) Harrington, S. E., Niehaus, G. (2004). Risk management and insurance. 2.izd., McGraw-Hill/Irwin.

179) Haselton, M. G., Nettle, D., & Andrews, P. W. (2015). The evolution of cognitive bias. U: Buss, D. M. (ur.) *The handbook of evolutionary psychology*, Wiley, 724-746.

180) Haynes, S. N., Richard, D., & Kubany, E. S. (1995). Content validity in psychological assessment: A functional approach to concepts and methods. *Psychological assessment*, *7*(3), 238–247.

181) Heal, G., Kearns M., Kleindorfer, P. & Kunreuther, H. (2006) Interdependent Security in Interconnected networks. Dostupno na: http://opim.wharton.upenn.edu/risk/IDS/Papers/Heal_et_al_2006.pdf, pristupljeno [20.9.2020.].

182) Heidt, M., Olt, C. M., & Buxmann, P. (2019). To (psychologically) own data is to protect data: How psychological ownership determines protective behavior in a work and private context, 14th International Conference on Wirtschaftsinformatik, Siegen, German. Dostupno na: https://aisel.aisnet.org/wi2019/track11/papers/2/, pristupljeno [15.10.2022.].

183) Heilbroner, R. L., & Milberg, W. S. (1996). *The crisis of vision in modern economic thought*. Cambridge University Press.

184) Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the academy of marketing science*, *43*, 115-135.

185) Herath, H. S., & Herath, T. C. (2011). Copula-based actuarial model for pricing cyber-insurance policies. *Insurance Markets and Companies*, *2*(1), 7-20.

186) Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154-165.

187) Hewitt, B., & White, G. L. (2020). Optimistic bias and exposure affect security incidents on home computer. *Journal of Computer Information Systems*, *62*(1), 50-60.

188) Hina, S., Selvam, D. D. D. P., & Lowry, P. B. (2019). Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. *Computers & Security*, *87*, 101594.

189) Hodgkinson, G. P., & Clarke, I. (2007). Conceptual note: Exploring the cognitive significance of organizational strategizing: A dual-process framework and research agenda. *Human Relations*, *60*(1), 243-255.

190) Hodgkinson, G. P., Bown, N. J., Maule, A. J., Glaister, K. W., & Pearman, A. D. (1999). Breaking the frame: An analysis of strategic cognition and decision making under uncertainty. *Strategic management journal*, *20*(10), 977-985.

191) Hofmann, A., & Ramaj, H. (2011). Interdependent risk networks: the threat of cyber attack. *International Journal of Management and Decision Making*, *11*(5-6), 312-323.

192) Hogan, M. D., & Newton, E. M. (2015). Supplemental Information for the Interagency Report on Strategic US Government Engagement in International Standardization to Achieve US Objectives for Cybersecurity. Dostupno na: https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v2.pdf , pristupljeno [15.5.2023.].

193) Høiland, C. (2003). "Not My Responsibility!": A Comparative Case Study of Organizational Cybersecurity Subcultures. Master's thesis: University of Agder, Faculty of Social Sciences, Department of Information Systems. Dostupno na: https://uia.brage.unit.no/uia-

xmlui/bitstream/handle/11250/3080485/no.uia:inspera:143804570:36996920.pdf?sequence=1, pristupljeno [1.10.2023.].

194) Hong, Y., & Furnell, S. (2021). Understanding cybersecurity behavioral habits: Insights from situational support. *Journal of Information Security and Applications*, *57*, 102710.

195) Hooper, V., & Blunt, C. (2019). Factors influencing the information security behaviour of IT employees. *Behaviour & Information Technology*, *39*(8), 862-874.

196) Hoppe, F., Gatzert, N., & Gruner, P. (2021). Cyber risk management in SMEs: insights from industry surveys, *The Journal of Risk Finance. 22*(3/4), 240-260.

197) Hoskisson, R. E., Chirico, F., Zyung, J., & Gambeta, E. (2017). Managerial risk taking: A multitheoretical review and future research agenda. *Journal of management*, *43*(1), 137-169.

198) Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea. *Information & Management*, *49*(2), 99-110.

199) Hovav, A., & D'Arcy, J. (2003). The impact of denial-of-service attack announcements on the market value of firms. *Risk Management and Insurance Review*, *6*(2), 97-121.

200) Hoyt, R. E., & Liebenberg, A. P. (2011). The value of enterprise risk management. *Journal of risk and insurance*, *78*(4), 795-822.

201) Hoyt, R. E., & Liebenberg, A. P. (2015). Evidence of the value of enterprise risk management. *Journal of Applied Corporate Finance*, *27*(1), 41-47.

202) Hrvatska agencija za nadzor financijskih usluga. (2021). Obavijesti subjektima nadzora. Rješenje izdano prema društvu Zagrebačka burza d.d., dostupno na: https://www.hanfa.hr/media/5678/5-zagreba%C4%8Dka-burza.pdf [15.6.2021.].

203) Hrvatska gospodarska komora. (2023). Digitalna komora. dostupno na: https://digitalnakomora.hr/home, pristupljeno [11.4.2023.].

204) Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. Decision Sciences, *43*(4), 615-660.

205) Huy, Q. N. (1999). Emotional capability, emotional intelligence, and radical change. *Academy of Management review*, *24*(2), 325-345.

206) Hwang, I., Kim, D., Kim, T., & Kim, S. (2017). Why not comply with information security? An empirical approach for the causes of non-compliance. *Online Information Review*, *41*(1), 2-18.

207) Hwang, I., Wakefield, R., Kim, S., & Kim, T. (2021). Security awareness: The first step in information security compliance behavior. *Journal of Computer Information Systems*, *61*(4), 345-356.

208) IBM (2023). What is cyber risk management?. International Business Machines Corporation Dostupno na: https://www.ibm.com/topics/cyber-risk-management, pristupljeno [20.11.2023.].

209) Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83-95.

210) Institute of Risk Management. (2014). Cyber Risk. National Association of Insurance Commissioners Dostupno na: https://content.naic.org/cipr_topics/topic_cybersecurity.htm, pristupljeno [20.6.2020.].

211) International Communication Union. (2008). Communications And Security - Overview of cybersecurity. Telecommunication. International Communication Union. Dostupno na: file:///C:/Users/Korisnik/Desktop/Downloads/T-REC-X.1205-200804-I!!PDF-E-1.pdf, pristupljeno [20.11.2023.].

212) International Organization for Standardization. (2009). *Risk management — Vocabulary (ISO Guide 73:2009). ISO*/IEC. Dostupno na: https://www.iso.org/standard/44651.html, pristupljeno [20.11.2023.].

213) International Organization for Standardization. (2018). *Information technology — Security techniques — Information security management systems — Overview and vocabulary* (ISO/IEC 27000:2018). *ISO*/IEC. Dostupno na: https://www.iso.org/standard/73906.html, pristupljeno [20.11.2023.].

214) International Organization for Standardization. (2018). *Risk management - Guidelines* (ISO 31000:2018). *ISO*/IEC. Dostupno na: https://www.iso.org/standard/65694.html, pristupljeno [20.11.2023.].

215) International Organization for Standardization. (2020). Information technology — Cybersecurity — Overview and concepts (ISO/IEC TS 27100:2020[en]). *ISO*/IEC. Dostupno na: https://www.iso.org/obp/ui/#iso:std:iso-iec:ts:27100:ed-1:v1:en, pristupljeno [20.11.2023.].

216) International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection - Guidance on managing information security*

risks (ISO/IEC 27005:2022). *ISO*/IEC. Dostupno na: https://www.iso.org/standard/80585.html, pristupljeno [20.11.2023.].

217) International Organization for Standardization. (2023). Cybersecurity - Guidelines for Internet security (ISO/IEC 27032:2023). *ISO*/IEC. Dostupno na: https://www.iso.org/standard/76070.html, pristupljeno [20.11.2023.].

218) Isen, A. M. (2001). An influence of positive affect on decision making in complex situations: Theoretical issues with practical implications. *Journal of consumer psychology*, *11*(2), 75-85.

219) Ismail, N., Kinchin, G., & Edwards, J. A. (2018). Pilot study, Does it really matter? Learning lessons from conducting a pilot study for a qualitative PhD thesis. *International Journal of Social Science Research*, *6*(1), 1-17.

220) Jalali, M. S., Siegel, M., & Madnick, S. (2019). Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. *The Journal of Strategic Information Systems*, *28*(1), 66-82.

221) Jefferson, A., Bortolotti, L., & Kuzmanovic, B. (2017). What is unrealistic optimism?. *Consciousness and cognition*, *50*, 3-11.

222) Johnson, D. D., Blumstein, D. T., Fowler, J. H., & Haselton, M. G. (2013). The evolution of error: Error management, cognitive constraints, and adaptive decision-making biases. *Trends in ecology & evolution*, *28*(8), 474-481.

223) Johnston, A. C., & Hale, R. (2009). Improved security through information security governance. *Communications of the ACM*, *52*(1), 126-129.

224) Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS quarterly*, *34*(3), 549-566.

225) Jones, C. M. (2009). *Utilizing the technology acceptance model to assess employee adoption of information systems security measures*. Nova Southeastern University.

226) Kadena, E., & Gupi, M. (2021). Human Factors in Cybersecurity: Risks and Impacts. *Security science journal*, *2*(2), 51-64.

227) Kahneman, D. (2011). *Thinking, fast and slow*. Farrar, Straus and Giroux.

228) Kahneman, D., & Frederick, S. (2002). Representativeness revisited: Attribute substitution in intuitive judgment. *Heuristics and biases: The psychology of intuitive judgment*, *49*(49-81), 74.

229) Kahneman, D., & Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk. *Econometrica, 47*(2), 263-292.

230) Kahneman, D., Lovallo, D., & Sibony, O. (2019). A structured approach to strategic decisions. *MIT Sloan Management Review*, 60(3): 67–73.

231) Kahneman, D., Slovic, P., & Tversky, A. (1982). *Judgment under uncertainty: Heuristics and biases*. Cambridge university press.

232) Kannelønning, K., & Katsikas, S. K. (2023). A systematic literature review of how cybersecurity-related behavior has been assessed. *Information & Computer Security*. *31*(4), 463-477.

233) Kapko, M. (2022). Cybersecurity spending on pace to surpass $260B by 2026. Cybersecurity Dive. Dostupno na: https://www.cybersecuritydive.com/news/security-spending-balloons/634365/ , pristupljeno [11.4.2023.].

234) Keil, M., Wallace, L., Turk, D., Dixon-Randall, G., & Nulden, U. (2000). An investigation of risk perception and risk propensity on the decision to continue a software development project. *Journal of Systems and Software*, *53*(2), 145-157.

235) Kendrick, R. (2010). *Cyber risks for business professionals: A management guide*. IT Governance Ltd.

236) Kianpour, M., Øverby, H., Kowalski, S. J., & Frantz, C. (2019). Social preferences in decision making under cybersecurity risks and uncertainties. U: *International Conference on Human-Computer Interaction*. Springer, Cham, 149-163. Dostupno na: https://link.springer.com/chapter/10.1007/978-3-030-22351-9_10, pristupljeno [1.8.2023.].

237) Kim, H. W., & Kankanhalli, A. (2009). Investigating user resistance to information systems implementation: A status quo bias perspective. *MIS quarterly*, *33*(3), 567-582.

238) Kleffner, A. E., Lee, R. B., & McGannon, B. (2003). The effect of corporate governance on the use of enterprise risk management: Evidence from Canada. *Risk Management and insurance review*, *6*(1), 53-73.

239) Klein, C. T., & Helweg-Larsen, M. (2002). Perceived control and the optimistic bias: A meta-analytic review. *Psychology and health*, *17*(4), 437-446.

240) Kline, R. B. (2015). *Principles and practice of structural equation modeling*. Guilford publications.

241) Knapp, K. J., Marshall, T. E., Rainer Jr, R. K., & Morrow, D. W. (2006). The top information security issues facing organizations: What can government do to help. *Network security*, *15(4)*, 51-58.

242) Kosub, T. (2015). Components and challenges of integrated cyber risk management. *Zeitschrift für die gesamte Versicherungswissenschaft*, *104*, 615-634.

243) Kovač, D. (2021). Ulaganje u kibernetičku sigurnost. *Zbornik radova Veleučilišta u Šibeniku*, *15*(1-2), 61-73.

244) Krause, T. A., & Tse, Y. (2016). Risk management and firm value: recent theory and evidence. *International Journal of Accounting and information management*, *24*(1), 56-81.

245) Kudryavtsev, A., Cohen, G., & Hon-Snir, S. (2013). 'Rational'or'Intuitive': Are behavioral biases correlated across stock market investors?. *Contemporary economics*, *7*(2), 31-53.

246) Kure, H. I., Islam, S., & Razzaque, M. A. (2018). An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences*, *8*(6), 898.

247) Lachowicz, M. J., Preacher, K. J., & Kelley, K. (2018). A novel measure of effect size for mediation analysis. *Psychological Methods*, *23*(2), 244.

248) Lam, L. W. (2012). Impact of competitiveness on salespeople's commitment and performance. *Journal of Business Research*, *65*(9), 1328-1334.

249) Landman, J. (1993). *Regret: The persistence of the possible*. Oxford University Press.

250) Langer, E. J., & Roth, J. (1975). Heads I win, tails it's chance: The illusion of control as a function of the sequence of outcomes in a purely chance task. *Journal of personality and social psychology*, *32*(6), 951-955.

251) Lanz, J. (2018). Enterprise Technology Risk in a New COSO ERM World: Eight Challenges Facing Management. *The CPA Journal*, *88*(6), 6-10.

252) Larrick, R. P., & Boles, T. L. (1995). Avoiding regret in decisions with feedback: A negotiation example. *Organizational Behavior and Human Decision Processes*, *63*(1), 87-97.

253) Larsen, M. H., & Lund, M. S. (2021). Cyber risk perception in the maritime domain: a systematic literature review. *IEEE Access*, *9*, 144895-144905.

254) Lawrence, J., Quade, D., & Becker, J. (2014). Integrating the effects of flood experience on risk perception with responses to changing climate risk. *Natural Hazards*, *74*, 1773-1794.

255) Lawshe, C. H. (1975). A quantitative approach to content validity. *Personnel psychology*, *28*(4), 563-575.

256) Lazuras, L., Barkoukis, V., Mallia, L., Lucidi, F., & Brand, R. (2017). More than a feeling: The role of anticipated regret in predicting doping intentions in adolescent athletes. *Psychology of Sport and Exercise*, *30*, 196-204.

257) Lebek, B., Uffen, J., Neumann, M., Hohler, B., & H. Breitner, M. (2014). Information security awareness and behavior: a theory-based literature review. *Management Research Review*, *37*(12), 1049-1092.

258) Lechner, P., & Gatzert, N. (2018). Determinants and value of enterprise risk management: empirical evidence from Germany. *The European Journal of Finance*, *24*(10), 867-887.

259) Lechowska, E. (2018). What determines flood risk perception? A review of factors of flood risk perception and relations between its basic elements. *Natural Hazards*, *94*(3), 1341-1366.

260) Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, *18*(2), 177-187.

261) Lei, W., Hu, S., & Hsu, C. (2023). Unveiling the process of phishing precautions taking: The moderating role of optimism bias. *Computers & Security*, *129*, 103249.

262) Lerner, J. S., & Keltner, D. (2001). Fear, anger, and risk. *Journal of personality and social psychology*, *81*(1), 146-159.

263) Lerner, J. S., Li, Y., Valdesolo, P., & Kassam, K. S. (2015). Emotion and decision making. *Annual review of psychology*, *66*, 799-823.

264) Lewis, B. R., Snyder, C. A., & Rainer Jr, R. K. (1995). An empirical assessment of the information resource management construct. *Journal of Management Information Systems*, *12*(1), 199-223.

265) Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13-24.

266) Li, S., Zhou, K., Sun, Y., Rao, L. L., Zheng, R., & Liang, Z. Y. (2009). Anticipated regret, risk perception, or both: which is most likely responsible for our intention to gamble?. *Journal of Gambling Studies*, *26*, 105-116.

267) Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS quarterly*, *33*(1), 71-90.

268) Liang, H., & Xue, Y. L. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the association for information systems*, *11*(7), 394-413.

269) Lin, X. (2019). Feeling is believing? Evidence from earthquake shaking experience and insurance demand. *Journal of Risk and Insurance*, *87*(2), 351-380.

270) Liu, C., Wang, N., & Liang, H. (2020). Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment. *International Journal of Information Management*, *54*, 102152.

