Dujam Kovač, mag. oec.[1]

ULAGANJE U KIBERNETIČKU SIGURNOST

Pregledni rad / Review
UDK / UDC: 330.46
DOI: 10.51650/ezrvs.15.1-2.4
Primljeno / Received: 11/12/2020
Prihvaćeno / Accepted: 4/1/2021

Ubrzani razvoj tehnologija i njihova sve učestalija primjena unutar poslovnih organizacija stvaraju brojne prednosti u smislu brzine izvršavanja i automatizacije poslovnih procesa, lakšeg pristupa i razmjene informacija, obavljanja poslovnih aktivnosti na daljinu, lakšeg pristupa tržištima, smanjivanja troškova poslovanja i dr. Istodobno, poslovne organizacije izložene su kibernetičkim rizicima odnosno prijetnjama koje postaju sve različitije, složenije te bilježe kontinuiran rast. Različiti oblici kibernetičkih rizika manifestiraju se kroz kompromitaciju informacijskih sustava poslovnih organizacija što može izazvati značajne izravne i neizravne financijske gubitke. Premda je uočena sve veća ranjivosti na kibernetičke rizike, posebno u smislu njihovog intenziteta utjecaja na poslovanje organizacija, i dalje je prisutan manjak aktivnosti upravljanja kibernetičkom sigurnošću. Velik broj poslovnih organizacija ignorira odnosno podcjenjuje kibernetičke rizike ili se oslanja na generičke proizvode. Unatoč činjenici kako kibernetički rizici postaju sve važniji čimbenik utjecaja na poslovanje organizacija i rezultata njihovog djelovanja, istraživanja kibernetičkih rizika u ekonomskoj literaturi te u njezinom užem području upravljanja rizicima, nisu adekvatno zastupljena. Cilj ovog rada je pružiti pregled istraživanja u području ulaganja u kibernetičku sigurnost kao metode fizičke kontrole šteta koja je neizostavna pretpostavka povjerljivost, dostupnost i cjelovitost informacija te informacijskih sustava. Nadalje cilj rada je ulaganje u kibernetičku sigurnost usporediti s metodom financijske kontrole te istaknuti važnost kombiniranja ovih dviju metoda u cilju postizanja kibernetičke sigurnosti.

Ključne riječi: *kibernetička sigurnost, kibernetički rizici, ulaganje u sigurnost, fizička kontrola šteta.*

1. Uvod

Kibernetički rizici jesu operativni rizici koji imaju potencijalno negativan učinak na kibernetičku sigurnost. Potonju definiramo kao aktivnosti i mjere kojima se postiže autentičnost, povjerljivost, cjelovitost te dostupnost podataka i infrastrukture unutar kibernetičkog prostora. Kibernetički prostor predstavlja virtualnu cjelinu unutar koje se realizira razmjena informacija između mrežnih i informacijskih sustava neovisno o njihovoj povezanosti na internet (CERT, 2016).

[1] Ekonomski fakultet Sveučilišta u Splitu, e-mail: dujam.kovac@efst.hr

Cebula i Young (2010) prvi su koji kibernetičke rizike opisuju kroz učinak na povjerljivost, dostupnost i cjelovitost informacija te informacijskih sustava, a kibernetička sigurnost temeljena je na istoimenim načelima. Povjerljivost podrazumijeva ograničenje pristupa informacijama odnosno zabranu pristupa informacijama neovlaštenim osobama u svrhu zaštite privatnosti informacija. Nadalje, načelo dostupnosti pretpostavlja kako isključivo ovlašteni korisnik, u skladu sa zadanim uvjetima, ima pravo raspolagati ovlaštenim informacijama. Konačno, načelo cjelovitosti podrazumijeva zaštitu povjerljivih informacija od bilo kakvog oblika modifikacije.

U današnje vrijeme kada je primjena informacijske tehnologije u poslovanju i životu pojedinca sve izraženija, kibernetički rizici mogu ozbiljno utjecati na odvijanje poslovnih procesa unutar organizacija, kao i na živote pojedinaca. Utjecaj je izraženiji što je veća primjena informacijske tehnologije. Stoga se kibernetički rizici značajno povećavaju, a prema Ćurak (2019), isti postaju jednim od najznačajnijih operativnih rizika poslovnih organizacija. Navedeno dokazuje istraživanje koje je provelo Allianz Global Corporate & Speciality (AGCS) prema kojem je preko dvije i pol tisuće stručnjaka u području upravljanja rizicima, kibernetičke rizike izdvojilo kao glavnu prijetnju u poslovanju (AGCS, 2020), a da je riječ o aktualnom izazovu potvrđuje podatak Ponemon Institute (2020) koji otkriva kako je preko 91% poslovnih organizacija pretrpjelo barem jedan kibernetički incident u protekla 24 mjeseca, što je potvrđeno na uzorku od preko dvije tisuće stručnjaka u području informacijskih tehnologija i informacijske sigurnosti.