271) Loebbecke, C., & Picot, A. (2015). Reflections on societal and business model transformation arising from digitization and big data analytics: A research agenda. *The Journal of Strategic Information Systems*, *24*(3), 149-157.

272) Loewenstein, G. (2004). Emotions in economics. *New England Economic Review*, *1*, 17-18.

273) Loewenstein, G. F., Weber, E. U., Hsee, C. K., & Welch, N. (2001). Risk as feelings. *Psychological bulletin*, *127*(2), 267.

274) Loewenstein, G., & Lerner, J. S. (2003). The role of affect in decision making. U: R. J. Davidson, K. R. Scherer, & H. H. Goldsmith (ur.), *Handbook of affective sciences*. Oxford University Press, 619–642.

275) Loomes, G., & Sugden, R. (1982). Regret theory: An alternative theory of rational choice under uncertainty. *The economic journal*, *92*(368), 805-824.

276) Lovallo, D., & Sibony, O. (2010). The case for behavioral strategy. *McKinsey Quarterly*, Dostupno na: http://dln.jaipuria.ac.in:8080/jspui/bitstream/123456789/2496/1/The%20case%20for%20behavioral%20strategy.pdf, pristupljeno [20.11.2023.].

277) Lowry, P. B., Moody, G. D., Parameswaran, S., & Brown, N. (2023). Examining the Differential Effectiveness of Fear Appeals in Information Security Management Using Two-Stage Meta-Analysis. *Journal of Management Information Systems (JMIS)*. Dostupno na: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4416590, pristupljeno [17.7.2023.].

278) Lu, Y. (2018). Cybersecurity research: A review of current research topics. *Journal of Industrial Integration and Management*, *3*(04), 1850014.

279) M. Mejovšek (2008). *Metode znanstvenog istraživanja u društvenim i humanističkim znanostima*. Naklada Slap.

280) Ma, Q., Schmidt, M. B., & Pearson, J. M. (2009). An Integrated Framework for Information Security Management. *Review of Business*, *30*(1), 58-69.

281) Ma, X. (2022). IS professionals' information security behaviors in Chinese IT organizations for information security protection. *Information Processing & Management*, *59*(1), 102744.

282) Ma, X., Kim, S. H., & Kim, S. S. (2014). Online gambling behavior: The impacts of cumulative outcomes, recent outcomes, and prior use. *Information Systems Research*, *25*(3), 511-527.

283) Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity*, *3*(1), 1-18.

284) Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of experimental social psychology*, *19*(5), 469-479.

285) Măirean, C., Havârneanu, G. M., Barić, D., & Havârneanu, C. (2021). Cognitive biases, risk perception, and risky driving behaviour. *Sustainability*, *14*(1), 77.

286) Malhotra, A., & Kubowicz Malhotra, C. (2011). Evaluating customer information breaches as service failures: An event study approach. *Journal of Service Research*, *14*(1), 44-59.

287) Malmendier, U., & Tate, G. (2005). Does overconfidence affect corporate investment? CEO overconfidence measures revisited. *European financial management*, *11*(5), 649-659.

288) March, J. G., & Shapira, Z. (1987). Managerial perspectives on risk and risk taking. Management science, *33*(11), 1404-1418.

289) Marotta, A., & McShane, M. (2018). Integrating a proactive technique into a holistic cyber risk management approach. *Risk Management and Insurance Review*, *21*(3), 435-452.

290) Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). Cyber-insurance survey. *Computer Science Review*, *24*, 35-61.

291) Marsh. (2019). 2019 Global Cyber Risk Perception Survey Dostupno na: https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf, pristupljeno [1.9.2022.].

292) Marshall, J. A., Trimmer, P. C., Houston, A. I., & McNamara, J. M. (2013). On evolutionary explanations of cognitive biases. *Trends in ecology & evolution*, *28*(8), 469-473.

293) Maule, A. J., Hockey, G. R. J., & Bdzola, L. (2000). Effects of time-pressure on decision-making under uncertainty: changes in affective state and information processing strategy. *Acta psychologica*, *104*(3), 283-301.

294) McMath, B. F., & Prentice-Dunn, S. (2005). Protection motivation theory and skin cancer risk: The role of individual differences in responses to persuasive appeals. *Journal of Applied Social Psychology*, *35*(3), 621-643.

295) McShane, M. (2018). Enterprise risk management: history and a design science proposal. *The Journal of Risk Finance*, *19*(2), 137-153.

296) McShane, M. K., Nair, A., & Rustambekov, E. (2011). Does enterprise risk management increase firm value?. *Journal of Accounting, Auditing & Finance*, *26*(4), 641-658.

297) McShane, M., & Nguyen, T. (2020). Time-varying effects of cyberattacks on firm value. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *45*, 580-615.

298) Mellers, B. A., Schwartz, A., Ho, K., & Ritov, I. (1997). Decision affect theory: Emotional reactions to the outcomes of risky options. *Psychological Science*, *8*(6), 423-429.

299) Menard, P., Bott, G. J., & Crossler, R. E. (2017). User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems*, *34*(4), 1203-1230.

300) Miloš Sprčić, D., Kožul, A., & Pecina, E. (2017). Managers' support–a key driver behind enterprise risk management maturity. *Zagreb international review of economics & business*, *20*(SCI), 25-39.

301) Mintzberg, H. (1973). *The nature of managerial work*. Prentice-Hall.

302) Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS quarterly*, *42*(1), 285-311.

303) Morgan, M. G. (2001). *Risk communication: A mental models approach*. Cambridge University Press.

304) Morgan, S. (2022). Cybercrime To Cost The World 8 Trillion Annually In 2023. Cybercrime Magazine, Dostupno na: https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/, pristupljeno [17.7.2023.].

305) Morrison, T. G., Morrison, M. A., & McCutcheon, J. M. (2017). Best practice recommendations for using structural equation modelling in psychological research. *Psychology*, 8(09), 1326-1341.

306) Morse, E. A., Raval, V., & Wingender Jr, J. R. (2011). Market price effects of data security breaches. *Information Security Journal: A Global Perspective*, *20*(6), 263-273.

307) Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure IT or not?. *Decision Support Systems*, *56*, 11-26.

308) Mukhopadhyay, A., Saha, D., Chakrabarti, B. B., Mahanti, A., & Podder, A. (2005). Insurance for cyber-risk: A Utility Model. *Decision*, *32*(1), 153-169.

309) Mullainathan, S., & Thaler, R. H. (2001). Behavioral Economics. In N. J. Smelser & P. B. Baltes (ur.), *International Encyclopedia of the Social and Behavioral Sciences*. Elsevier Science Ltd.

310) Narodne novine. (2018). Zakon o provedbi Opće uredbe o zaštiti podataka NN 42/2018. Hrvatski sabor, 805, 1-2. Dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html, pristupljeno [20.11.2023.].

311) Narodne novine. (2018). Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga NN 68/2018. Vlada Republike Hrvatske, 1399, 1-82. Dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/2018_07_68_1399.html, pristupljeno [20.11.2023.].

312) Narodne novine. (2018). Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga NN 64/2018. Hrvatski sabor, 1305, 1-37. Dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/2018_07_64_1305.html, pristupljeno [20.11.2023.].

313) Narodne novine. (2022). Odluka o primjerenom upravljanju informacijskim sustavom, NN 110/2022. Hrvatska narodna banka. 1629, 1-103. Dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/2022_09_110_1629.html, pristupljeno [20.11.2023.].

314) Narodne novine. (2022). Zakon o provedbi kibernetičke sigurnosne certifikacije NN 63/2022. Hrvatski sabor, 908, 1-16. Dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/full/2022_06_63_908.html, pristupljeno [20.11.2023.].

315) National Association of Insurance Commissioners. (2018). Cybersecurity Risk Management, *National Association of Insurance Commissioners* (NAIC). Dostupno na: https://content.naic.org/cipr-topics/cybersecurity, pristupljeno [1.9.2023.].

316) National Institute of Standards and Technology. (2006). Minimum security requirements for federal information and information systems, Federal Information Processing Standards Publication FIPS PUB 200, *National Institute of Standards and Technology (NIST)*, Gaithersburg, MD. Dostupno na: https://csrc.nist.gov/pubs/fips/200/final, pristupljeno [1.9.2023.].

317) National Institute of Standards and Technology. (2023). Cyberspace. National Institute of Standards and Technology. Dostupno na: https://csrc.nist.gov/glossary/term/cyberspace pristupljeno [20.11.2023.].

318) Nehme, A., Warkentin, M., Jang, K., & Kim, S. (2022). Beyond Rational Information Security Decisions: An Alternate View", *AMCIS 2022, Proceedings*. 26, Dostupno na: https://aisel.aisnet.org/amcis2022/sig_sec/sig_sec/26, pristupljeno [20.10.2022.].

319) Nieuwesteeg, B., Visscher, L., & de Waard, B. (2018). The law and economics of cyber insurance contracts: a case study. *European Review of Private Law*, *26*(3), 371 – 420.

320) Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. *HOLISTICA–Journal of Business and Public Administration*, *9*(3), 71-88.

321) Nocco, B. W., & Stulz, R. M. (2006). Enterprise risk management: Theory and practice. *Journal of Applied Corporate Finance*, *18*(4), 8-20.

322) Oakley, M., Mohun Himmelweit, S., Leinster, P., & Casado, M. R. (2020). Protection motivation theory: a proposed theoretical extension and moving beyond rationality—the case of flooding. *Water*, *12*(7), 1848.

323) OECD. (2017). Types of cyber incidents and losses. In enhancing the role of insurance in cyber risk management. OECD Publishing, Paris. Dostupno na: https://www.oecd.org/daf/fin/insurance/Enhancing-the-Role-of-Insurance-in-Cyber-Risk-Management.pdf, pristupljeno [1.6.2020.].

324) Ogbanufe, O. M., & Baham, C. (2022). Using Multi-Factor Authentication for Online Account Security: Examining the Influence of Anticipated Regret. *Information Systems Frontiers*, *25*, 897–916.

325) Ogbanufe, O., & Pavur, R. (2022). Going through the emotions of regret and fear: Revisiting protection motivation for identity theft protection. *International Journal of Information Management*, *62*, 102432.

326) Ogbeibu, S., Jabbour, C. J. C., Gaskin, J., Senadjki, A., & Hughes, M. (2021). Leveraging STARA competencies and green creativity to boost green organisational innovative evidence: A praxis for sustainable development. *Business Strategy and the Environment*, *30*(5), 2421-2440.

327) Öğüt, H., Raghunathan, S., & Menon, N. (2011). Cyber security risk management: Public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection. *Risk Analysis: An International Journal*, *31*(3), 497-512.

328) Ordonez, L., & Benson III, L. (1997). Decisions under time pressure: How time constraint affects risky decision making. *Organizational Behavior and Human Decision Processes*, *71*(2), 121-140.

329) Ormerod, P. (1995). *The death of economics*. Faber & Faber.

330) Ossareh, A., Pourjafar, M. S., & Kopczewski, T. (2021). Cognitive Biases on the Iran Stock Exchange: Unsupervised Learning Approach to Examining Feature Bundles in Investors' Portfolios. *Applied Sciences*, *11*(22), 10916.

331) Otuteye, E., & Siddiquee, M. (2019). Underperformance of actively managed portfolios: some behavioral insights. *Journal of Behavioral Finance*, *21*(3), 284-300.

332) Pagach, D., & Warr, R. (2011). The characteristics of firms that hire chief risk officers. *Journal of risk and insurance*, *78*(1), 185-211.

333) Park, T., Ju, I., Ohs, J. E., & Hinsley, A. (2021). Optimistic bias and preventive behavioral engagement in the context of COVID-19. *Research in Social and Administrative Pharmacy*, *17*(1), 1859-1866.

334) Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & security*, *42*, 165-176.

335) Patterson, W., & Winston-Proctor, C. E. (2019). *Behavioral cybersecurity: Applications of personality psychology and computer science*. CRC Press.

336) Payne, J. W., Bettman, J. R., & Johnson, E. J. (1993). *The adaptive decision maker*. Cambridge university press.

337) Peters, G., Shevchenko, P. V., & Cohen, R. (2018). Understanding cyber-risk and cyber-insurance. *Macquarie University Faculty of Business & Economics Research Paper*. Dostupno na: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3200166, pristupljeno [20.11.2023.].

338) Petter, S. (2018). "Haters Gonna Hate": PLS and information systems research. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *49*(2), 10-13.

339) Pfleeger, S. L., Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & security*, *31*(4), 597-611.

340) Pirounias, S., Mermigas, D., & Patsakis, C. (2014). The relation between information security events and firm market value, empirical evidence on recent disclosures: An extension of the GLZ study. *Journal of Information Security and Applications*, *19*(4-5), 257-271.

341) Pohl, R. F., & Erdfelder, E. (2017). Hindsight bias. U: R. F. Pohl (ur.), *Cognitive illusions: Intriguing phenomena in thinking, judgment and memory*, Routledge/Taylor & Francis Group, 424–445.

342) Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: an integrated methodological approach. *Cognition, Technology & Work*, *24*(2), 371-390.

343) Ponemone Institute. (2022). Cost of a Data Breach Report 2022. IBM security. Dostupno na: https://www.ibm.com/reports/data-breach, pristupljeno [1.2.2022.].

344) Ponemone Institute. (2023). Cost of a Data Breach Report 2022. IBM security, https://www.ibm.com/reports/data-breach, pristupljeno [15.10.2023.].

345) Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, *32*(4), 179-214.

346) Posey, C., Roberts, T., Lowry, P. B., Courtney, J., & Bennett, B. (2011). Motivating the insider to protect organizational information assets: Evidence from protection motivation theory and rival explanations. U: *The Dewald Roode workshop in information systems security*. Dostupno na: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2273594, pristupljeno [30.10.2022.].

347) Powell, T. C., Lovallo, D., & Fox, C. R. (2011). Behavioral strategy. *Strategic Management Journal*, *32*(13), 1369-1386.

348) Pretorius, R., & Blaauw, D. (2022). Digital Risk Management: Investigating Human-Factor Security with a Behaviorist Approach. U: *International Conference on Cyber Warfare and Security, 17(*1), 513-521. Dostupno na: file:///C:/Users/Korisnik/Desktop/Downloads/Pretorius+043.pdf, pristupljeno [3.8.2023.].

349) Price Waterhouse Coopers. (2018). Strengthening Digital Society against Cyber Shocks: Key Findings from The Global State of Information Security ® Survey 2018." Dostupno na: https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey/strengthening-digital-society-against-cyber-shocks.html, pristupljeno [1.9.2022.].

350) Price Waterhouse Coopers. (2021). PwC's 2021 Annual Corporate Directors Survey (The director's new playbook: Taking on change, Issue. Dostupno na:

https://www.pwc.com/us/en/services/governance-insightscenter/assets/pwc-2021-annual-corporate-directors-survey.pdf, pristupljeno [1.3.2023.].

351) Price Waterhouse Coopers. (2023). Rethink your cyber budget to get more out of it. Dostupno na: https://www.pwc.com/kz/en/services/global-digital-trust-insights/cyber-budget.html [12.5.2023.].

352) Protte, M., Fahr, R., & Quevedo, D. E. (2020). Behavioral economics for human-in-the-loop control systems design: Overconfidence and the hot hand fallacy. *IEEE Control Systems Magazine*, *40*(6), 57-76.

353) Pryor, J.J. (2023). The Complete List of 219 Cognitive Biases, Effects, and Phenomenons. Dostupno na: https://threwthelookingglass.com/cognitive-biases/, pristupljeno [5.10.2023].

354) Rabin, M. (1998). Psychology and economics. *Journal of economic literature*, *36*(1), 11-46.

355) Rajab, M., & Eydgahi, A. (2019). Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Computers & Security*, *80*, 211-223.

356) Rangel, A., Camerer, C., & Montague, P. R. (2008). A framework for studying the neurobiology of value-based decision making. *Nature reviews neuroscience*, *9*(7), 545-556.

357) Ratchford, M. M., & Wang, Y. (2019). Byod-insure: A security assessment model for enterprise byod. U: *2019 Fifth Conference on Mobile and Secure Services (MobiSecServ)*. IEEE, 1-10. Dostupno na: https://ieeexplore.ieee.org/abstract/document/8686551?casa_token=S3aCR0hJj1oAAAAA:0JMd5sDcziZEGB4SnldB4v0xBidwytzUrXnDdQsCZXWS6a_PeYkayAcxx_aPvLsMXolJHolGyYfxQA, pristupljeno [3.8.2023.].