Morgan (2019) izvještava kako će do 2021. godine na globalnoj razini štete uzrokovane kibernetičkim kriminalom, a koji prema Eling i Schnell (2016) predstavlja segment ukupnih kibernetičkih rizika, iznositi 6 trilijuna dolara godišnje. Predviđa se da će na globalnoj razini troškovi proizvoda i usluga koji podupiru kibernetičku sigurnost premašiti 1 bilijun dolara u razdoblju od 2017. do 2021. godine. Različite su procjene ukupnih troškova realizacije kibernetičkih rizika, kao i pitanje obuhvata vrsta kibernetičkog incidenta, odnosno uzroka kibernetičkih incidenata koji određuje i apsolutne procjene utjecaja kibernetičkih rizika na ekonomiju. Međutim, jasno je kako trendovi ukazuju na porast troškova. Istraživanje AON (2019), koje se u suradnji s Ponemon Institutom provodi nad zaposlenicima angažiranima na aktivnostima upravljanja rizicima, potvrđuje kako više od dvije trećine ispitanih očekuje da će nastupiti povećanje izloženosti poslovnih organizacija kibernetičkim rizicima. Biener et al. (2015) i Aldasoro et al. (2020) razmatraju razliku prema sektorima te empirijski potvrđuju kako banke i društva za osiguranje (financijski sektor) imaju manje prosječne troškove prema nastalom kibernetičkom incidentu, a isto objašnjavaju povećanom regulacijom koja potiče na veće ulaganje u kibernetičku sigurnost.

Kada je riječ o razini razvoja upravljanja kibernetičkim rizicima, brojke potvrđuju kako se ne vodi dovoljno računa o kibernetičkim rizicima. Prema Deloitte (2020) koji u suradnji s Touche LLP i The Financial Services Information Sharing and Analysis Center (FS-ISAC) provodi godišnje istraživanje nad članovima FS-ISAC-a, manje je od 0.5% godišnjeg prihoda utrošeno je na postizanje kibernetičke sigurnosti te približno 11% godišnjeg budžeta odjela za informacijske tehnologije namijenjeno je održavanju kibernetičke sigurnosti. Podaci su ostali nepromijenjeni u posljednje tri godine od kada se provode istraživanja. Ashby et al. (2018), upravljanje kibernetičkim rizicima uspoređuju s praksama i metodama integriranog upravljanja rizicima (ERM) te zaključuju kako ERM zanemaruje kibernetičke rizike koji nisu u dovoljnoj mjeri integrirani u koncept objedinjenog upravljanja rizicima kod poslovnih organizacija. Potonju tezu potvrđuje

globalna anketa o informacijskoj sigurnosti koju provode Price Waterhouse Coopers (2018), a koja navodi kako se kibernetički rizici unutar uprava poslovnih organizacija još uvijek razmatraju kao problemi i zadaće niže razine odnosno funkcijskog odjela. Prema Madnick (2017), iako su aktivnosti zaštite od kibernetičkog napada protokom vremena napredovale, stupanj napredovanja je vidljiv i kod pokretača napada (hakera), stoga Jalali et al. (2018) navode kako nije pitanje; „Hoće li organizacija pretrpjeti napad?", nego je pitanje; „Kada će pretrpjeti napad i kojim intenzitetom?". Unatoč sve većoj ranjivosti na kibernetičke rizike, posebno u smislu njihovog intenziteta utjecaja na poslovanje organizacije, i dalje je prisutan manjak aktivnosti upravljanja kibernetičkom sigurnošću.

Istraživanja u ekonomskoj literaturi te u njezinom užem području upravljanju rizicima, nisu adekvatno zastupljena, posebice nije zastupljeno u istraživanjima domaćih autora. Cilj ovog rada je pružiti pregled istraživanja u području ulaganja u kibernetičku sigurnost kao metode fizičke kontrole šteta koja je neizostavna pretpostavka povjerljivosti, dostupnosti i cjelovitosti informacija te informacijskih sustava. Nadalje cilj rada je ulaganje u kibernetičku sigurnost usporediti s metodom financijske kontrole te istaknuti važnost kombiniranja ovih dviju metoda u upravljanju kibernetičkim rizicima.

U nastavku se opisuju metode upravljanja kibernetičkim rizicima, potom se pruža pregled literature u području ulaganja u kibernetičku sigurnost koja je segmentirana prema metodologiji optimizacije ulaganja u kibernetičku sigurnost. Nakon toga, ulaganje u kibernetičku sigurnost se razmatra kao metoda u kombinaciji s metodom transfera rizika na društva za osiguranje. U posljednjem dijelu rada iznijeti su zaključci te promišljanja, odnosno prijedlog vezan za buduća istraživanja.

2. Upravljanje kibernetičkim rizicima

Upravljanje kibernetičkim rizicima obuhvaća primjenu metoda fizičke kontrole, koja u slučaju izloženosti prema kibernetičkim rizicima uključuje smanjivanje rizika kroz poduzimanje mjera kibernetičke sigurnosti. Pored toga, obuhvaća metode financijske kontrole koje imaju oblik zadržavanja rizika odnosno prijenos rizika na društva za osiguranje. Cijeli proces upravljanja objedinjuje aktivnosti: identifikacije, kvantifikacije, integracije, prioritizacije, izbora i primjene metode upravljanja rizicima te nadzor (Harrington i Niehaus, 2004).

Ulaganje u kibernetičku sigurnost metoda je fizičke kontrole kojom se smanjuje rizik. Međutim, iako metode fizičke kontrole rizika uključuju i izbjegavanje rizika, kada je riječ o kibernetičkim rizicima, iste nije moguće izbjeći (Marotta et al., 2017). Naime, izbjeći takve rizike značilo bi provoditi poslovne aktivnosti bez primjene tehnoloških rješenja (RSA, 2016). Primjerice, danas uobičajene zadaće poslovne organizacije, kao što su obračun plaća te zaprimanje ulaznih i kreiranje izlaznih računa, nemoguće je zamisliti bez tehničke podrške, a posebno je nemoguće zamisliti poslovne aktivnosti višeg stupnja složenosti kao što su međunarodna trgovina ili preuzimanje i spajanje tvrtki. Upravljanje kibernetičkim rizicima potpunim izbjegavanjem negativnih implikacija kibernetičkih rizika pretpostavlja izostanak tehničke podrške unutar poslovnih procesa što nije očekivani učinak upravljanja kibernetičkim rizicima iz razloga što isto dovodi do operacija niže efikasnosti i niže kvalitete te ugrožava osnovne ciljeve poslovanja, a oportunitetne troškove čini značajno višima. Stoga se

ulaganje u kibernetičku sigurnost razmatra kao metoda fizičke kontrole kojom se utječe na smanjenje rizika s kojim se suočava poslovna organizacija. Smanjenje rizika rezultat je smanjenja broja kibernetičkih incidenata (frekvencije šteta), odnosno smanjenje visine šteta uzrokovane kibernetičkim incidentima (intenzitet šteta).

Ulaganje u kibernetičku sigurnost pretpostavlja utrošak novčanih sredstava (kupnju softverskih rješenja) te angažman kvalificiranog osoblja koje će uložiti napor i utrošiti vrijeme za postavljanje sustava kibernetičke sigurnosti te njegovog održavanja. Korist takvog ulaganja je smanjenje sredstava angažiranih u nadoknadi troškova koje uzrokuju kibernetički incidenti. Mukhopadhyay et al. (2005) učinke uzorkovane kibernetičkim incidentima dijele na izravne i neizravne. Izravni učinci odnose se na štete uzrokovane nedozvoljenim pristupom u mrežu, štete na infrastrukturi pomoću kojih se odvija razmjena informacija, štete uzrokovane neautoriziranim pristupom podacima, odnosno nedostupnosti mreže pomoću koje se odvija razmjena informacija. Neizravni učinci pojavljuju se u obliku smanjenja tržišne kapitalizacije, narušene privatnosti klijenata, odštetih zahtjeva trećih strana, sudskih sporova te gubitka reputacije. Dakle, nositelji odluka o ulaganju u kibernetičku sigurnost zasigurno će nastojati provoditi optimalnu kontrolu šteta razmatrajući koristi i troškove poduzetih aktivnosti s ciljem smanjenja šteta.

Prema Sokri (2020), tradicionalne tehnike zaštite od kibernetičkih rizika uključuju: tehnike zaštite od neovlaštenog pristupa (engl. *tamperproof techniques*), kriptografiju (engl. *cryptography*), tehnike otkrivanja i prevencije (engl. *detection and prevention techniques*), mamac za detekciju zlonamjernih aktivnosti (engl. *honeypot*) te pripisivanje napada (engl. *technical attribution*). Sve navedene tehnike predstavljaju važne mehanizme kibernetičke sigurnosti, međutim iste nisu panaceja (Roy et al., 2010).

U nastavku se iznosi pregled literature segmentiran prema kriteriju metodologije određenja optimalnog ulaganja u kibernetičku sigurnost. Naime, prvi segment usmjerava se na teoriju očekivane koristi odnosno razmatra visinu potrebnog ulaganja kojim će se optimizirati odnos između utroška resursa i generirane koristi koja se prema Alter i Sherer (2004) manifestira kroz ukupno smanjenje utjecaja rizika na poslovnu organizaciju. Drugi segment iz metodološke perspektive pripada području teorije igara koji se pokazuje najprikladnijim u smislu modeliranja interakcije između ograničenog broja sudionika u konkretnom slučaju poslovne organizacije koja štiti vlastito poslovanje i poduzima aktivnosti ulaganja u kibernetičku sigurnost te napadača (hakera) koji ima namjeru ugroziti sigurnost poslovne organizacije. Sigurnosne prijetnje koje uvjetuje namjera napadača segmentirane su u ciljane napade koji dolaze od hakera čije su namjere usmjerene u nedozvoljeno pristupanje podacima točno određenog sustava odnosno u distribuirane napade koji se šire mrežom bez određenog cilja. Potonju klasu napada, Huang i Behara (2013) nazivaju oportunistički napadi budući da ih napadači kreiraju s namjerom širenja zaraze na bilo koji dostupni informacijski sustav putem mreže.