358) Rea-Guaman, A. M., San Feliu, T., Calvo-Manzano, J. A., & Sánchez-García, I. D. (2018). Systematic review: cybersecurity risk taxonomy. U: *Trends and Applications in Software Engineering: Proceedings of the 6th International Conference on Software Process Improvement (CIMPS 2017) 6*. Springer International Publishing, 137-146. Dostupno na: https://link.springer.com/chapter/10.1007/978-3-319-69341-5_13, pristupljeno [1.8.2023.].

359) Redseal. (2016). *The Rise of Cyber-Overconfidence in C-Suite*. https://www.redseal.net/wpcontent/. Dostupno na: https://www.redseal.net/wp-

content/uploads/2016/12/RedSeal-CEO-Survey-Executive-Summary.pdf, pristupljeno [5.11.2023].

360) Reeves, A., Parsons, K., & Calic, D. (2020). Whose risk is it anyway: How do risk perception and organisational commitment affect employee information security awareness?. U: *International Conference on Human-Computer Interaction*. Springer International Publishing, 232-249. Dostupno na: https://link.springer.com/chapter/10.1007/978-3-030-50309-3_16, pristupljeno [1.8.2023.].

361) Refsdal, A., Solhaug, B., Stølen, K., Refsdal, A., Solhaug, B., & Stølen, K. (2015). *Cyber-risk management*. Springer International Publishing.

362) Rehman, T. (2016). Historical context of behavioral economics. *Intellectual Economics*, *10*(2), 128-132.

363) Reinsel, D., Gantz, J., & Rydning, J. (2018). The digitization of the world from edge to core. *IDC white paper, 13. Dostupno na: https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf*, pristupljeno [2.3.2023.].

364) Reynolds, W. W., & Nelson, R. M. (2007). Risk perception and decision processes underlying informed consent to research participation. *Social science & medicine*, *65*(10), 2105-2115.

365) Rhee, H. S., Ryu, Y. U., & Kim, C. T. (2012). Unrealistic optimism on information security management. *Computers & Security*, *31*(2), 221-232.

366) Rhee, H. S., Ryu, Y., & Kim, C. T. (2005). I am fine but you are not: Optimistic bias and illusion of control on information security. *ICIS 2005 proceedings*, 32. Dostupno na: http://aisel.aisnet.org/icis2005/32, pristupljeno [30.11.2022.].

367) Richard, R., van der Pligt, J., & De Vries, N. (1996). Anticipated affect and behavioral choice. *Basic and Applied Social Psychology, 18*(2), 111–129.

368) Richardson, V. J., Smith, R. E., & Watson, M. W. (2019). Much ado about nothing: The (lack of) economic impact of data privacy breaches. *Journal of Information Systems*, *33*(3), 227-265.

369) Ringle, C., Silva, D. & Bido, D. (2014). Structural Equation Modeling with the Smartpls. *Brazilian Journal Of Marketing*, *13*(2), 56-73.

370) RiskOptics. (2023). Cyber Risk Viewpoints Report. Dostupno na: https://reciprocity.com/, pristupljeno [14.4.2023.].

371) Rogers, R. W. (1983). Cognitive and physiological processes in fear-based attitude change: A revised theory of protection motivation. U: Cacioppo, J., & Petty, R. (ur.) *Social psychophysiology: A sourcebook*, Guilford, 153-176.

372) Romanosky, S., & Petrun Sayers, E. L. (2023). Enterprise risk management: how do firms integrate cyber risk? *Management Research Review*. Vol. ahead-of-print No. ahead-of-print. Dostupno na: https://www.emerald.com/insight/content/doi/10.1108/MRR-10-2021-0774/full/html, pristupljeno [20.11.2023.].

373) Ross, D. (2012). The Economic Agent: Not Human, But Important. U: *Handbook of the Philosophy of Science, Philosophy of Economics*, 691-735. Dostupno na: https://doi.org/10.1016/B978-0-444-51676-3.50023-3, pristupljeno [15.11.2023.].

374) Rothrock, R. (2018). *Digital resilience: Is your company ready for the next cyber threat?*. Amacom.

375) Rydning, D. R. J. G. J., Reinsel, J., & Gantz, J. (2018). The digitization of the world from edge to core. *Framingham: International Data Corporation. 16, 1-28. Dostupno na: https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf,* pristupljeno [20.11.2023.].

376) Samuelson, W., & Zeckhauser, R. (1988). Status quo bias in decision making. *Journal of risk and uncertainty*, *1*, 7-59.

377) Sandberg, T., & Conner, M. (2008). Anticipated regret as an additional predictor in the theory of planned behaviour: A meta-analysis. *British journal of social psychology*, *47*(4), 589-606.

378) Sarstedt, M., Ringle, C. M. & Hair, J. F., (2017). Partial least squares structural equation modeling. U: Homburg, C., Klarmann, M. & Vomberg, A. E. (ur.) *Handbook of market research*. Cham: Springer, 587-632.

379) Sarstedt, M., Ringle, C. M., & Hair, J. F. (2021). Partial least squares structural equation modeling. U: Homburg, C., Klarmann, M., Vomberg, A. (ur.) *Handbook of market research*. Springer International Publishing, 587-632.

380) Sax, J., & Andersen, T. J. (2019). Making risk management strategic: Integrating enterprise risk management with strategic planning. *European Management Review*, *16*(3), 719-740.

381) Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law*, *12*(2), 56-68.

382) Schmitt, M. N. (Ed.). (2013). *Tallinn manual on the international law applicable to cyber warfare*. University Press.

383) Schuetz, S. W., Benjamin Lowry, P., Pienta, D. A., & Bennett Thatcher, J. (2020). The effectiveness of abstract versus concrete fear appeals in information security. *Journal of Management Information Systems*, *37*(3), 723-757.

384) Schwenk, C. H. (1986). Information, cognitive biases, and commitment to a course of action. *Academy of Management Review*, *11*(2), 298-310.

385) Schwenk, C. R. (1984). Cognitive simplification processes in strategic decision-making. *Strategic management journal*, *5*(2), 111-128.

386) Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security*, *124*, 102974.

387) Sharifi, S. (2023). A Novel Approach to the Behavioral Aspects of Cybersecurity. Dostupno na: https://arxiv.org/abs/2303.13621, pristupljeno [20.11.2023.].

388) Sharot, T. (2011). *The optimism bias: A tour of the irrationally positive brain*. Pantheon.

389) Sheeran, P., Harris, P. R., & Epton, T. (2014). Does heightening risk appraisals change people's intentions and behavior? A meta-analysis of experimental studies. *Psychological bulletin*, *140*(2), 511-543.

390) Shefrin, H. (2002). *Beyond greed and fear: Understanding behavioral finance and the psychology of investing*. Oxford University Press.

391) Sheppard, B. H., Hartwick, J., & Warshaw, P. R. (1988). The theory of reasoned action: A meta-analysis of past research with recommendations for modifications and future research. *Journal of consumer research*, *15*(3), 325-343.

392) Shepperd, J. A., Carroll, P., Grace, J., & Terry, M. (2002). Exploring the causes of comparative optimism. *Psychologica Belgica*, *42*, 65–98.

393) Shepperd, J. A., Klein, W. M., Waters, E. A., & Weinstein, N. D. (2013). Taking stock of unrealistic optimism. *Perspectives on Psychological Science*, *8*(4), 395-411.

394) Shepperd, J. A., Pogge, G., & Howell, J. L. (2017). Assessing the consequences of unrealistic optimism: Challenges and recommendations. *Consciousness and Cognition*, *50*, 69-78.

395) Shih, E., & Schau, H. J. (2011). To justify or not to justify: the role of anticipated regret on consumers' decisions to upgrade technological innovations. *Journal of Retailing*, *87*(2), 242-251.

396) Simon, H. A. (1955). A behavioral model of rational choice. *The quarterly journal of economics*, *69*(1), 99-118.

397) Simon, H. A. (1972). Theories of bounded rationality. U: C. B. McGuire & R. Radner (ur.), *Decision and organization.* North-Holland Publishing Company, 161–176.

398) Simonet, J., & Teufel, S. (2019). The influence of organizational, social and personal factors on cybersecurity awareness and behavior of home computer users. U: *IFIP international conference on ICT systems security and privacy protection*. Springer, Cham, 194-208. Dostupno na: https://link.springer.com/chapter/10.1007/978-3-030-22312-0_14, pristupljeno [1.8.2023.].

399) Simonson, I. (1992). The influence of anticipating regret and responsibility on purchase decisions. *Journal of Consumer Research, 19*(1), 105–118.

400) Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & management*, *51*(2), 217-224.

401) Sjöberg, L. (2000). Factors in risk perception. *Risk Analysis*, *20*(1), 1-11.

402) Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. *International Journal of Accounting Information Systems*, *44*, 100548.

403) Slovic, P., Finucane, M. L., Peters, E., & MacGregor, D. G. (2004). Risk as Analysis and Risk as Feelings: Some Thoughts about Affect, Reason, Risk, and Rationality. *Risk Analysis*, 24(2), 311–322.

404) Solarino, A. M., & Aguinis, H. (2021). Challenges and best-practice recommendations for designing and conducting interviews with elite informants. *Journal of Management Studies*, *58*(3), 649-672.

405) Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management & Computer Security*, *22*(1), 42-75.

406) Sommestad, T., Karlzén, H., & Hallberg, J. (2015a). The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information & Computer Security*, *23*(2), 200-217.

407) Sommestad, T., Karlzén, H., & Hallberg, J. (2015b). A meta-analysis of studies on protection motivation theory and information security behaviour. *International Journal of Information Security and Privacy (IJISP)*, *9*(1), 26-46.

408) Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215-225.

409) Spanos, G., & Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. *Computers & Security*, *58*, 216-229.

410) Sprčić, D. M., Kožul, A., & Pecina, E. (2015). State and perspectives of Enterprise risk management system development-the case of Croatian companies. *Procedia Economics and Finance*, *30*, 768-779.

411) Starcke, K., & Brand, M. (2012). Decision making under stress: a selective review. *Neuroscience & Biobehavioral Reviews*, *36*(4), 1228-1248.

412) Statista. (2023). Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2020, with forecasts from 2021 to 2025. Dostuno na: https://www.statista.com/statistics/871513/worldwide-data-created/, pristupljeno [13.4.2023.].

413) Stine, K., Quinn, S., Witte, G., Scarfone, K., Gardner, R. (2020). Integrating Cybersecurity and Enterprise Risk Management. *National Institute of Standards and Technology*. Dostupno na: https://complexdiscovery.com/wp-content/uploads/2020/03/NIST.IR_.8286.pdf, pristupljeno [20.11.2023.].

414) Straub, D., Boudreau, M. C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information systems*, *13*(1), 380-427.

415) Strupczewski, G. (2021). Defining cyber risk. *Safety science*, *135*, 105143.

416) Stulz, R. M. (1984). Optimal hedging policies. *Journal of Financial and Quantitative analysis*, *19*(2), 127-140.

417) Suomala, J., & Kauttonen, J. (2023). Computational meaningfulness as the source of beneficial cognitive biases. *Frontiers in Psychology*, *14*, 1189704.

418) Tatar, Ü., & Karabacak, B. (2012). An hierarchical asset valuation method for information security risk analysis. U: *International Conference on Information Society*

(i-Society 2012) IEEE, 286-291. Dostupno na: https://ieeexplore.ieee.org/abstract/document/6284977, pristupljeno [20.6.2023.].

419) Tayaksi, C., Ada, E., Kazancoglu, Y., & Sagnak, M. (2022). The financial impacts of information systems security breaches on publicly traded companies: reactions of different sectors. *Journal of Enterprise Information Management*, *35*(2), 650-668.

420) Telang, R., & Wattal, S. (2007). An empirical analysis of the impact of software vulnerability announcements on firm stock price. *IEEE Transactions on Software engineering*, *33*(8), 544-557.

421) Terpstra, T. (2009). Flood preparedness: thoughts, feelings and intentions of the Dutch public. Disertacija: University of Twente. Twente. Dostupno na: https://research.utwente.nl/en/publications/flood-preparedness-thoughts-feelings-and-intentions-of-the-dutch-, pristupljeno [1.8.2023.].

422) Thaler, R. H. (1999). Mental accounting matters. *Journal of Behavioral decision making*, *12*(3), 183-206.

423) The Decision Lab. (2022). Biases. Dostupno na: https://thedecisionlab.com/biases-index, pristupljeno [1.9.2022.].

424) Tojib, D. R., & Sugianto, L. F. (2006). Content validity of instruments in IS research. *Journal of Information Technology Theory and Application (JITTA)*, *8*(3), 31-56.

425) Trend micro (2023). Trend micro security predictions for 2023: Future/Tense. Dostupno na: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2023, pristupljeno [13.4.2023.].

426) Triplett, W. J. (2022). Addressing human factors in cybersecurity leadership. *Journal of Cybersecurity and Privacy*, *2*(3), 573-586.

427) Tsai, H. Y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, *59*, 138-150.

428) Tu, C. Z., Yuan, Y., Archer, N., & Connelly, C. E. (2018). Strategic value alignment for information security management: A critical success factor analysis. *Information & Computer Security*, *26*(2), 150-170.

429) Tu, Z., Turel, O., Yuan, Y., & Archer, N. (2015). Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination. *Information & Management*, *52*(4), 506-517.

430) Tu, Z., Yuan, Y. (2014). Critical success factors analysis on effective information security management: a literature review. CSF Analysis on Effective Information

Security. U: Twentieth Americas Conference on Information. Dostupno na: https://core.ac.uk/download/pdf/301361904.pdf, prustupljeno [2.8.2023.].

431) Tversky, A., & Kahneman, D. (1974). Judgment under Uncertainty: Heuristics and Biases: Biases in judgments reveal some heuristics of thinking under uncertainty. *Science*, *185*(4157), 1124-1131.

432) Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & security*, *29*(4), 476-486.

433) VanBoskirk, S., Gill, M., Green, D., Berman, A., Swire, J., & Birrell, R. (2017). The digital maturity model 5.0. Forrester Research. Dostupno na: https://foloop.in/uploads/images/stock/The-Digital-Maturity-Model-5.0-1.pdf, pristupljeno [1.8.2023.].

434) Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*(3-4), 190-198.

435) Venkatesh, V. (1999). Creation of favorable user perceptions: Exploring the role of intrinsic motivation. *MIS quarterly*, *23*(2), 239-260.

436) Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management science*, *46*(2), 186-204.

437) Verčič, A. T., Sinčić, D., & Vokić, N. P. (2010). *Priručnik za metodologiju istraživačkog rada: kako osmisliti, provesti i opisati znanstveno i stručno istraživanje*. MEP.

438) Verizon. (2022). Data Breach Investigations Report. Dostupno na: https://www.verizon.com/business/resources/reports/dbir/, pristupljeno [12.4.2023.]

439) Verkijika, S. F. (2018). Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. *Computers & Security*, *77*, 860-870.

440) Verkijika, S. F. (2019). "If you know what to do, will you take action to avoid mobile phishing attacks": Self-efficacy, anticipated regret, and gender. *Computers in Human Behavior*, *101*, 286-296.

441) Vila, J., Briggs, P., Branley-Bell, D., Gomez, Y., & Coventry, L. (2020). Behavioural Issues in Cybersecurity. U: Insua, D. R.,, Baylon, C., Vila, V. (ur.) *Security Risk Models for Cyber Insurance*. Chapman and Hall/CRC, 27-48.

442) Von der Embse, N. P. (2016). What School Psychologists Need to Know about Structural Equation Modelling. *School Psychologists as Consumers of Research*, *44*, 10-12.

443) von Neumann, J., Morgenstern, O. (1944). *The theory of games and economic behavior*. Princeton University Press

444) Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102.

445) Vrhovec, S., & Mihelič, A. (2021). Redefining threat appraisals of organizational insiders and exploring the moderating role of fear in cyberattack protection motivation. *Computers & Security*, *106*, 102309.

446) Vuković, M. (2022). Strukturalno modeliranje utjecaja bihevioralnih faktora na odlučivanje i performanse investitora na financijskom tržištu. Disertacija. Split: Sveučilište u Splitu, Ekonomski fakultet. Split. Dostupno na: https://repozitorij.efst.unist.hr/islandora/object/efst:4792, pristupljeno [20.11.2023.].

447) Wall, J. D., & Buche, M. W. (2017). To fear or not to fear? A critical review and analysis of fear appeals in the information security context. *Communications of the Association for Information Systems*, *41*(13), 277-300.

448) Wallner, J. (2014). Cyber Risk Management. *Wiley StatsRef: Statistics Reference Online*.

449) Wang, Q. H., & Kim, S. H. (2009). Cyber attacks: Cross-country interdependence and enforcement. U: *Proceedings of the 8th Workshop on Economics of Information Security (WEIS)*. Dostupno na: https://ink.library.smu.edu.sg/sis_research/3301, pristupljeno [20.11.2023.]

450) Wangzhou, K., Khan, M., Hussain, S., Ishfaq, M., & Farooqi, R. (2021). Effect of regret aversion and information cascade on investment decisions in the real estate sector: The mediating role of risk perception and the moderating effect of financial literacy. *Frontiers in Psychology*, *12*, 736753.

451) Warkentin, M., Xu, Z., & Mutchler, L. A. (2013). *I'm safer than you: the role of optimism bias in personal IT risk assessments*. Proceedings of 2013 IFIP 8.11/11.13 Dewald Roode Information Security Research Workshop. Dostupno na: https://www.researchgate.net/profile/Merrill-Warkentin/publication/275462749_I'm_Safer_than_You_The_Role_of_Optimism_Bias_in_Personal_IT_Risk_Assessments/links/55f4350a08ae63926cf269f3/Im-Safer-

than-You-The-Role-of-Optimism-Bias-in-Personal-IT-Risk-Assessments.pdf, pristupljeno [20.11.2023.].

452) Weinstein, N. D. (1980). Unrealistic optimism about future life events. *Journal of personality and social psychology*, *39*(5), 806-820.

453) Weinstein, N. D. (1987). Unrealistic optimism about susceptibility to health problems: Conclusions from a community-wide sample. *Journal of behavioral medicine*, *10*(5), 481-500.

454) Weinstein, N. D. (1989). Optimistic biases about personal risks. *Science*, *246*(4935), 1232-1233.

455) Weinstein, N. D., & Klein, W. M. (1996). Unrealistic optimism: Present and future. *Journal of Social and Clinical Psychology*, *15*(1), 1-8.

456) Weston, R., & Gore, P. A. (2006). A Brief Guide to Structural Equation Modeling. The Counseling Psychologist, *34*(5)*,* 719-751.

457) White, D. M. (2010). The federal information security management act of 2002: a Potemkin village. Federal Information Security Management Act (FISMA). *Fordham L. Rev.*, *79*, 369. Dostupno na: https://security.cms.gov/learn/federal-information-security-management-act-fisma, pristupljeno [1.8.2023.].

458) Wilke A., Mata R. (2012). Cognitive Bias. U: Ramachandran, V.S. (ur.) *The Encyclopedia of Human Behavior*, Academic Press, *1*, 531-535. Dostupno na: https://webspace.clarkson.edu/~awilke/EoHB_Wilke_12.pdf, pristupljeno [15.11.2023.].

459) Williams, B. T. (2014). The joint force commander's guide to cyberspace operations. *Joint Force Quarterly*, *73*(2), 12-19.

460) Willis. (2013). Willis Fortune 500 Cyber Disclosure Study, 2013, Dostupno na: https://docplayer.net/8256053-Willis-fortune-1000-cyber-disclosure-report.html, pristupljeno [20.11.2023.].

461) Wilson, F. R., Pan, W., & Schumsky, D. A. (2012). Recalculation of the critical values for Lawshe's content validity ratio. *Measurement and evaluation in counseling and development*, *45*(3), 197-210.

462) Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in human behavior*, *24*(6), 2799-2816.

463) World Economic Forum. (2012). Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience. Dostupno na:

https://www.weforum.org/reports/risk-and-responsibility-hyperconnected-world-pathways-global-cyber-resilience/, pristupljeno [1.9.2022.].

464) World Economic Forum. (2020). Partnership against Cybercrime. Shaping the Future of
Cybersecurity and Digital Trust, Insight report. Dostupno na: https://www3.weforum.org/docs/WEF_Partnership_against_Cybercrime_report_2020.pdf, pristupljeno [11.4.2023.].

465) World Economic Forum. (2023). Global Cybersecurity Outlook 2023, Insight report. Dostupno na: https://www.weforum.org/publications/global-cybersecurity-outlook-2023/, pristupljeno [11.4.2023.].

466) Wrede, D., Freers, T., & Graf von der Schulenburg, J. M. (2018). Herausforderungen und Implikationen für das Cyber-Risikomanagement sowie die Versicherung von Cyberrisiken–Eine empirische Analyse. *Zeitschrift für die gesamte Versicherungswissenschaft*, *107*(4), 405-434.

467) Wu, J. H., & Wang, S. C. (2005). What drives mobile commerce?: An empirical evaluation of the revised technology acceptance model. *Information & management*, *42*(5), 719-729.

468) Xue, Y., Liang, H., & Wu, L. (2011). Punishment, justice, and compliance in mandatory IT settings. *Information Systems Research*, *22*(2), 400-414.

469) Yayla, A. A., & Hu, Q. (2011). The impact of information security events on the stock value of firms: The effect of contingency factors. *Journal of Information Technology*, *26*(1), 60-77.

470) Yoon, C., & Kim, H. (2013). Understanding computer security behavioral intention in the workplace: An empirical study of Korean firms. *Information Technology & People*, *26*(4), 401-419.

471) Young, D., Beebe, N., & Chang, F. (2012). *Prospect theory and information security investment decisions*. *AMCIS 2012, Proceedings. 8*, Dostupno na: http://aisel.aisnet.org/amcis2012/proceedings/ISSecurity/8, pristupljeno [30.11.2022.].

472) Zaalberg, R., Midden, C., Meijnders, A., & McCalley, T. (2009). Prevention, adaptation, and threat denial: Flooding experiences in the Netherlands. *Risk Analysis: An International Journal*, *29*(12), 1759-1778.

473) Zängerle, D., & Schiereck, D. (2023). Cyberrisiken–Vom Begriffswirrwarr zu einem einheitlichen Begriffsverständnis. *HMD Praxis der Wirtschaftsinformatik*, *60*(1), 214-229.

474) Zeelenberg, M. (1999). Anticipated regret, expected feedback and behavioral decision making. *Journal of behavioral decision making*, *12*(2), 93-106.

475) Zeelenberg, M., & Pieters, R. (2004). Consequences of regret aversion in real life: The case of the Dutch postcode lottery. *Organizational Behavior and Human Decision Processes*, *93*(2), 155-168.

476) Zeelenberg, M., Beattie, J., Van der Pligt, J., & De Vries, N. K. (1996). Consequences of regret aversion: Effects of expected feedback on risky decision making. *Organizational behavior and human decision processes*, *65*(2), 148-158.

477) Zelenika, R. (2000). *Metodologija i tehnologija izrade znanstvenog i stručnog djela*. Ekonomski fakultet Sveučilišta u Rijeci.

478) Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security*, *17*(4), 330-340.

479) Zhang, M., Nazir, M. S., Farooqi, R., & Ishfaq, M. (2022). Moderating Role of Information Asymmetry Between Cognitive Biases and Investment Decisions: A Mediating Effect of Risk Perception. *Frontiers in Psychology*, *13*, 828956.

480) Zhen, J., Xie, Z., & Dong, K. (2020). Positive emotions and employees' protection-motivated behaviours: a moderated mediation model. *Journal of Business Economics and Management*, *21*(5), 1466-1485.

481) Zhen, J., Xie, Z., Dong, K., & Chen, L. (2021). Impact of negative emotions on violations of information security policy and possible mitigations. *Behaviour & information technology*, *41*(11), 2342-2354.

POPIS TABLICA I SLIKA

PRILOZI

PRILOG A - Pregled sektora, podsektora te ključnih usluga za koje su identificirani operatori dužni provoditi aktivnosti održavanja visokog stupanja kibernetičke sigurnosti

Sektor	Podsektor	Ključna usluga
Energetika	Električna energija	Proizvodnja električne energije
		Prijenos električne energije
		Distribucija električne energije
	Nafta	Transport nafte naftovodima
		Proizvodnja nafte
		Proizvodnja naftnih derivata
		Skladištenje nafte i naftnih derivata
	Plin	Distribucija plina
		Transport plina
		Skladištenje plina
		Prihvat i otprema UPP – a
		Proizvodnja prirodnog plina
Prijevoz	Zračni promet	Zračni prijevoz putnika i tereta
		Upravljanje infrastrukturom zračne luke, uključujući upravljanje pomoćnim objektima zračne luke
		Kontrola zračnog prometa
	Željeznički promet	Upravljanje i održavanje željezničke infrastrukture, uključujući upravljanje prometom i prometno-upravljačkim i signalno-sigurnosnim podsustavom
		Usluge prijevoza robe i/ili putnika željeznicom
		Upravljanje uslužnim objektima i pružanje usluga u uslužnim objektima
		Pružanje dodatnih usluga koje su nužne za pružanje usluga prijevoza robe ili putnika željeznicom
	Vodni prijevoz	Nadzor kretanja brodova (VTS usluga)
		Obavljanje poslova pomorske radijske službe
		Održavanje objekata sigurnosti plovidbe
		Prijevoz putnika u međunarodnom i/ili domaćem prometu
	Vodni prijevoz	Ukrcaj i iskrcaj tereta u lukama u međunarodnom i domaćem prometu
		Prijevoz putnika, tereta i vozila u unutarnjim morskim vodama i teritorijalnom moru Republike Hrvatske koji se obavlja na unaprijed utvrđenim linijama prema javno objavljenim uvjetima reda plovidbe i cjenikom usluga

Sektor	Podsektor	Ključna usluga
		Praćenje i lociranje plovila u unutarnjoj plovidbi
		Obavijesti brodarstvu u unutarnjoj plovidbi
		Pristup elektroničkim navigacijskim kartama u unutarnjoj plovidbi
		Baza podataka o trupu plovila u unutarnjoj plovidbi
		Međunarodno elektroničko izvještavanje u unutarnjoj plovidbi
	Cestovni prijevoz	Javni prijevoz putnika
		Korištenje cestovne infrastrukture
		Upravljanje prometnim tokovima ili informiranje vozača (ITS)
Bankarstvo		Platne usluge
Infrastrukture financijskog tržišta		Usluge mjesta trgovanja
		Usluge središnjih drugih ugovornih strana (CCP)
Zdravstveni sektor		Primarna zdravstvena zaštita
		Sekundarna zdravstvena zaštita
		Tercijarna zdravstvena zaštita
		Transfuzijska medicina i transplantacija organa
		Zdravstveno osiguranje i prekogranična zdravstvena zaštita
		Sigurnost hrane
		Zaštita od opasnih kemikalija
		Distribucija i sigurnost lijekova i medicinskih proizvoda
		Nadzor nad zdravstvenim stanjem stanovništva i ljudskim resursima u zdravstvu kroz vođenje javnozdravstvenih registara
Opskrba vodom za piće i njezina distribucija		Opskrba krajnjih korisnika
Digitalna infrastruktura		DNS usluga za .hr TLD
		Registar naziva domena za .hr TLD
		Sustav za registriranje i administriranje sekundarne domene
		Usluga IXP
Poslovne usluge za državna tijela		Usluge u sustavu
		e – Građani
		Poslovne usluge za korisnike državnog proračuna

Izvor: Narodne novine (2018). Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, NN 64/2018.

PRILOG B – Pregled nadležnih sektorskih tijela, CSIRT-ova i tehničkog tijela za ocjenu sukladnosti prema sektorima ključnih usluga

Jedinstvena nacionalna kontaktna točka – Ured Vijeća za nacionalnu sigurnost			
Sektor ključnih usluga	**Nadležno sektorsko tijelo**	**CSIRT**	**Tehničko tijelo za ocjenu sukladnosti**
Energetika	Tijelo državne uprave nadležno za energetiku	Zavod za sigurnost informacijskih sustava	Zavod za sigurnost informacijskih sustava
Prijevoz	Tijelo državne uprave nadležno za promet	Zavod za sigurnost informacijskih sustava	Zavod za sigurnost informacijskih sustava
Bankarstvo	Hrvatska narodna banka	Nacionalni CERT	–
Infrastrukture financijskog tržišta	Hrvatska agencija za nadzor financijskih usluga	Nacionalni CERT	–
Zdravstveni sektor	Tijelo državne uprave nadležno za zdravstvo	Zavod za sigurnost informacijskih sustava	Zavod za sigurnost informacijskih sustava
Opskrba vodom za piće i njezina distribucija	Tijelo državne uprave nadležno za vodno gospodarstvo	Zavod za sigurnost informacijskih sustava	Zavod za sigurnost informacijskih sustava
Digitalna infrastruktura	Središnji državni ured za razvoj digitalnog društva	Nacionalni CERT	Hrvatska akademska i istraživačka mreža – CARNET
Poslovne usluge za državna tijela	Središnji državni ured za razvoj digitalnog društva	Zavod za sigurnost informacijskih sustava ili Nacionalni CERT*	Zavod za sigurnost informacijskih sustava ili Nacionalni CERT**
Davatelji digitalnih usluga			
Davatelji digitalnih usluga	Tijelo državne uprave nadležno za gospodarstvo	Nacionalni CERT	Zavod za sigurnost informacijskih sustava

Izvor: Narodne novine (2018). Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, NN 64/2018.

PRILOG C - Područja zaštite ključnih sustava

Naziv područja	
Fizička sigurnost	Zaštita od narušavanja raspoloživosti ključnog sustava
Sigurnost opskrbe	Razvoj i održavanje ključnih sustava
Upravljanje ugovornim odnosima	Upravljanje projektima
Upravljanje eksternalizacijom	Upravljanje sklopovskom imovinom
Kontrola pristupa prostorima	Upravljanje promjenama programske imovine
Fizičko i logičko razdvajanje ključnih sustava	Konfiguracija ključnih sustava
Kontrola pristupa ključnom sustavu	Preventivne provjere ranjivosti ključnih sustava
Zaštita podataka koji se obrađuju, pohranjuju i prenose u ključnom sustavu	Upravljanje kontinuitetom poslovanja
Zaštita od zlonamjernog programskog koda	Pričuvna pohrana

Izvor: Narodne novine (2018). Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, NN 68/2018.

PRILOG D - Rezultati istraživanja - Pristranost optimizma u kontekstu i izvan područja kibernetičkih rizika

Istraživački rad	Godina	Područje istraživanja	Zemlja	Populacija	Tko je izložen riziku?	Istražuje pristranost optimizma u ulozi nezavisne varijable	Istražuje pristranost optimizma u ulozi moderatora	Zavisna varijabla	Metodologija	Broj ispitanika	Teorijski okvir
Haltinner et al.	2015.	Percepcije rizika, sigurnost i privatnost u online prostoru	SAD	Studenti	Pojedinac	**Da**	Ne	Percepcija	Dubinski intervju	21 student	Nema primjene PMT-a
Chen et al.	2021.	Zaštita podataka u kontekstu e-otpada	Kina	Fizička osoba	Pojedinac	**Da**	**Da**	Namjera	SEM	348 uzorkovanih	PMT
Oakley et al.	2020.	Odlučivanje u vezi rizika od poplave	/	/	/	**Da**	Ne	Percepcija prijetnje, Percepcija suočavanja, Odgovornost (procjena vlasništva)	Kvalitativan pristup koji isključuje empiriju	/	PMT-a
Park et al.	2021.	Upravljanja rizikom od virusa	SAD	Fizička osoba	Pojedinac	**Da**	Ne	Anksioznost, Strah	Multivarijatna linearna regresijska analiza	293 ispitanika	HBM (Model uvjerenja o zdravlju)
Măirean et al.	2021.	Odlučivanje u vezi rizične vožnje	Rumunjska	Vozač	Pojedinac	**Da**	Ne	Rizično ponašanje u vožnji	SEM	366 vozača	PMT-a
Zhang	2022.	Investicijsko odlučivanje u području nekretnina	Zemlje u razvoju	Investitori	Pojedinac	**Da**	Ne	Investicijska odluka	PROCESS	317 ispitanika	Prospektna teorija
Lei et al.	2022.	Stav prema usvajanju mjera opreza protiv krađe identiteta	Prikupljanje podataka putem Amazon Mechanical Turk (što uključuje 43 zemlje)	Fizička osoba	Pojedinac	Ne	Da	Stav	SEM	196 uzorkovanih	TRA
Chen et al.	2022.	Investicijsko odlučivanje	Zemlje u razvoju	Investitori	Pojedinac	**Da**	Ne	Stvarno ponašanje	PROCESS	370 ispitanika	Prospektna teorija

Izvor: Izrada autora

PRILOG E - Rezultati istraživanja – Zabluda povoljnog povijesnog ishoda u kontekstu ekonomskih odluka