3. Maksimizacija ekonomske koristi kao kriterij optimizacije ulaganja u kibernetičku sigurnost

Gordon i Loeb (2002) predstavljaju ekonomski model kojim određuju optimalni iznos ulaganja u informacijsku odnosno kibernetičku sigurnost. Model razmatra ranjivost na kibernetičke incidente te potencijalni gubitak koji rezultira kibernetičkim incidentom. Primjenjiv je na

ulaganja koja imaju različite ciljeve kao što su zaštita povjerljivosti, dostupnosti, vjerodostojnosti i integriteta podataka. Iako su autori svjesni mogućeg nesklada, odnosno sukoba koji se javlja među pojedinačnim ciljevima, model razmatra kako ranjivost podataka na propuste u sigurnosti i potencijalni gubitak utječu na odluku o raspodijeli resursa koji bi trebali promicati sigurnost. Rezultati istraživanja sugeriraju kako poslovne organizacije ne bi trebale svoja ulaganja resursa usmjeriti na zaštitu najranjivijih skupova podataka. Naime, zaštita izuzetno ranjivih skupova podataka može biti troškovno zahtjevna, stoga je za poslovnu organizaciju optimalno usmjeriti resurse na srednje ranjive skupove podataka. Nadalje, ukupna vrijednost ulaganja u sigurnost ne bi trebala iznositi iznad 36,8% očekivanog gubitka uzrokovanog narušenom povjerljivosti, dostupnosti, vjerodostojnosti ili integritetom podataka. Zaključeno je kako model pruža pogled iz ekonomske perspektive koja, u svrhu optimizacije ulaganja u sigurnost, ukazuje kako veća sigurnost, iako je to i cilj, nije uvijek opravdana u smislu porasta troškova koji proizlaze iz dostizanja višeg stupnja sigurnosti. Kritika modela jest da se ne bavi važnim aspektima odluka o ulaganju u informacijsku sigurnost, među kojima izdvajamo problem odlučivanja u jednom razdoblju što povlači pitanje kako pratiti dinamiku (promjenu) odluka. Nastavno na navedeno, sugerira se proširenje modela uz uvođenje više razdoblja u razmatranje. Na taj način bilo bi moguće razmotriti kako napadači na informacijski sustav mijenjaju napadačku strategiju kao reakciju na poduzeta ulaganja u informacijsku sigurnost.

Huang et al. (2008) predstavljaju model korisnosti od ulaganja u informacijsku sigurnost iz perspektive donositelja odluka, koji za razliku od Gordon-Loeb modela, pretpostavlja nesklonost donositelja odluka prema riziku. Na osnovi prospektne teorije autori sugeriraju kako će donositelji odluka neskloni riziku vjerojatnije ulagati u kibernetičku sigurnost kako bi smanjili rizike. Uporište u razmatranju modela koji pretpostavlja donositelja odluke nesklonom riziku pronalazi se i u agencijskoj teoriji koja navodi kako će nesklonost riziku biti izraženija u slučaju postojanja povezanosti osobnog bogatstva donositelja odluka s uspjehom poslovanja organizacije u kojoj je donositelj odluka zaposlen. Stoga razmatrani model, koji pretpostavlja averziju prema riziku te spremnost donositelja odluka na ulaganje u sigurnost, pruža dragocjen menadžerski uvid u to kako tvrtke trebaju donositi odluke pri ulaganju u sigurnost informacijskog sustava. Model pokazuje kako se ulaganje u informacijsku sigurnost nužno ne povećava s povećanjem averzije donositelja odluka prema riziku. Na tragu rezultata istraživanja Gordon i Loeb (2002), potvrđuje se kako optimalno ulaganje u kibernetičku sigurnost ne premašuje potencijalni gubitak koji nastupa uslijed sigurnosnog propusta. Pored toga, model ukazuje kako ulaganje u informacijsku sigurnost nije potrebno sve dok potencijalni gubitak nema značajnost za poslovnu organizaciju. Iz tog razloga donositelji odluka trebaju pažljivo procijeniti ranjivost svojih sustava i procijeniti potencijalne gubitke prije odluke o ulaganju u sigurnost.

Huang i Behara (2013) kritiziraju pretpostavke prethodnih studija u smislu kako je ograničavajuće pretpostavljati da se organizacije suočavaju s pojedinačnim napadom, odnosno da raspolažu neograničenim proračunom kojim financiraju aktivnosti zaštite od kibernetičkih rizika. U stvarnosti se poslovne organizacije često istovremeno suočavaju s različitim vrstama sigurnosnih izazova, gdje je svaki od izazova individualnih svojstava što zahtjeva različite pristupe održavanju kibernetičke sigurnosti. Uz spomenuto, sposobnost poslovne organizacije u financiranju sigurnosti i zaštite od rizika ograničena je sredstvima zbog čega autori razvijaju analitički model za raspodjelu ulaganja u sigurnost pod pretpostavkom postojanja ograničenog proračuna poslovne organizacije. Napade dijele prema prema karakteristikama

na ciljane i oportunističke (distribuirane napade). Rezultati istraživanja sugeriraju kako je za poslovnu organizaciju koja se suočava s ograničenjima proračuna namijenjenom održanju sigurnosti bolje da se veći dio, odnosno cijelo ulaganje usmjeri na zaštitu od jednog oblika napada. Ciljani napadi rezultiraju većim gubicima u odnosu na oportunističke napade iako su potonji učestaliji. Ranjivost na ciljane napade izraženije je što su informacijski sustavi više umreženi, odnosno otvoreniji. Stoga, donositelji odluka nužno trebaju usmjeriti ulaganje u sigurnost kako bi izbjegli ciljane napade na informacijske sustave. U slučaju ciljanih napada, optimalno ulaganje u sigurnost se povećava s većom ranjivosti sustava. Međutim, prije nego poslovna organizacija odluči uložiti resurse u vlastitu kibernetičku sigurnost potrebno je utvrditi kojim prijetnjama je izložena.