Istraživački rad	Godina	Područje istraživanja	Zemlja	Populacija	Ključni zaključak istraživanja	Metodologija	Broj ispitanika	Teorijski okvir
Kudryavtsev et al.	2012.	Investitori na tržištu kapitala	Izrael	Investitori	Segmentirajući investitore na profesionalne i neprofesionalne, uočava se kako su pristranosti jednako snažno prisutne kod obje populacije. Pojava zablude povoljnih povijesnih ishoda je konzistentna i s pojavom ostalih oblika pristranosti kod ulagač te se zaključuje kako se investitori ponašanju na dosljedan intuitivan način.	Korelacijska analiza	41 menadžer portfelja 305 neprofesionalni tržišni investitori	Bihevioralne financije
Otuteye i Siddiquee	2019.	Investitori na tržištu kapitala	/	Investitori	Korištenje usluge upravitelja fonda pripisuje se učinku zablude povoljnog povijesnog ishoda, nedostatku znanja kao i zastrašivanju ili nesigurnosti i pristranosti prema statusu quo.	Kvalitativan pristup	/	Bihevioralne financije
Ossareh et al.	2021.	Investitori na tržištu kapitala	Iran	Investitori	Izloženost kognitivnim pristranostima značajno se razlikuje zbog individualnih karakteristika investitora. Skupina koja je najosjetljivija na gotovo sve analizirane pristranosti, time i na zabludu povoljnog povijesnog ishoda su mlađi ulagači.	Testiranje razlike u grupama; Analiza glavnih komponenata, Klasteriranje	104	Bihevioralne financije

Izvor: Izrada autora

PRILOG F - Rezultati istraživanja – Zabluda nepovoljnog povijesnog ishoda u kontekstu ekonomskih odluka

Istraživački rad	Godina	Područje istraživanja	Zemlja	Populacija	Ključni zaključak istraživanja	Metodologija	Broj ispitanika	Teorijski okvir
Zaalberg et al.	2009.	Upravljanje rizicima	Nizozemska	Fizičke osobe	Rezultati pokazuju da su žrtve izvijestile o jačim emocijama (negativnim i pozitivnim) zbog prošlih poplava u odnosu na pojedince koji nisu pretrpjeli iskustvo štete uzrokovano poplavom. Pojedinci koji su pretrpjeli iskustvo poplave se više brinu o budućim poplavama, doživljavaju se ranjivijima na buduće poplave, doživljavaju posljedice budućih poplava kao teže i imaju jače namjere poduzeti korake prilagodbe u budućnosti. Potonji učinak u potpunosti posredovan specifičnim iskustvima i procjenama.	Modeliranje strukturnih jednadžbi	509	**Teorija motivacije za zaštitom**

Istraživački rad	Godina	Područje istraživanja	Zemlja	Populacija	Ključni zaključak istraživanja	Metodologija	Broj ispitanika	Teorijski okvir
Lin	2019.	Odluke u vezi kupnje osiguranja	SAD (Zapadna obala)	Fizičke osobe	Financijske odluke mogu biti motivirane ne samo iskustvom gubitka, već i nedavnim iskustvom bez gubitka.	Panel analiza i analiza Google trendova	1042	**Bihevioralne financije**

Izvor: Izrada autora

PRILOG G - Rezultati istraživanja temeljenih na PMT teoriji – Percepcija prijetnje

						Percepcije prijetnje		
Istraživački rad	**Godina**	**Područje istraživanja**	**Zemlja**	**Populacija**	**Tko je izložen riziku?**	**Vjerojatnost prijetnje**	**Intenzitet prijetnje**	**Zavisna varijabla**
Barlette et al.	2015.	Odluke u području informacijske sigurnosti	Francuska	CEO	Organizacija	Značajno	Nije značajno	Namjera/Motivacija
Tu et al.	2015.	Odluke u području informacijske sigurnosti	SAD	Zaposlenici	Organizacija	Značajno*	Značajno*	Namjera/Motivacija
Hanus et al.	2018.	Usklađenost s politikom informacijske sigurnosti	SAD	Zaposlenici	Organizacija	Značajno	Značajno	Namjera/Motivacija
Blythe i Coventry	2018.	Odluke u području informacijske sigurnosti – Program za suzbijanje zlonamjernog softvera	UK	Zaposlenici	Organizacija	Značajno	Nije značajno	Namjera/Motivacija
Hooper i Blunt	2019.	Odluke u području informacijske sigurnosti - online	Novi Zeland	Zaposlenici	Organizacija	Nije značajno	Značajno	Namjera/Motivacija
Li et al	2019.	Ponašanje u vezi s kibernetičkom sigurnošću	SAD	Zaposlenici	Organizacija	Značajno	Nije značajno	Stvarno ponašanje
Rajab i Eydgahi	2019.	Usklađenost s politikom informacijske sigurnosti	SAD	Zaposlenici	Organizacija	Značajno	Nije značajno	Namjera/Motivacija
Heidt et al	2019.	Odluke u području informacijske sigurnosti – zaštita putem lozinke	Njemačka	Zaposlenici	Organizacija	Nije značajno	Nije značajno	Namjera/Motivacija
Hina et al	2019.	Usklađenost s politikom informacijske sigurnosti	Malezija	Zaposlenici	Organizacija	Značajno	Značajno	Namjera/Motivacija

						Percepcije prijetnje		
Istraživački rad	**Godina**	**Područje istraživanja**	**Zemlja**	**Populacija**	**Tko je izložen riziku?**	**Vjerojatnost prijetnje**	**Intenzitet prijetnje**	**Zavisna varijabla**
Aurigemma i Mattson -Studija 1	2019.	Usklađenost s politikom informacijske sigurnosti	SAD	Zaposlenici	Organizacija	Nije značajno	Značajno	Namjera/Motivacija
Aurigemma i Mattson - Studija 2	2019.	Odluke u području informacijske sigurnosti	SAD	Zaposlenici	Organizacija	Nije značajno	Značajno	Namjera/Motivacija
Ameen et al. - Uzorak 1	2020.	Odluke u području informacijske sigurnosti – Sigurnost pametnih telefona	SAD	Zaposlenici	Organizacija	Nije značajno	Nije značajno	Namjera/Motivacija
Ameen et al. - Uzorak 2	2020.	Odluke u području informacijske sigurnosti – Sigurnost pametnih telefona	UAE	Zaposlenici	Organizacija	Nije značajno	Djelomično značajno	Namjera/Motivacija

Značenje simbola: * Jedinstven indeks koji objedinjuje vjerojatnosti i intenzitet prijetnje/rizika.
Izvor: Izrada autora

PRILOG H - Rezultati istraživanja temeljenih na PMT teoriji uz proširenje modela za varijablu strah – Percepcija prijetnje

						Percepcije prijetnje		Medijator - Strah		
Istraživački rad	**Godina**	**Područje istraživanja**	**Zemlja**	**Populacija**	**Tko je izložen riziku?**	**Vjerojatnost prijetnje**	**Intenzitet prijetnje**	**Vjerojatnost prijetnje**	**Intenzitet prijetnje**	**Zavisna varijabla**
Posey et al.	2011.	Odluke u području informacijske sigurnosti - korištenje zaštite pristupa računu	SAD	Zaposlenici	Organizacija	Nije značajno	Nije značajno	Nije značajno	Nije značajno	Namjera/ Motivacija
Burns et al.	2017.	Informacijska sigurnost u organizaciji	SAD			/	Značajno	Nije značajno	Nije značajno	Stvarno ponašanje
Vrhovec i Mihelič	2021.	Odluke u području kibernetičke sigurnosti	Slovenija			Nije značajno	Značajno	Nije značajno	Nije značajno	Namjera/ Motivacija
Ma	2022.	Odluke u području informacijske sigurnosti	Kina			/	/	Značajno	Značajno	Stvarno ponašanje

Značenje simbola: / varijabla nije razmotrena u okviru modela
Izvor: Izrada autora

PRILOG I - Rezultati istraživanja – Emocija žaljenje u kontekstu i izvan područja kibernetičkih rizika

Emocija žaljenje u kontekstu kibernetičkog rizika

Istraživački rad	Godina	Područje istraživanja	Zemlja	Populacija	Tko je izložen riziku?	Istražuje odbojnost prema žaljenju u ulozi medijatora	Istražuje direktan utjecaj odbojnosti prema žaljenju na namjeru/motiv	Zavisna varijabla	Metodologija	Broj ispitanika	Teorijski okvir
Chen i Li	2017.	Privatnosti korisnika mobilnog uređaja	Kina	Studenti	Pojedinac	Ne	**Da**	Motivacija	SEM	284	TTAT (Teorija izbjegavanja tehnoloških prijetnji)
Ogbanufe i Baham	2022.	Korištenje višefaktorske provjere autentičnosti za sigurnost računa na mreži	Amazon Mechanical Turk (MTurk)	Fizička osoba	Pojedinac	Da (Dodatno istražuje u ulozi egzogene varijable)	Ne	Motivacija/ Stvarno ponašanje	/*	/*	PMT i Teorija žaljenja
Ogbanufe i Pavur	2022.	Zaštita od krađe identiteta	Amazon Mechanical Turk (uključuje 43 zemlje)	Fizička osoba	Pojedinac	**Da**	Ne	Motivacija	SEM + Provođenje tretmana (niski i značajni apeli straha)	318	PMT i Teorija žaljenja

Emocija žaljenje izvan konteksta kibernetičkog rizika

Istraživački rad	Godina	Područje istraživanja	Zemlja	Populacija	Tko je izložen riziku?	Istražuje odbojnost prema žaljenju u ulozi medijatora	Istražuje direktan utjecaj odbojnosti prema žaljenju na namjeru/motiv	Zavisna varijabla	Metodologija	Broj ispitanika	Teorijski okvir
Shih i Scha	2011.	Očekivano žaljenje zbog odluka potrošača da nadograde tehnološke inovacije	SAD	Fizičke osobe	Kupci	Ne	**Da**	Stvarno ponašanje	Eksperiment	86	Teorija žaljenja
Brewer et al.	2016.	Očekivano žaljenje i zdravstveno ponašanje	Pedeset i šest studija bilo je iz Europe, 17 iz Sjeverne Amerike, šest iz Australije i Novog Zelanda i dvije iz Azije	/	/	/	**Da**	Namjere/ Stvarno ponašanje	Meta analiza	81 studija / 45.618	HBM (Model uvjerenja o zdravlju)
Wangzou	2021.	Odluke u području investiranja u nekretnine	Pakistan	Fizičke osobe	Investitor	Da	**Da**	Stvarno ponašanje	SEM	200	Prospektna teorija i Teorija žaljenja

Izvor: Izrada autora

PRILOG J - Rezultati istraživanja temeljenih na PMT teoriji – Varijable percepcije suočavanja

						Percepcija suočavanja			
Istraživački rad	**Godina**	**Područje istraživanja**	**Zemlja**	**Populacija**	**Tko je izložen riziku?**	**Učinkovitost**	**Samoučinkovitost**	**Troškovi**	**Zavisna varijabla**
Barlette et al.	2015.	Odluke u području informacijske sigurnosti	Francuska	CEO	Organizacija	Značajno	Značajno	Značajno	Namjera/Motivacija
Tu et al.	2015.	Odluke u području informacijske sigurnosti	SAD	Zaposlenici	Organizacija	Značajno	Značajno	/	Namjera/Motivacija
Tsai et al.	2016.	Odluke u području informacijske sigurnosti - online	SAD	Zaposlenici	Osoba	Značajno	Nije značajno	Značajno	Namjera/Motivacija
Burns et al.	2017.	Informacijska sigurnost u organizaciji	SAD	Zaposlenici	Organizacija	Značajno	/	Značajno	Stvarno ponašanje
Hanus et al.	2018.	Usklađenost s politikom informacijske sigurnosti	SAD	Zaposlenici	Organizacija	Značajno	Značajno	Nije značajno	Namjera/Motivacija
Blythe i Coventry	2018.	Odluke u području informacijske sigurnosti - Program za suzbijanje zlonamjernog softvera	UK	Zaposlenici	Organizacija	Značajno	Značajno	Značajno	Namjera/Motivacija
Hooper i Blunt	2019.	Odluke u području informacijske sigurnosti - online	Novi Zeland	Zaposlenici	Organizacija	Nije značajno	Nije značajno	Nije značajno	Namjera/Motivacija
Li et al	2019.	Ponašanje u vezi s kibernetičkom sigurnošću	SAD	Zaposlenici	Organizacija	Značajno	Značajno	Značajno	Stvarno ponašanje
Rajab i Eydgahi	2019.	Usklađenost s politikom informacijske sigurnosti	SAD	Zaposlenici	Organizacija	Značajno	Nije značajno	Značajno	Namjera/Motivacija
Heidt et al	2019.	Odluke u području informacijske sigurnosti – zaštita putem lozinke	Njemačka	Zaposlenici	Organizacija	Značajno	Značajno	Značajno	Namjera/Motivacija
Hina et al	2019.	Usklađenost s politikom informacijske sigurnosti	Malezija	Zaposlenici	Organizacija	Nije značajno	Značajno	/	Namjera/Motivacija
Simonet i Teufel	2019.	Ponašanje u vezi s kibernetičkom sigurnošću	Švicarska	Zaposlenici	Organizacija	Značajno	Značajno	Značajno	Stvarno ponašanje

						Percepcija suočavanja			
Istraživački rad	**Godina**	**Područje istraživanja**	**Zemlja**	**Populacija**	**Tko je izložen riziku?**	**Učinkovitost**	**Samoučinkovitost**	**Troškovi**	**Zavisna varijabla**
Aurigemma i Mattson - Study 1	2019.	Usklađenost s politikom informacijske sigurnosti	SAD	Zaposlenici	Organizacija	Značajno	Značajno	/	Namjera/Motivacija
Aurigemma i Mattson - Studija 2	2019.	Odluke u području informacijske sigurnosti	SAD	Zaposlenici	Organizacija	Značajno	Značajno	/	Namjera/Motivacija
Ameen et al. - Uzorak 1	2020.	Odluke u području informacijske sigurnosti - Sigurnost pametnih telefona	SAD	Zaposlenici	Organizacija	Nije značajno	/	Značajno	Namjera/Motivacija
Ameen et al. - Uzorak 2	2020.	Odluke u području informacijske sigurnosti - Sigurnost pametnih telefona	UAE	Zaposlenici	Organizacija	Nije značajno	/	Nije značajno	Namjera/Motivacija
Vrhovec i Mihelič	2021.	Odluke u području kibernetičke sigurnosti	Slovenija	Zaposlenici	Organizacija	Značajno	Djelomično značajno	/	Namjera/Motivacija
Ma	2022.	Odluke u području informacijske sigurnosti	Kina	Zaposlenici	Organizacija	/	Značajno	Značajno	Stvarno ponašanje

Značenje simbola: * Izračen jedinstven indeks koji objedinjuje vjerojatnosti i intenzitet prijetnje/rizika; / varijabla nije razmotrena u okviru modela

Izvor: Izrada autora

PRILOG K - ISTRAŽIVANJE S GRUPOM EKSPERATA – Molba za sudjelovanje u istraživanju

Poštovani g. [*Prezime*], / Poštovana gđa [*Prezime*],

koristim priliku i pozivam Vas na sudjelovanje u istraživanju u okviru doktorskog istraživanja kojeg provodim na temu: *„Utjecaj percepcije prijetnje na namjeru upravljanja kibernetičkim rizicima: Uloga kognitivnih pristranosti i emocija"*. Izrada disertacije se provodi pod mentorstvom prof. dr. sc. Marijane Ćurak.

Cilj istraživanja je na uzorku glavnih izvršnih menadžera u organizacijama proučiti:

- *utjecaj kognitivnih pristranosti na razinu percepcije prijetnje kibernetičkih rizika*

- *utjecaj percepcije prijetnje kibernetičkih rizika na namjeru upravljanja kibernetičkim rizicima*

- *ulogu emocija kao faktora koji intenzivira utjecaj percepcije prijetnje na namjeru upravljanja kibernetičkim rizicima*

S obzirom na znanja i iskustvo koje posjedujete u području [*upravljanje rizicima OR kibernetičkih rizika OR bihevioralne ekonomije OR metode strukturalnog modeliranja*] odabrani ste kao ekspert, čija ekspertiza može **uvelike doprinijeti razvoju predstavljenog istraživanja**.

Cilj Vašeg angažmana je pomoći u razvoj instrumenta istraživanja, gdje se temeljem procjene grupe eksperata planira razmotriti valjanost mjernog instrumenta.

Vrijeme potrebno za provedbu vrednovanja je procijenjeno na maksimalno 50 minuta.

U privitku dopisa šaljem xls. pod nazivom „**Ekspertna skupina - Valjanost čestica**" za potrebe vrednovanja čestica s detaljnijom uputom.

Molim Vas da xls. elektronički popunite te da ga do **5. travnja 2023.** godine pošaljete putem e-maila.

Nadam se da ste u mogućnosti izdvojiti vrijeme za sudjelovanje u istraživanju.

Slobodno se obratite za sva dodatna pitanja.

Unaprijed se zahvaljujem na Vašem trudu i vremenu.

Srdačan pozdrav,

Dujam Kovač, mag. oec.
Asistent i doktorand
Katedra za financije
Ekonomski fakultet Sveučilišta u Splitu
Cvite Fiskovića 5
e-mail: dujam.kovac@efst.hr

PRILOG L - ISTRAŽIVANJE S GRUPOM EKSPERATA – Upute

Radni list „Uputa“

Poštovani,

zahvaljujem se na iskazanoj spremnosti da izdvojite svoje vrijeme za sudjelovanje u istraživanju i svojom stručnošću doprinesete predstavljenom istraživanju.

Ključne upute:

- Pročitajte dokument s uputama i ukoliko imate nejasnoće, budite slobodni kontaktirati me na:

  e-mail: **dujam.kovac@efst.hr** ili mob: **+385 91 … ….**

U radnom listu pod nazivom "Valjanost čestica":

- Dodijelite razinu važnosti svakoj čestici (*pitanje ili tvrdnja u anketi*) s obzirom na konstrukt (*varijabla*) koji mjeri, na sljedeći način:

  1 - čestica je **neophodna** u mjerenju konstrukta

  2 - čestica je **korisna** u mjerenju konstrukta, ali nije nužna

  3 - čestica **nema važnost** u mjerenju konstrukta

- Ukoliko smatrate da predložena čestica nije dovoljno jasna ili nije cjelovita, sugerirajte izmjenu čestice (*preformulirajte česticu*).

- Ukoliko smatrate da predložena čestica nema važnost, obrazložite Vaš stav.

- Ukoliko smatrate da određena čestica **nedostaje**, a po Vašem mišljenju je neophodna, molio bih Vas da:

  - upišete česticu u nastavku (počevši od 75 reda)

  - objasnite važnost uključivanja čestice te koji konstrukt (*varijablu*) nadopunjuje (*opisuje*)

S obzirom da se primjenjuje **strukturalno modeliranje (SEM metoda)** u empirijskom dijelu istraživanja, **konstrukt** (varijable) je moguće mjeriti većim brojem čestica (*pitanja, tvrdnji*). Stoga je **moguće većem broju čestica dodijeliti razinu važnosti** koji opisujemo kao "**neophodna**".

Svrha prethodno navedenih koraka je da;

- identificirane čestice budu što jasnije potencijalnim sudionicima istraživanja (*glavni izvršni menadžeri u organizacijama*)

- anketa sadrži sve neophodne i relevantne čestice kojima će se moći prikupiti činjenice vezane uz proučavani predmet

- svi identificirani čimbenici budu mjereni dostatnim brojem čestica i to česticama koje ih najbolje opisuju

- prikupljeni podaci budu valjani.

Dodatni, radni list pod nazivom **"Demografske karakteristike"** sastoji se od nekoliko pitanja koja imaju svrhu pružiti uvid u demografske karakteristike eksperata koji su pomogli u istraživačkom procesu.

Radni list „Valjanost čestica“

Kategorija koja se mjeri (konstrukt)	Br. čestice	Čestica	Metrika		Važnost čestice	Prijedlog promjene	Objašnjenje promjene
Procjena vjerojatnosti nastupa kibernetičkog rizika/prijetnje za organizaciju		Organizacija kojom upravljam	**Likertova skala od 1-5**				
	1	… izložena je kibernetičkim rizicima	U potpunosti se ne slažem	U potpunosti se slažem			
	2	… je u opasnosti da pretrpi gubitak ili krađu povjerljivih informacija	U potpunosti se ne slažem	U potpunosti se slažem			
	3	… je u opasnosti da pretrpi prekid rada ili štetu na informacijsko-komunikacijskoj infrastrukturi *(ICT infrastrukturi)*	U potpunosti se ne slažem	U potpunosti se slažem			
		Vjerojatnost nastupa kibernetičkih rizika u organizaciji kojom upravljam	**Likertova skala od 1-5**				
	4	… procijenio bih kao	Veoma mala vjerojatnost pojave	Veoma visoka vjerojatnost pojave			
	5	… temeljem čega će nastupiti gubitak ili krađa povjerljivih informacija, procijenio bih kao	Veoma mala vjerojatnost pojave	Veoma visoka vjerojatnost pojave			
	6	… temeljem čega će nastupiti prekid rada ili šteta na ICT infrastrukturi, procijenio bih kao	Veoma mala vjerojatnost pojave	Veoma visoka vjerojatnost pojave			
	7	… temeljem čega će nastupiti financijski gubitak, procijenio bih kao	Veoma mala vjerojatnost pojave	Veoma visoka vjerojatnost pojave			
	8	… temeljem čega će nastupiti gubitak ugleda, procijenio bih kao	Veoma mala vjerojatnost pojave	Veoma visoka vjerojatnost pojave			
…		…	**…**				
	…	…	…	…			
	…	…	..	..			
	…	…	..	..			
Razina namjeravanog upravljanja kibernetičkim rizicima		Poslovna organizacija pod mojim upravljanjem planira u razdoblju od sljedećih 12 mjeseci	**Likertova skala od 1-5**				
	51	… poticati aktivnosti kojima je cilj zaštita od kibernetičkih rizika	U potpunosti se ne slažem	U potpunosti se slažem			
	52	… ulagati u resurse za potrebe upravljanja kibernetičkim rizicima	U potpunosti se ne slažem	U potpunosti se slažem			
	53	… nadograđivati politike i pravila upravljanja kibernetičkim rizicima	U potpunosti se ne slažem	U potpunosti se slažem			
	54	… primjenjivati suvremene standarde upravljanja kibernetičkim rizicima	U potpunosti se ne slažem	U potpunosti se slažem			
	55	… razvijati plan upravljanja identificiranim kibernetičkim rizicima	U potpunosti se ne slažem	U potpunosti se slažem			
	56	… jačati svijesti kod zaposlenika o kibernetičkim rizicima i njihovom doprinosu u promicanju sigurnosti organizacije	U potpunosti se ne slažem	U potpunosti se slažem			
	57	… razvijati praksu izvještavanja i komunikacije o kibernetičkim rizicima i njegovom upravljanju	U potpunosti se ne slažem	U potpunosti se slažem			
		SUGESTIJA - NOVE ČESTICE					
	58						
	57						
	58						
	59						
	60						

Radni list „Demografske karakteristike“

Odabrani demografski podaci o ekspertima				
Spol _____				
Obrazovanje _____				
Radno mjesto koje obavljate: _____				
Ukupno radno iskustvo u godinama _____				
Razina ekspertize u području:	**1** **Ne poznajem područje**	**2** **Imam dostatno znanje**	**3** **Vrlo dobro poznajem**	**4** **Ekspert sam**
Upravljanje rizicima				
Kibernetički rizici				
Bihevioralna ekonomija				
SEM metodologija				

PRILOG M - ISTRAŽIVANJE S GRUPOM EKSPERATA – Rezultati pokazatelja valjanosti

Redni broj	Oznaka za mjernu česticu	CVR	AVRI	Temeljem odluke eksperata zadržati/brisati/dodati	Temeljem sugestija eksperata minimalna dorada u cilju promicanja jasnoće	Komentar
1	PROB_1_1	1,00	1,00	Zadržati		
2	PROB_1_2	1,00	1,00	Zadržati	Da	
3	PROB_1_3	1,00	1,00	Zadržati	Da	
4	PROB_2	1,00	1,00	Zadržati	Da	
5	PROB_3_1	1,00	1,00	Zadržati	Da	
6	PROB_3_2	1,00	1,00	Zadržati	Da	
7	PROB_3_3	1,00	1,00	Zadržati	Da	
8	PROB_3_4	1,00	1,00	Zadržati	Da	
9	SEV_1_1	0,33	1,33	Isključiti		
9'	SEV_1_1'			Izmijeniti		
10	SEV_1_2	0,11	1,44	Isključiti		
11	SEV_2_1	1,00	1,00	Zadržati	Da	
12	SEV_2_2	1,00	1,00	Zadržati	Da	
13	SEV_2_3	1,00	1,00	Zadržati	Da	
14	SEV_2_4	1,00	1,00	Zadržati	Da	
15	EFF_1	1,00	1,00	Zadržati		
16	EFF_2	0,56	1,22	Isključiti		Odlukom istraživača zadržano u cilju dodatne provjere kroz pilot istraživanje
17	EFF_3	1,00	1,00	Zadržati		
18	EFF_4	1,00	1,00	Zadržati		
19	SEFF_1	1,00	1,00	Zadržati		
20	SEFF_2	1,00	1,00	Zadržati	Da	
21	SEFF_3	1,00	1,00	Zadržati		
22	SEFF_4	0,33	1,33	Isključiti		
23	SEFF_5	0,56	1,22	Isključiti		Odlukom istraživača zadržano u cilju dodatne provjere kroz pilot istraživanje
24	COST_1	1,00	1,00	Zadržati	Da	
25	COST_2	1,00	1,00	Zadržati	Da	
25'	COST_2'			Dodati		
26	COST_3	-0,11	1,78	Isključiti		
27	INT_1	1,00	1,00	Zadržati		

Redni broj	Oznaka za mjernu česticu	CVR	AVRI	Temeljem odluke eksperata zadržati/brisati/dodati	Temeljem sugestija eksperata minimalna dorada u cilju promicanja jasnoće	Komentar
28	INT_2	1,00	1,00	Zadržati		
29	INT_3	1,00	1,00	Zadržati		
30	INT_4	0,56	1,22	Isključiti		Odlukom istraživača zadržano u cilju dodatne provjere kroz pilot istraživanje
31	INT_5	1,00	1,00	Zadržati		
32	INT_6	1,00	1,00	Zadržati		
33	INT_7	0,33	1,33	Isključiti		
34	FEA_1	0,56	1,22	Isključiti		Odlukom istraživača zadržano u cilju dodatne provjere kroz pilot istraživanje
35	FEA_2	1,00	1,00	Zadržati		
36	FEA_3	1,00	1,00	Zadržati		
37	FEA_4	1,00	1,00	Zadržati		
38	REG_1	0,78	1,22	Zadržati	Da	
39	REG_2	1,00	1,00	Zadržati	Da	
40	REG_3	1,00	1,00	Zadržati	Da	
41	REG_4	1,00	1,00	Zadržati	Da	
42	OPB_1_1	0,78	1,11	Zadržati	Da	
43	OPB_1_2	1,00	1,00	Zadržati	Da	
44	OPB_1_3	0,78	1,11	Zadržati	Da	
45	OPB_1_4	0,78	1,11	Zadržati	Da	
46	OPB_2_1	0,33	1,44	Isključiti		
47	OPB_2_2	1,00	1,00	Zadržati	Da	
48	OPB_2_3	0,11	1,44	Isključiti		
49	OPB_2_4	1,00	1,00	Zadržati	Da	
50	OPB_2_5	1,00	1,00	Zadržati	Da	
51	REC_1_1	1,00	1,00	Zadržati	Da	
52	REC_1_2	1,00	1,00	Zadržati	Da	
53	REC_1_3	1,00	1,00	Zadržati	Da	
54	REC_2_1	1,00	1,00	Zadržati	Da	
55	REC_2_2	0,56	1,22	Isključiti		
56	REC_2_3	0,78	1,11	Zadržati	Da	
57	REC_2_4	1,00	1,00	Zadržati	Da	
58'	REC_2_4'			Dodati		

PRILOG N - PILOT ISTRAŽIVANJE – Molba za sudjelovanje u istraživanju

Poštovani/a [*Ime studenta*] ,

koristim priliku i pozivam Vas na sudjelovanje u istraživanju u okviru poslijediplomskog sveučilišnog studija kojeg provodim na temu: *„Utjecaj percepcije prijetnje na namjeru upravljanja kibernetičkim rizicima: Uloga kognitivnih pristranosti i emocija“*.

Putem poveznice [*Anketa*] moguće je pristupiti pilot istraživanju čija je temeljna svrha dobivanje uvida u valjanost postavljenih pitanja te unaprjeđenje glavnog istraživanja.

Anketa se sastoji od šest dijelova. **Prvi dio** se odnosi na demografske karakteristike. **Drugi dio** obuhvaća pitanja koja se odnose na procjenu kibernetičkog rizika kao prijetnje za organizaciju kojom ste imali priliku upravljati u okviru kolegija Marketing menadžment. **Treći dio** se odnosi na procjenu sposobnosti organizacije u upravljanju kibernetičkim rizicima. **Četvrti dio** sadrži pitanja usporedbe Vaše organizacije s drugim poduzećima u industriji te ranija iskustva s kibernetičkim rizicima. **Peti dio** obuhvaća pitanja vezana uz procjenu jačine emocija koje se pojavljuju u vezi s kibernetičkim rizicima. Posljednji, **šesti dio** ankete se odnosi na procjenu Vaše namjere da na razini organizacije upravljate kibernetičkim rizicima.

Svi prikupljeni podaci korist će se u agregiranom obliku te je u potpunoj mjeri zajamčena anonimnost.

Vrijeme potrebno za ispunjavanje upitnika procijenjeno je na 10 minuta.

Slobodno se obratite za sva dodatna pitanja ili komentare koje možete uputiti na e-mail: dujam.kovac@efst.hr.

Unaprijed se zahvaljujem na Vašem trudu i vremenu.

Srdačan pozdrav,

Dujam Kovač, mag. oec.
Asistent i doktorand
Katedra za financije
Ekonomski fakultet Sveučilišta u Splitu
Cvite Fiskovića 5
e-mail: dujam.kovac@efst.hr

PRILOG O - PILOT ISTRAŽIVANJE – Anketni upitnik

DEM1 Spol
- ○ Muško (1)
- ○ Žensko (2)
- ○ Ne želim se izjasniti (3)

DEM2 Dob (iskazati u godinama)

_____

DEM3 Studijski smjer
- ○ Financijski menadžment (1)
- ○ Informatički menadžment (2)
- ○ Menadžment (3)
- ○ Marketing (4)
- ○ Računovodstvo i revizija (5)

DEM4 Jeste li pohađali **edukaciju** na temu kibernetičkih rizika ili kibernetičke sigurnosti ili informacijskih rizika?
- ○ Da (1)
- ○ Ne (2)
- ○ Nisam siguran/a (3)

DEM5 Jeste li samoinicijativno **istraživali područje** kibernetičkih rizika ili kibernetičke sigurnosti ili informacijskih rizika?
- ○ Da (1)
- ○ Ne (2)
- ○ Nisam siguran/a (3)

DEM6 Koje **tržišno mjesto** ste **zauzeli** u igri "**Marketing game**" u okviru kolegija *Marketing menadžment*?
- ○ 1. mjesto u industriji (1)
- ○ 2. mjesto u industriji (2)
- ○ 3. mjesto u industriji (3)
- ○ 4. mjesto u industriji (4)
- ○ 5. mjesto u industriji (11)

INFO
Prije nastavka popunjavanja ankete, molim Vas da pročitate tekst u nastavku:

Ukoliko uvažite iskustvo sudjelovanja u igri tržišnog natjecanja **„Marketing game"** u okviru kolegija *Marketing menadžment* te se **vodite pretpostavkom kako je organizacija kojom ste upravljali stvarna,** u nastavku označite u kojoj mjeri se slažete odnosno ne slažete s ponuđenim tvrdnjama. *Sve tvrdnje navedene su u muškom rodu, a odnose se i na muški i ženski spol.*

U stvarnom tržišnom natjecanju organizacije se *suočavaju sa stvarnim tržišnim prijetnjama i izazovima* što **uključuje i kibernetičke rizike**.

Kibernetički rizici su vrsta operativnih rizika čija realizacija ima utjecaj na *povjerljivost, cjelovitost i dostupnost informacija* koje se **pohranjuju u digitalnom obliku** i **prenose putem informacijsko-komunikacijskih sustava**.
Povjerljivost - informacije su **zaštićene od neovlaštenog pristupa** ili izlaganja neovlaštenim pojedincima
Cjelovitost - informacije su **točne, potpune i zaštićene od neovlaštenih izmjena**
Dostupnost - IT sustavi, informacije i podaci **pravovremeno dostupni ovlaštenim korisnicima**

Kibernetičke rizike segmentiramo prema njihovom izvoru:
Izvan organizacije – uključuju hakerske napade i ucjene, utjecaj prirodnih sila.
Unutar organizacije – uključuju zlonamjerno djelovanje, nemarnost ili slučajne propuste zaposlenika.