Nastavljajući se na pitanje različitih pretpostavki modela, Mayadunne i Park (2016) u svojoj studiji nude usporedbu odluka između donositelja odluka unutar poslovnih organizacija koji su skloni izlaganju riziku i onih koje su indiferentni prema riziku. Uočeno je kako se donositelji odluka koji su skloni riziku koncentriraju na zaštitu od onih rizika koji su frekventniji, ali čiji je intenzitet štete niži. S druge strane, donositelji odluka koji su indiferentni na rizik veću pažnju će posvetiti rizicima koji mogu rezultirati značajnim intenzitetom štete.

Predstavljeni radovi za cilj imaju optimizaciju ulaganja u kibernetičku sigurnost pomoću modelskog pristupa, međutim, razvoj modela pretpostavljen je uz ograničenja na koja treba naći odgovor. Primjerice donositelj odluka u poslovnim organizacijama svojim stavom prema riziku ne mora odgovarati profilu vlasnika i njegovom stavu prema riziku i stoga je korisno razmatrati model koji pretpostavlja sučeljene interese donositelja odluka unutar poslovnih organizacija i vlasnika poslovnih organizacija.

Jedno od ograničenja modela maksimizacije ekonomske koristi izostanak je informacija o interakciji između povezanih poslovnih organizacija i uvažavanja činjenice kako sigurnost poslovne organizacije ne ovisi samo o vlastito usvojenim mjerama i praksama sigurnosti. Zhao et al. (2013) naglašavaju kako svaka poslovna organizacija donosi odluku o ulaganju u vlastitu sigurnost. Međutim, sigurnost iste, razmatrane organizacije ne ovisi samo o usvojenim mjerama i praksama sigurnosti, nego i o odlukama ulaganja drugih povezanih poslovnih organizacija. Stoga je sugestija da modeli ulaganja u sigurnost trebaju obuhvatiti stratešku interakciju između povezanih poslovnih organizacija, a upravo je teorija igara prikladna za modeliranje interakcija između poslovnih subjekata. Sudionici unutar interakcije su poslovne organizacije koje se nastoje zaštiti od rizika te napadači koji imaju interes narušiti funkcioniranje informacijskog sustava napadnute poslovne organizacije. Alternativno, sudionike je moguće promatrati kao partnere, primjerice trgovac i dobavljač, koji pokušavaju pojedinačno ili zajednički zaštiti se od utjecaja kibernetičkih rizika.

4. Teorija igara kao koncept optimizacije ulaganja u kibernetičku sigurnost

Wu et al. (2015) primjenjuju teoriju igara s ciljem modeliranja optimalnog ulaganja u sigurnost, uvažavajući obilježja poslovne organizacije i uključujući njezino okružje koje je određeno, prvenstveno, partnerima s kojima dolazi do razmjene informacija. Modelom uvažavaju činjenicu kako se poslovne organizacije suočavaju s različitim vrstama napada. Sukladno prethodnim studijama, identificiraju ciljane i oportunističke napade s kojima se poslovne organizacije susreću.

Ono što je doprinos u odnosu na ranije istraživanja jest da model razmatra informacijske sustave međusobno povezanih tvrtki, što je pretpostavka koja bolje oslikava stvarni kontekst poslovnog okružja i načina na koji su postavljeni informacijski sustavi. Studijom se sugerira kako nije ekonomski opravdano zaštiti poslovnu organizaciju od svih kibernetičkih rizika. Naime, paralelno povećanje ulaganja u sigurnost s povećanjem potencijalnog gubitka nije opravdano, posebno kada je riječ o rizicima čiji razmjeri šteta mogu biti katastrofalni. Stoga je za poslovne organizacije sugestija koristiti druge mjere upravljanja rizicima, među kojima autori ovog rada ističu metodu prijenosa rizika. Pored toga, za poslovne organizacije bolje je da se ne ulaže u sigurnost dok potencijalni gubitak ne dosegne kritičnu razinu. U cilju optimizacije ulaganja u sigurnost ključno je provesti adekvatnu procjenu potencijalnih gubitaka i utvrđivanje prirode, odnosno obilježja prijetnje. Primjena zatvoreničke dileme prilikom odlučivanja o ulaganju u sigurnost nudi rješenje. Međutim, nužan uvjet je postaviti jasna pravila razmjene informacija te odgovornosti koja proizlazi iz međuovisnosti poslovnih organizacija, a koja nastupa razmjenom informacija. U tom smislu, međusobno povezane organizacije postižu višu razinu sigurnosti u poslovanju te smanjuju ukupne očekivane troškove. Sukladno rezultatima istraživanja, pokazalo se kako poslovne organizacije imaju više poticaja da zajednički odlučuju o ulaganjima kada se suočavaju s oportunističkom vrstom rizika. Kritika predstavljenog modela je da se ne razmatra ponašanje sudionika koji imaju namjeru narušiti sigurnost druge poslovne organizacije te se razmatra isključivo strana koja teži postići sigurnost. Nadalje, unutar modela izostaje pretpostavka kako napad, bez obzira je li riječ o ciljanom ili oportunističkom napadu, može nastupiti simultano.