Upravljanje kibernetičkim rizicima u organizaciji uključuje *implementaciju politika i mjera* osmišljenih za zaštitu osjetljivih informacija, sprječavanje kibernetičkih napada i odgovor na sigurnosne incidente.

PROB1 Organizacija kojom upravljam

	1 - u potpunosti se ne slažem (1)	2 - uglavnom se ne slažem (2)	3 - niti se slažem niti se ne slažem (3)	4 - uglavnom se slažem (4)	5 - u potpunosti se slažem (5)
… izložena je kibernetičkim rizicima (1)	○	○	○	○	○
… izložena je riziku gubitka ili krađe povjerljivih informacija (2)	○	○	○	○	○
… izložena je riziku prekida rada ili štete na informacijsko-komunikacijskoj infrastrukturi *(ICT infrastrukturi)* (3)	○	○	○	○	○

PROB2 Procijenite vjerojatnost pojave kibernetičkih rizika u organizaciji kojom upravljate

- ○ 1 - veoma mala vjerojatnost pojave (1)
- ○ 2 - mala vjerojatnost pojave (2)
- ○ 3 - umjerena vjerojatnost pojave (3)
- ○ 4 - visoka vjerojatnost pojave (4)
- ○ 5 - veoma visoka vjerojatnost pojave (5)

PROB3 Procijenite vjerojatnost pojave kibernetičkih rizika u organizaciji kojom upravljate

	1 - veoma mala vjerojatnost pojave (1)	2 - mala vjerojatnost pojave (2)	3 - umjerena vjerojatnost pojave (3)	4 - visoka vjerojatnost pojave (4)	5 - veoma visoka vjerojatnost pojave (5)
Rizici temeljem kojih će nastupiti gubitak ili krađa povjerljivih informacija (1)	○	○	○	○	○
Rizici temeljem kojih će nastupiti prekid rada ili šteta na ICT infrastrukturi (2)	○	○	○	○	○
Rizici temeljem kojih će nastupiti financijski gubitak (3)	○	○	○	○	○
Rizici temeljem kojih će nastupiti gubitak ugleda (4)	○	○	○	○	○

SEV1 Kada bi se u organizaciji kojom upravljam realizirao kibernetički rizik

- ○ 1 - izostao bi negativan utjecaj (1)
- ○ 2 - nastupio bi neznačajan prekid rada, mala količina podataka bi bila ugrožena (2)
- ○ 3 - nastupio bi značajan prekid rada, značajna količina podataka bi bila ugrožena (3)
- ○ 4 - nastupio bi financijski gubitak te bi bio narušen ugled (4)
- ○ 5 - ugrozila bi se održivost poslovanja (5)

SEV2 Pod pretpostavkom da kod organizacije kojom upravljam nastupi

	1 - u potpunosti bezopasan (1)	2 - niske štetnosti (2)	3 - umjerene štetnosti (3)	4 - značajne štetnosti (4)	5 - u potpunosti štetan (5)
… gubitak ili krađa povjerljivih informacija, procjenjujem da bi utjecaj na organizaciju bio (1)	○	○	○	○	○
… prekid rada ili šteta na ICT infrastrukturi, procjenjujem da bi utjecaj na organizaciju bio… (2)	○	○	○	○	○
… kibernetički rizik, procjenjujem da bi utjecaj na financijski gubitak bio… (3)	○	○	○	○	○
… kibernetički rizik, procjenjujem da bi utjecaj na gubitak ugleda bio… (4)	○	○	○	○	○

EFF1 Upravljanje kibernetičkim rizicima doprinosi

	1 - u potpunosti se ne slažem (1)	2 - uglavnom se ne slažem (2)	3 - niti se slažem niti se ne slažem (3)	4 - uglavnom se slažem (4)	5 - u potpunosti se slažem (5)
… smanjenju vjerojatnosti pojavljivanja kibernetičkih rizika (1)	○	○	○	○	○
… otpornosti organizacije na kibernetičke rizike (2)	○	○	○	○	○
… smanjenju financijskih gubitaka koji nastaju zbog kibernetičkih rizika (3)	○	○	○	○	○
… smanjenju negativnog utjecaja na ugled koji nastaje zbog kibernetičkih rizika (4)	○	○	○	○	○

SEFF1 Organizacija kojom upravljam

	1 - u potpunosti se ne slažem (1)	2 - uglavnom se ne slažem (2)	3 - niti se slažem niti se ne slažem (3)	4 - uglavnom se slažem (4)	5 - u potpunosti se slažem (5)
... raspolaže financijskim resursima potrebnim za upravljanje kibernetičkim rizicima (1)	○	○	○	○	○
... raspolaže tehničkim resursima *(alati za skeniranje ranjivosti, sustav za otkrivanje upada u mrežu, alati za prevenciju gubitka podataka, alati za zaštitu pristupa podacima, sustavi upravljanja identitetom i pristupom i sl.)* potrebnim za upravljanje kibernetičkim rizicima (2)	○	○	○	○	○
... ima stručnost i znanje potrebno za upravljanje kibernetičkim rizicima (3)	○	○	○	○	○
... može efikasno upravljati kibernetičkim rizicima (4)	○	○	○	○	○

COST1 Za organizaciju kojom upravljam, upravljanje kibernetičkim rizicima zahtjeva

	1 - u potpunosti se ne slažem (1)	2 - uglavnom se ne slažem (2)	3 - niti se slažem niti se ne slažem (3)	4 - uglavnom se slažem (4)	5 - u potpunosti se slažem (5)
… značajna ulaganja u tehnologiju i napredna rješenja zaštite od kibernetičkih rizika (1)	○	○	○	○	○
... mnogo vremena i truda zaposlenika u obrazovanju i treningu (2)	○	○	○	○	○
… mnogo vremena i truda zaposlenika u uvođenju naprednih tehnologija i kreiranju rješenja zaštite (3)	○	○	○	○	○

OPBI1

U ovom pitanju procjenu temeljite na uvjerenjima u nastanak slučajnog događaja, a ne na temelju uvjerenja u sposobnosti Vaše organizacije.

Kada organizaciju kojom upravljam usporedim s drugom organizacijom usporedne veličine i djelatnosti, uvjerenja sam kako

	1 - u potpunosti se ne slažem (1)	2 - uglavnom se ne slažem (2)	3 - niti se slažem niti se ne slažem (3)	4 - uglavnom se slažem (4)	5 - u potpunosti se slažem (5)
… je kibernetički rizik više svojstven drugoj (usporednoj) organizaciji (1)	○	○	○	○	○
… je manja vjerojatnost da će se u organizaciji kojom upravljam realizirati kibernetički rizik (2)	○	○	○	○	○
… bi posljedice kibernetičkog rizika manje ugrozile poslovanje organizacije kojom upravljam (3)	○	○	○	○	○
… je organizacija kojom upravljam manje osjetljiva na kibernetičke rizike (4)	○	○	○	○	○

OPBI2 Izostanak negativnog iskustva s kibernetičkim rizicima na razini organizacije kojom upravljam, potaknuo bi moje uvjerenje

	1 - u potpunosti se ne slažem (1)	2 - uglavnom se ne slažem (2)	3 - niti se slažem niti se ne slažem (3)	4 - uglavnom se slažem (4)	5 - u potpunosti se slažem (5)
… kako je organizacija sigurna od kibernetičkih rizika u sljedećih 12 mjeseci (1)	○	○	○	○	○
… da neće biti financijskog gubitka zbog djelovanja kibernetičkih rizika u sljedećih 12 mjeseci (2)	○	○	○	○	○
… da neće biti negativnog utjecaja na ugled organizacije zbog djelovanja kibernetičkih rizika u sljedećih 12 mjeseci (3)	○	○	○	○	○

REC1 U zadnjih 12 mjeseci realizirani kibernetički rizik u organizaciji kojom upravljam

	1 - u potpunosti se ne slažem (1)	2 - uglavnom se ne slažem (2)	3 - niti se slažem niti se ne slažem (3)	4 - uglavnom se slažem (4)	5 - u potpunosti se slažem (5)
… rezultirao je gubitkom ili krađom povjerljivih podataka (1)	○	○	○	○	○
… uzrokovao je financijske gubitke (2)	○	○	○	○	○
… uzrokovao je negativni utjecaj na ugled (3)	○	○	○	○	○

REC2 Na moje mišljenje o kibernetičkim rizicima kao izazovima za poslovanje organizacije kojom upravljam su utjecali

	1 - u potpunosti se ne slažem (1)	2 - uglavnom se ne slažem (2)	3 - niti se slažem niti se ne slažem (3)	4 - uglavnom se slažem (4)	5 - u potpunosti se slažem (5)
… aktualni izvještaji u medijima (1)	○	○	○	○	○
… aktualni izvještaji za industriju (2)	○	○	○	○	○
…aktualna iskustva organizacija koja su bila izložena kibernetičkim rizicima (3)	○	○	○	○	○
… aktualna osobna iskustva iz privatnog života (4)	○	○	○	○	○

FEA1 Procijenite razinu straha koju kod Vas stvaraju sljedeće spoznaje:

	1 - ne osjećam strah (1)	2 - osjećam blagi strah (2)	3 - osjećam umjereni strah (3)	4 – strah je izražen (4)	5 – strah je intenzivno izražen (5)
Spoznaja da kibernetički rizik prijeti poslovanju organizacije kojom upravljam (1)	○	○	○	○	○
Spoznaja da kibernetički rizik može dovesti do gubitka ili krađe povjerljivih informacija koje pripadaju organizaciji kojom upravljam (2)	○	○	○	○	○
Spoznaja da kibernetički rizik može utjecati na uspješnost poslovanja organizacije kojom upravljam (3)	○	○	○	○	○
Spoznaja da kibernetički rizik može utjecati na ugled organizacije kojom upravljam (4)	○	○	○	○	○

REG1 U kojoj mjeri biste osjećali žaljenje ako bi organizacija kojom upravljate

	1 - ne bih žalio (1)	2 - osjećao bih blago žaljenje (2)	3 - osjećao bih umjereno žaljenje (3)	4 - osjećaj žaljenja bi izražen (4)	5 - osjećaj žaljenja bi bio intenzivno izražen (5)
… pretrpjela kibernetički rizik (1)	○	○	○	○	○
... pretrpjela kibernetički rizik, a nisu uloženi raspoloživi resursi za upravljanje kibernetičkim rizicima (2)	○	○	○	○	○
…pretrpjela kibernetički rizik, što je u negativno utjecalo na rezultat poslovanja (3)	○	○	○	○	○
... pretrpjela kibernetički rizik, što je negativno utjecalo na ugled organizacije (4)	○	○	○	○	○

INT1 Poslovna organizacija pod mojim upravljanjem planira u razdoblju od sljedećih 12 mjeseci

	1 - u potpunosti se ne slažem (1)	2 - uglavnom se ne slažem (2)	3 - niti se slažem niti se ne slažem (3)	4 - uglavnom se slažem (4)	5 - u potpunoti se slažem (5)
… poticati aktivnosti kojima je cilj zaštita od kibernetičkih rizika (1)	○	○	○	○	○
… ulagati u resurse za potrebe upravljanja kibernetičkim rizicima (2)	○	○	○	○	○
… nadograđivati politike i pravila upravljanja kibernetičkim rizicima (3)	○	○	○	○	○
… primjenjivati suvremene standarde upravljanja kibernetičkim rizicima (4)	○	○	○	○	○
… razvijati plan upravljanja identificiranim kibernetičkim rizicima (5)	○	○	○	○	○
… jačati svijesti kod zaposlenika o kibernetičkim rizicima i njihovom doprinosu u promicanju sigurnosti organizacije (6)	○	○	○	○	○

PRILOG P - GLAVNO ISTRAŽIVANJE – Molba za sudjelovanje u istraživanju

Poštovani/a,

moje ime je Dujam Kovač, doktorand sam na Sveučilištu u Splitu te **provodim istraživanje** u području upravljanja rizicima pri čemu je svrha doprinijeti razumijevanju **odluka u vezi upravljanja kibernetičkim rizicima u poslovnim organizacijama**.

Istraživanje se provodi među **populacijom glavnih izvršnih menadžera** (CEO) u **poslovnim subjektima na području Republike Hrvatske**.

Anketom je predviđeno prikupiti osobne stavove i promišljanja najviše rangirane osobe u organizaciji u vezi kibernetičkih rizika te će se **svi prikupljeni podaci koristiti u agregiranom obliku**. **Sukladno GDPR odredbi u potpunoj mjeri je zajamčena anonimnost**.

Izražavam molbu za Vašim sudjelovanjem u anketi što bi bilo od iznimnog doprinosa za provedbu istraživanja. Procijenjeno vrijeme za ispunjavanje ankete je 10 minuta, a moguće je pristupiti putem sljedeće poveznice: "Sveučilište u Splitu - Anketa"

Ukoliko se e-mail ne odnosi na Vas, molim Vas da ga proslijedite vodstvu organizacije.

Unaprijed se zahvaljujem na Vašem vremenu i doprinosu.

Srdačan pozdrav,

Dujam Kovač, mag. oec.
Asistent i doktorand
Katedra za financije
Ekonomski fakultet Sveučilišta u Splitu
Cvite Fiskovića 5
e-mail: dujam.kovac@efst.hr

PRILOG R - GLAVNO ISTRAŽIVANJE – Anketni upitnik

DEM1 Spol

- Muško (1)
- Žensko (2)
- Ne želim se izjasniti (3)

DEM2 Dob

- 18-25 (1)
- 26-35 (2)
- 36-45 (3)
- 46-55 (4)
- 56-65 (5)
- 66 i više (6)

DEM3 Razina obrazovanja

- Srednja stručna sprema (1)
- Viša stručna sprema (2)
- Visoka stručna sprema (3)
- Magisterij ili specijalistički poslijediplomski studij (4)
- Doktorat (5)

DEM4 Vaše godine iskustva rada na poziciji glavnog izvršnog menadžera (u godinama)

- <1 (1)
- 1-3 (2)
- 4-6 (3)
- 7-10 (4)
- >10 (5)

DEM5 Vaše ranije iskustvo rada na IT zadacima (poslovima informacijske i tehnološke podrške poslovanju) (u godinama)

- Nemam ranija iskustva (1)
- <1 (2)
- 1-5 (3)
- >5 (4)

DEM6 Vaše ranije iskustvo rada na zadacima upravljanja rizicima (u godinama)

- Nemam ranija iskustva (1)
- <1 (2)
- 1-5 (3)
- >5 (4)

DEM7 Poslovna organizacija kojom upravljam identificirana je kao **operator ključnih usluga ili davatelj digitalnih usluga** *(sukladno Zakonu o kibernetičkoj sigurnosti NN 64/18)*

- Da (1)
- Ne (2)
- Nisam siguran/a (3)

DEM8 Poslovna organizacija kojom upravljam ima; *detaljno razrađenu* **digitalnu strategiju** koja je *usklađena s cjelokupnom poslovnom strategijom*, *potpuno integrirana* **digitalna rješenja u poslovanju**, **kulturu** koja *kontinuirano* ***inovira i potiče digitalnu transformaciju***.

- 1 - u potpunosti se ne slažem (1)
- 2 - uglavnom se ne slažem (2)
- 3 - niti se slažem niti se ne slažem (3)
- 4 - uglavnom se slažem (4)
- 5 - u potpunosti se slažem (5)

INFO
Prije nastavka popunjavanja ankete, **u cilju informiranja**, molim Vas da pročitate tekst u nastavku:
Kibernetički rizici proizlaze iz upotrebe informacijsko-komunikacijske tehnologije (ICT), a pojava kibernetičkog rizika ima utjecaj na *povjerljivost, cjelovitost i dostupnost* informacija* koje se pohranjuju u digitalnom obliku.

Kibernetički rizici **mogu biti uzrokovani faktorima:**
- *izvan organizacije* (uključuju hakerske napade i ucjene, utjecaj prirodnih sila) te
- *unutar organizacije* (uključuju zlonamjerno djelovanje, nemarnost ili slučajne propuste zaposlenika).

Upravljanje kibernetičkim rizicima u organizaciji uključuje implementaciju politika i mjera osmišljenih za zaštitu osjetljivih informacija, sprječavanje kibernetičkih napada i odgovor na sigurnosne incidente.

DEM9 Je li kibernetički rizik tijekom dosadašnjeg poslovanja značajno negativno utjecao na organizaciju kojom upravljate?