Qian et al. (2017), vodeći se pretpostavkom kako ulaganje poslovne organizacije u sigurnost ne doprinosi isključivo sigurnosti vlastitog sustava, nego i sigurnosti sustava drugih poslovnih organizacija, razmatraju Nash-ovu ravnotežu. Potonja otkriva kako povećanje broja poslovnih organizacija u okružju, usprkos činjenici što isto povećava kibernetičku ranjivost, potiče poslovne organizacije na smanjeno ulaganje u sigurnost iz razloga što se u okružju pojavljuju „slobodni jahači". Pojava poslovnih organizacija koje se odlučuju na izostanak ulaganja u sigurnost narušava opću otpornost na kibernetičke prijetnje. Prisutnost „slobodnih jahača" podupire odluku o smanjenom ulaganju u sigurnost budući da je prisutna padajuća granična korist ulaganja koja je viša što je broj poslovnih organizacija u okružju veći. Iako model u suštini razmatra nedostatke povećanja poslovnog okružja u kojem se razmjenjuju informacije, što povećava ranjivost na kibernetičke rizike, model je moguće proširiti uzimajući u razmatranje koristi povećanja poslovnog okružja.

Prema Xu i Zhuang (2019), prethodno kreirani modeli optimizacije ulaganja, temeljeni na teoriji igara, pretpostavljaju jednaka obilježja među napadačima (hakerima), a pojednostavljena pretpostavka olakšava izradu modela i olakšava analizu. Međutim, u stvarnosti se napadači razlikuju sukladno svojim obilježjima. Primjerice razlikuju se prema sklonostima, interesima, resursima s kojima raspolažu i sl., a u tom slučaju sugerira se model koji pretpostavlja sekvencijalnu igru s potpunim informacijama koji obuhvaća više napadača. Uvođenjem modela koji uvažava pretpostavku heterogenosti napadača omogućava se optimizacija strategije ulaganja u sigurnost u situaciji kada su napadači različitih obilježja te kada je pretpostavka monolitnog igrača otklonjena. Modelom se razmatra jedan branitelj koji se obračunava s više napadača.

Li i Xu (2020) proučavaju izazove upravljanja sigurnosti u kontekstu upravljanja opskrbnim lancem. Studija potvrđuje kako poslovne organizacije unutar opskrbnog lanca trebaju

na odgovarajući način povećati ulaganja u kibernetičku sigurnost kada unutarnja ranjivost raste. Međutim, prevelika ranjivost dovodi do nedovoljnog ulaganja u kibernetičku sigurnost, pa tvrtke trebaju redizajnirati strukturu i hardversku konfiguraciju sustava. Tvrtke koje su u opskrbnom lancu s umjerenim brojem dobavljača trebale bi uložiti više sredstava u kibernetičku sigurnost u odnosu na velike tvrtke koje se povezuju s tisućama dobavljača, poput Amazon Inc. u kojoj je teško kontrolirati razinu sigurnosti. Vrijedi teza kako su poslovne organizacije otporne na kibernetičke rizike koliko je otporna njihova najslabija karika unutar opskrbnog lanca. Stoga, poslovna organizacija nužno treba uzeti u obzir ranjivosti svojih partnera s kojima ostvaruje suradnju, odnosno s kojima razmjenjuje informacije. Koordinirani pristup i odlučivanje vezano za sigurnost mogu učinkovito ublažiti negativne vanjske učinke i poboljšati razinu sigurnosti svih partnera u poslovnom okružju.

Nekoliko je budućih pravaca za istraživanje. Primjerice, model je moguće proširiti modeliranjem ponašanja između tvrtki i hakera kada su tvrtke međusobno povezane i hakeri dijele informacije. Buduća istraživanja trebala bi obuhvatiti pitanje poticajnih mehanizama kojima bi bilo moguće potaknuti poslovne organizacije na zajedničku odluku o koordiniranom ulaganju u sigurnost i razmjenu sigurnosnih podataka s ciljem postizanja većeg stupnja otpornosti na kibernetičke rizike.

Razmatrajući ulaganje u sigurnost kao metodu fizičke kontrole, ali istovremeno prateći promijene koje nastupaju u polju razvoja metoda financijske kontrole rizika, pomoću kojih je moguće rizik prenijeti na društva za osiguranje, pitanje upravljanja rizicima susreće se s izazovom; na koji način kombinirati upravljanje rizicima između različitih metoda kontrole? Proizvodi osiguranja od kibernetičkih rizika ni u kojem slučaju nisu zamjena za ulaganje u kibernetičku sigurnost, ali iste je moguće razmatrati kao nadopunu fizičkoj kontroli te kao faktor poticanja uspješnijeg upravljanju kibernetičkim rizicima. Prema OECD (2017), tržište osiguranja doprinosi boljem upravljanju kibernetičkim rizicima na način da dijeli stručne preporuke i savjete o upravljanju rizicima. Pored toga, važna uloga osiguranja ogleda se u korekciji premija osiguranja koja nastupa usvajanjem dobre prakse, odnosno provedenim ulaganjima u sigurnost.

5. Ulaganje u kibernetičku sigurnost i osiguranje

Prema Mukhopadhyay et al. (2005), ulaganje u sigurnost ne jamči potpuno sprječavanje utjecaj kibernetičkih rizika, stoga je korisno dio kibernetičkih rizika prenijeti na društva za osiguranje. Upravo Gordon et al. (2003) optimalno upravljanje kibernetičkim rizicima opisuju kao ono koje kombinira ulaganje u sigurnost i prijenos rizika na društva za osiguranje. Međusobnu povezanost metode fizičke kontrole, koja obuhvaća ulaganje u sigurnost, i metode financijske kontrole, koja obuhvaća prijenos rizika na društva za osiguranje istražuju Lelarge i Bolot (2008). Kombiniraju teoriju rizika i mrežnog modeliranja s ciljem razvoja modela očekivane korisnosti koja proizlazi iz odluke o prijenosu rizika. Prijenos rizika na društvo za osiguranje ističe se kao prikladno sredstvo za apsorbiranje financijskih gubitaka uzrokovanih kibernetičkim incidentom, a prema Böhme (2005) tržište osiguranja je poticajni čimbenik izgradnje sigurnog okružja.

Wang (2019) predstavlja model za optimizaciju ulaganja u kibernetičku sigurnost i osiguranje od kibernetičkih rizika. Modelom se kvantificira utjecaj ulaganja u sigurnost, provedenog s ciljem smanjenja utjecaja kibernetičkog događaja, prijetnje i ranjivosti i to na očekivane poslovne gubitke. Model omogućava optimalnu kombinaciju ulaganja u kibernetičku

sigurnost kroz razvoj i osposobljavanje zaposlenika, ali i ulaganje u mjere koje pomažu ublažiti izloženost riziku. Međutim, privatne koristi ulaganja su manje od društvenih koristi, što je objašnjeno pojavom „slobodnog jahača", čije značenje objašnjavaju Baer i Parkinson (2007) te Qian et al. (2017). Zbog navedenog opravdano je postaviti pitanje koji je motiv ulaganja poslovne organizacije u kibernetičku sigurnost ako se poslovno okružje ne ponaša jednako odgovorno prema riziku. Međutim, osiguranje od kibernetičkih rizika ne može osigurati apsolutnu supstituciju fizičke kontrole rizika, tj. ulaganja u sigurnost i to, prije svega, zato što izostanak inicijative osiguranika, prema ulaganju u sigurnost, narušava pretpostavku osigurljivosti te promiče problem moralnog hazarda.

Razmatranje kombinacije ulaganja u kibernetičku sigurnost i prijenosa rizika na društva za osiguranje, dovodi do pitanja kako postići opći napredak u kibernetičkoj sigurnosti ako su ulaganja nedovoljna? Prema Hofmann i Ramaj (2011), ulaganja u sigurnost su nedovoljna, a isto pretpostavlja izostanak stanja optimalne društvene sigurnosti. Jedan od razloga nedovoljnog ulaganja moguće je potražiti upravo u onim organizacijama koje na proizvode osiguranja gledaju kao na jedini način postizanja sigurnosti (situacija u kojoj ulaganje u sigurnost i osiguranje postaju supstituti) (Öğüt et al., 2011). Takvo ponašanje dovodi do stanja u kojem se police osiguranja kupuju u mjeri većoj od optimalne, a ulaganja u kibernetičku sigurnost su ispod optimalne razine. Stoga je važna uloga osiguratelja u smislu nagrađivanja nižom premijom onih osiguranika kod kojih postoji inicijativa za ulaganja u kibernetičku sigurnost.

6. Zaključak

Utjecaj kibernetičkih rizika na poslovne organizacije postaje sve izraženiji, stoga je sve prisutnija svijest o nužnosti postojanja kibernetički sigurnog okružja kod donositelja odluka u organizacijama. Potreba za upravljanjem kibernetičkim rizicima usmjerila je nastojanja istraživača prema razumijevanju istih rizika, metoda upravljanja i njihovog kombiniranja te optimiziranja uporabe resursa u cilju dostizanja željene razine kibernetičke sigurnosti.

Istraživanja u području kibernetičke sigurnosti mogu se razdijeliti prema kriteriju korištene metodologije u cilju optimizacije ulaganja u kibernetičku sigurnost u dva segmenta; istraživanja koja primjenjuju teoriju očekivane koristi odnosno istraživanja koja primjenjuju teoriju igara. Prvi segment pristupa analizi odluke o ulaganju u kibernetičku sigurnost temeljem teorije očekivane koristi što je tradicionalno prihvaćen model procjene ulaganja u kibernetičku sigurnost. Međutim, sigurnost poslovne organizacije ne ovisi samo o usvojenim mjerama i praksama sigurnosti, nego i o odlukama ulaganja drugih povezanih poslovnih organizacija. Stoga je sugestija da modeli ulaganja u sigurnost trebaju obuhvatiti stratešku interakciju između povezanih poslovnih organizacija, a upravo je teorija igara prikladna za modeliranje interakcija između poslovnih subjekata. Teorija igara je usmjerena na definiranje odluke o optimizaciji ulaganju uvažavajući akcije i reakcije poslovnih organizacija koje pokušavaju zaštiti svoju informacijsku imovinu i napadača koji namjeravaju narušiti pretpostavke kibernetičke sigurnosti. Teorija igara korisna je u smislu razmatranju ishoda i koristi donesene odluke u području kibernetičke sigurnost s obzirom na djelovanje (odluke) svih prisutnih aktera. Nadalje, korisna je u mogućnosti postavljanja specifičnih obilježja prisutnih aktera što ostavlja prostor za nastavak primjene teorije igara u optimiziranju odluka o ulaganju. Na tom tragu, za buduća istraživanja, predlaže se razvoj modela optimalnog ulaganja u kibernetičku

sigurnost koji pretpostavlja međusobnu povezanost više tvrtki, razmjenu informacija između napadača na informacijske sustave te definiranje poticajnih mehanizama kojima bi bilo moguće potaknuti poslovne organizacije na zajedničku odluku o koordiniranom ulaganju u sigurnost i razmjenu sigurnosnih podataka.