- Da (1)
- Ne (2)
- Nisam siguran/a (3)

PROB1 Procijenite vjerojatnost pojave kibernetičkog rizika u organizaciji kojom upravljate

- 1 - veoma mala vjerojatnost pojave (1)
- 2 - mala vjerojatnost pojave (2)
- 3 - umjerena vjerojatnost pojave (3)
- 4 - visoka vjerojatnost pojave (4)
- 5 - veoma visoka vjerojatnost pojave (5)

PROB2 Procijenite vjerojatnost pojave kibernetičkog rizika u organizaciji kojom upravljate

	1 - veoma mala vjerojatnost pojave (1)	2 - mala vjerojatnost pojave (2)	3 - umjerena vjerojatnost pojave (3)	4 - visoka vjerojatnost pojave (4)	5 - veoma visoka vjerojatnost pojave (5)
Rizik temeljem kojeg će nastupiti gubitak ili krađa povjerljivih informacija (1)	○	○	○	○	○
Rizik temeljem kojeg će nastupiti prekid rada ili šteta na informacijsko-komunikacijskoj infrastrukturi *(ICT infrastrukturi)* (2)	○	○	○	○	○
Rizik temeljem kojeg će nastupiti financijski gubitak (3)	○	○	○	○	○
Rizik temeljem kojeg će nastupiti gubitak ugleda (4)	○	○	○	○	○

SEV1 Kada bi se u organizaciji kojom upravljam realizirao kibernetički rizik

- 1 - izostao bi negativan utjecaj (1)
- 2 - nastupio bi neznačajan prekid rada, mala količina podataka bi bila ugrožena (2)
- 3 - nastupio bi značajan prekid rada, značajna količina podataka bi bila ugrožena (3)
- 4 - nastupio bi financijski gubitak te bi bio narušen ugled (4)
- 5 - ugrozila bi se održivost poslovanja (5)

SEV2 Pod pretpostavkom da kod organizacije kojom upravljam nastupi

	1 - u potpunosti bezopasan (1)	2 - niske štetnosti (2)	3 - umjerene štetnosti (3)	4 - značajne štetnosti (4)	5 - u potpunosti štetan (5)
… gubitak ili krađa povjerljivih informacija, procjenjujem da bi utjecaj na organizaciju bio (1)	○	○	○	○	○
… prekid rada ili šteta na ICT infrastrukturi, procjenjujem da bi utjecaj na organizaciju bio… (2)	○	○	○	○	○
… kibernetički rizik, procjenjujem da bi utjecaj na financijski gubitak bio… (3)	○	○	○	○	○
… kibernetički rizik, procjenjujem da bi utjecaj na gubitak ugleda bio… (4)	○	○	○	○	○

EFF1 Upravljanje kibernetičkim rizicima doprinosi

	1 - u potpunosti se ne slažem (1)	2 - uglavnom se ne slažem (2)	3 - niti se slažem niti se ne slažem (3)	4 - uglavnom se slažem (4)	5 - u potpunosti se slažem (5)
… smanjenju vjerojatnosti pojavljivanja kibernetičkih rizika (1)	○	○	○	○	○
… smanjenju financijskih gubitaka koji nastaju zbog kibernetičkih rizika (2)	○	○	○	○	○
… smanjenju negativnog utjecaja na ugled koji nastaje zbog kibernetičkih rizika (3)	○	○	○	○	○

SEFF1 Organizacija kojom upravljam

	1 - u potpunosti se ne slažem (1)	2 - uglavnom se ne slažem (2)	3 - niti se slažem niti se ne slažem (3)	4 - uglavnom se slažem (4)	5 - u potpunosti se slažem (5)
... raspolaže financijskim resursima potrebnim za upravljanje kibernetičkim rizicima (1)	○	○	○	○	○
... raspolaže tehničkim resursima *(alati za skeniranje ranjivosti, sustav za otkrivanje upada u mrežu, alati za prevenciju gubitka podataka, alati za zaštitu pristupa podacima, sustavi upravljanja identitetom i pristupom i sl.)* potrebnim za upravljanje kibernetičkim rizicima (2)	○	○	○	○	○
... ima stručnost i znanje potrebno za upravljanje kibernetičkim rizicima (3)	○	○	○	○	○
... može efikasno upravljati kibernetičkim rizicima (4)	○	○	○	○	○

COST1 Upravljanje kibernetičkim rizicima zahtjeva od organizacije kojom upravljam

	1 - u potpunosti se ne slažem (1)	2 - uglavnom se ne slažem (2)	3 - niti se slažem niti se ne slažem (3)	4 - uglavnom se slažem (4)	5 - u potpunosti se slažem (5)
… značajna ulaganja u tehnologiju i napredna rješenja zaštite od kibernetičkih rizika (1)	○	○	○	○	○
... mnogo vremena i truda zaposlenika u obrazovanju i treningu (2)	○	○	○	○	○
… mnogo vremena i truda zaposlenika u uvođenju naprednih tehnologija i kreiranju rješenja zaštite (3)	○	○	○	○	○

INT1 Poslovna organizacija pod mojim upravljanjem planira u razdoblju od sljedećih 12 mjeseci

	1 - u potpunosti se ne slažem (1)	2 - uglavnom se ne slažem (2)	3 - niti se slažem niti se ne slažem (3)	4 - uglavnom se slažem (4)	5 - u potpunoti se slažem (5)
… poticati aktivnosti kojima je cilj zaštita od kibernetičkih rizika (1)	○	○	○	○	○
… ulagati u resurse za potrebe upravljanja kibernetičkim rizicima (2)	○	○	○	○	○
… nadograđivati politike i pravila upravljanja kibernetičkim rizicima (3)	○	○	○	○	○
… primjenjivati suvremene standarde upravljanja kibernetičkim rizicima (4)	○	○	○	○	○
… razvijati plan upravljanja identificiranim kibernetičkim rizicima (5)	○	○	○	○	○
… jačati svijesti kod zaposlenika o kibernetičkim rizicima i njihovom doprinosu u promicanju sigurnosti organizacije (6)	○	○	○	○	○

FEA1 Procijenite razinu straha koju kod Vas stvaraju sljedeće spoznaje:

	1 - ne osjećam strah (1)	2 - osjećam blagi strah (2)	3 - osjećam umjereni strah (3)	4 – strah je izražen (4)	5 – strah je intenzivno izražen (5)
Spoznaja da kibernetički rizik može dovesti do gubitka ili krađe povjerljivih informacija koje pripadaju organizaciji kojom upravljam (1)	○	○	○	○	○
Spoznaja da kibernetički rizik može utjecati na uspješnost poslovanja organizacije kojom upravljam (2)	○	○	○	○	○
Spoznaja da kibernetički rizik može utjecati na ugled organizacije kojom upravljam (3)	○	○	○	○	○

REG1 U kojoj mjeri biste osjećali žaljenje ako bi organizacija kojom upravljate

	1 - ne bih žalio/la (1)	2 – osjećao/la bih blago žaljenje (2)	3 – osjećao/la bih umjereno žaljenje (3)	4 - osjećaj žaljenja bi bio izražen (4)	5 - osjećaj žaljenja bi bio intenzivno izražen (5)
… pretrpjela kibernetički rizik (1)	○	○	○	○	○
... pretrpjela kibernetički rizik, a nisu uloženi raspoloživi resursi za upravljanje kibernetičkim rizicima (2)	○	○	○	○	○
… pretrpjela kibernetički rizik, što je negativno utjecalo na rezultat poslovanja (3)	○	○	○	○	○
... pretrpjela kibernetički rizik, što je negativno utjecalo na ugled organizacije (4)	○	○	○	○	○

OPBI1
Na sljedeće pitanje odgovor ponudite sukladno Vašem uvjerenju u nastanak budućeg događaja (isključite uvjerenje o sposobnosti organizacije u upravljanju kibernetičkim rizicima).

Kada organizaciju kojom upravljam usporedim s drugom organizacijom usporedne veličine i djelatnosti, uvjerenja sam kako

	1 - u potpunosti se ne slažem (1)	2 - uglavnom se ne slažem (2)	3 - niti se slažem niti se ne slažem (3)	4 - uglavnom se slažem (4)	5 - u potpunosti se slažem (5)
… je kibernetički rizik više svojstven drugoj (usporednoj) organizaciji (1)	○	○	○	○	○
… je manja vjerojatnost da će se u organizaciji kojom upravljam realizirati kibernetički rizik (2)	○	○	○	○	○
… bi posljedice kibernetičkog rizika manje ugrozile poslovanje organizacije kojom upravljam (3)	○	○	○	○	○
… je organizacija kojom upravljam manje osjetljiva na kibernetičke rizike (4)	○	○	○	○	○

OPBI2 *Bez obzira na stvarna ranija iskustva u vezi kibernetičkih rizika, izrazite razinu slaganja s navedenom hipotetskom tvrdnjom s obzirom na stupanj u kojem Vas opisuje.*

Izostanak negativnog iskustva s kibernetičkim rizicima na razini organizacije kojom upravljam, potaknuo bi moje uvjerenje

	1 - u potpunosti se ne slažem (1)	2 - uglavnom se ne slažem (2)	3 - niti se slažem niti se ne slažem (3)	4 - uglavnom se slažem (4)	5 - u potpunosti se slažem (5)
… kako je organizacija sigurna od kibernetičkih rizika u sljedećih 12 mjeseci (1)	○	○	○	○	○
… da neće biti financijskog gubitka zbog djelovanja kibernetičkih rizika u sljedećih 12 mjeseci (2)	○	○	○	○	○
… da neće biti negativnog utjecaja na ugled organizacije zbog djelovanja kibernetičkih rizika u sljedećih 12 mjeseci (3)	○	○	○	○	○

REC1 U zadnjih 12 mjeseci realizirani kibernetički rizik u organizaciji kojom upravljam

	1 - u potpunosti se ne slažem (1)	2 - uglavnom se ne slažem (2)	3 - niti se slažem niti se ne slažem (3)	4 - uglavnom se slažem (4)	5 - u potpunosti se slažem (5)
… rezultirao je gubitkom ili krađom povjerljivih podataka (1)	○	○	○	○	○
… uzrokovao je financijske gubitke (2)	○	○	○	○	○
… uzrokovao je negativni utjecaj na ugled (3)	○	○	○	○	○

REC2 Na moje mišljenje o kibernetičkim rizicima kao izazovima za poslovanje organizacije kojom upravljam su utjecali

	1 - u potpunosti se ne slažem (1)	2 - uglavnom se ne slažem (2)	3 - niti se slažem niti se ne slažem (3)	4 - uglavnom se slažem (4)	5 - u potpunosti se slažem (5)
… aktualni izvještaji u medijima (1)	○	○	○	○	○
… aktualni izvještaji za industriju (2)	○	○	○	○	○
…aktualna iskustva organizacija koja su bila izložena kibernetičkim rizicima (3)	○	○	○	○	○
… aktualna osobna iskustva iz privatnog života (4)	○	○	○	○	○

ŽIVOTOPIS AUTORA

Dujam Kovač rođen je 7. svibnja 1991. godine u Splitu. Završio je srednju Ekonomsko-birotehničku školu u Splitu. Nakon završetka srednje škole, upisao je Ekonomski fakultet u Splitu, gdje je završio sveučilišni preddiplomski i diplomski studij Poslovne ekonomije, smjer Financije, kao jedan od najuspješnijih studenata generacije. Dobitnik je Dekanove nagrade 2014. godine za ostvareni iznimni uspjeh tijekom studija te Rektorove nagrade 2016. godine za izvrsnost. Tijekom studiranja na diplomskom studiju, bio je angažiran kao demonstrator na kolegijima *Financijski menadžment, Međunarodne poslovne financije, Financijsko modeliranje, Poslovna statistika i Menadžment*.

Nakon stjecanja diplome 2015. godine, zapošljava se kao pripravnik u reviziji, pri čemu sudjeluje u provođenju operativnih aktivnosti kao što su analiziranje poslovnih procesa, prikupljanje podataka i njihova analiza sukladno praksi revizije. U 2016. godini zapošljava se na radnom mjestu financijski službenik, a glavno zaduženje bilo je uspostava procesa planiranja i praćenja realizacije novčanog tijeka investicijskih projekata, za što mu je 2017. godine dodijeljena nagrada Uprave. Dodatne aktivnosti uključivale su financijske analize te izradu izvještaja za potrebe podrške odlučivanja i financiranja. Od 2018. godine zaposlen je kao asistent na Katedri za financije Ekonomskog fakulteta u Splitu. Sudjeluje u izvođenju nastave na kolegijima prijediplomskog sveučilišnog studija: *Upravljanje rizicima, Financijske institucije i tržišta, Bankarstvo, Osnove financija, Financijski menadžment I, Monetarna ekonomija I*; na kolegijima diplomskom sveučilišnog studija: *Ekonomika osiguranja i Financijski menadžment II*, na kolegijima prijediplomskog stručnog studija: *Bankarstvo i osiguranje i Osnove financijskog menadžmenta* te na kolegiju stručnog diplomskog studija: *Upravljanje rizicima, Monetarne financije*. Obavlja zadatke tajnika na Katedri za financije, pri čemu je 2019. godine sudjelovao u organizaciji Interkatedarskog skupa i pripremi Znanstvene monografije pod naslovom „*Financijska kretanja – najnoviji događaji i perspektive*“.

Na Ekonomskom fakultetu u Splitu 2019. godine upisao je Poslijediplomski sveučilišni studij Ekonomije i poslovne ekonomije. U okviru ERASMUS+ programa kratkoročne mobilnosti za doktorske studente u lipnju i srpnju 2023. godine odlazi na „*University of Ljubljana, School of Economics and Business*“ što koristi za unaprjeđenje istraživačkih vještina te sudjelovanje u programu Ljubljana Summer School.

U koautorstvu je dosad objavio sedam znanstvenih radova te jedan samostalan rad. Aktivno je sudjelovao na četiri međunarodne te jednoj domaćoj znanstvenoj konferenciji. Redovito pohađa

edukacijske programe, pri čemu se izdvaja ERASMUS+ program osposobljavanja na „*University of Maribor, Faculty of Economics and Business*“ te Modeliranje strukturalnim jednadžbama u okviru programa kojeg organizira Statistical Horizon.

Član je organizacijskog odbora međunarodne znanstvene konferencije „*Challenges of Europe“* za što je 2019. godine dobio priznanje Ekonomskog fakulteta u Splitu za poticanje međunarodne suradnje te je član je radnog tima za izradu „*Strategije razvoja grada Splita do 2030. godine“*.

Aktivno se služi engleskim jezikom te računalnim statističkim programima *STATA, SPSS, SMART PLS* i *R*.

Popis objavljenih radova:

- **Kovač**, **D.**, Podrug, D. (2023). Improving portfolio liquidity: MCDM approach to share selection on the Zagreb Stock Exchange. Croatian Operational Research Review, 14(1), 29-39.
- Ćurak, M., **Kovač**, **D.**, Poposki, K. (2021). The Drivers of Voluntary Private Health Insurance Demand in European Countries. *Ekonomska misao i praksa*, *30*(2), 457-474. doi:10.17818/EMIP/2021/2.7.
- **Kovač**, **D.** (2021). Ulaganje u kibernetičku sigurnost. *Zbornik radova Veleučilišta u Šibeniku*, *15*(1-2), 61-73. doi:10.51650/ezrvs.15.1-2.4.
- Ćurak, M., **Kovač**, **D.** (2020). Upravljanje rizicima društava za neživotno osiguranje i reosiguranje primjenom tehnike sekuritizacije. *Ekonomski Vjesnik*, *33*(1), 287-302.
- Pepur, S., **Kovač**, **D.**, Ćurak, M. (2020). Factors behind trade credit financing of SMEs in Croatia. *Zbornik Veleučilišta u Rijeci*, *8*(1), 59-76 doi:10.31784/zvr.8.1.11
- Ćurak, M., Pepur, S., **Kovač**, **D.** (2020). Does Financial Literacy Make the Difference in Non-Life Insurance Demand Among European Countries?. *Ekonomski pregled*, *71*(4), 359-381. doi:10.32910/ep.71.4.3.
- Ćurak, M., **Kovač**, **D.**, Pepur, S. (2019) Informiranost korisnika financijskih usluga i potražnja za životnim osiguranjem. U: Družić, G., Lovrinović, I., Basarac Sertić, M., Nakić, M. (ur.) Svjetski financijski vrtlog - 30 godina poslije.
- Pivac, S., Marasović, B., **Kovač**, **D.** (2015) Economic and demographic determinants of demand for life insurance. U: Zadnik, Stirn, L., Žerovnik, J., Drobne, S. (ur.) Proceedings of the 13th International Symposium on Operational Research SOR'15.