Upravljanje rizikom postaje presudan zadatak čijim se izvršenjem umanjuje negativan utjecaj rizika, realizacija kojih predstavlja opterećenje u odvijanju poslovnih procesa te ugrozu za poslovanje. Prevencija velikih gubitaka, koji se mogu dogoditi zbog kibernetičkog napada ili kvarova unutar informacijskog sustava, obično je povezana s kontinuiranim ulaganjem u različite sigurnosne mjere. Ulaganje u kibernetičku sigurnost iziskuje angažman resursa, koji je s ekonomskog gledišta nužno optimizirati. Međutim, bez obzira koliko iscrpan angažman resursa pretpostavili, u razvoj kibernetičke sigurnosti, apsolutnu sigurnost nije moguće postići. Stoga, metodu fizičke kontrole treba kombinirati s metodom financijske kontrole koja uključuje odluku o prijenosu rizika na društva za osiguranje. Kombiniranje navedenih metoda pruža rješenje u postizanju cilja, a riječ je o postignutoj kibernetičkoj sigurnosti. S obzirom na recentna društvena zbivanja i utjecaj pandemije COVID-19, poslovne organizacije suočavaju se s izazovom dislociranja zaposlenika, ključnih nositelja poslovnih procesa, na rad od kuće. Navedene promijene pretpostavljaju ubrzanu digitalizaciju, ali promiču važnost upravljanja kibernetičkim rizicima te brigu o kibernetičkoj sigurnosti kao nikada do sada. Postavljanje strategija upravljanja kibernetičkim rizicima odnosno njihova prilagodba novim uvjetima poslovanja iziskivat će nikad veću pažnju i interes odgovornih pojedinaca u poslovnim organizacijama. Na tom tragu, predlaže se buduće istraživanje koje će razmatrati odluke o ulaganju u kibernetičku sigurnost odnosno njegovom kombiniranju s metodom prijenosa rizika u novim okolnostima koji potiče ranjivost poslovnih organizacija na kibernetičke rizike.

LITERATURA

1. Aldasoro, I.; Gambacorta, L., Giudici, P. i Leach, T. (2020.) The drivers of cyber risk, *BIS Working Papers*, Br. 865, str. 1-45
2. Allianz Global Corporate & Speciality (2020.) Allianz Risk Barometer - Identifying the Major Business Risks for 2020, http://www.agcs.allianz.com/assets/PDFs/Reports/AllianzRiskBarometerTop-BusinessRisks2016.pdf. (pristup: 27.8.2020.)
3. Alter, S. i Sherer, S. A. (2004.) A general, but readily adaptable model of information system risk, *The Communications of the Association for Information Systems*, God. 14., str. 1-28
4. AON (2019.) Intangible Assets Financial Statement Impact Comparison Report, Independently conducted by Ponemon Institute LLC, https://www.aon.com/getmedia/52401ebe-c9e7-4fe0-a2f0-f77a210aac6b/2019-Intangible-Assets-Financial-Statement-Impact-Comparison-Report.aspx (pristup: 18.9.2020.)
5. Ashby, S.; Buck, T., Nöth-Zahn, S. i Peisl, T. (2018.) Emerging IT risks: insights from German banking, *The Geneva Papers on Risk and Insurance-Issues and Practice*, God. 43., Br. 2, str. 180-207
6. Baer, W. S. i Parkinson, A. (2007.) Cyberinsurance in it security management, *IEEE Security & Privacy*, God. 5., Br. 3, str. 50-56
7. Biener, C., Eling, M. i Wirfs, J. H. (2015.) Insurability of cyber risk: An empirical analysis, *The Geneva Papers on Risk and Insurance-Issues and Practice*, God. 40., Br. 1, str. 131-158

8. Böhme, R. (2005.) Cyber-Insurance Revisited, *Workshop on the Economics of Information Security (WEIS),* Harvard University, Cambridge, MA, str. 14–17, http://infosecon.net/workshop/pdf/15.pdf (pristup: 10.9.2020.)
9. Cebula, J. L. i Young, L. R. (2010.) A taxonomy of operational cyber security risks, Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst, https://apps.dtic.mil/dtic/tr/fulltext/u2/a537111.pdf (pristup: 10.7.2020.)
10. CERT (2016.) Osnovni pojmovi kibernetičke sigurnosti, https://www.cert.hr/wp-content/uploads/2009/07/Pojmovnik.pdf (pristup: 10.9.2020.)
11. Ćurak, M. (2019.) Kibernetički rizici iz perspektive osiguranja, U: Rimac Smiljanić, A., Šimić Šarić, M.; Visković J. (ur.), *Financijska kretanja - najnoviji događaji i perspective*, Sveučilište u Splitu, Ekonomski fakultet, Split, str. 351-376
12. Deloitte (2020.) Reshaping the cybersecurity landscape, https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html#endnote-sup-2 (pristup: 18.9.2020.)
13. Eling, M. i Schnell, W. (2016.) What do we know about cyber risk and cyber risk insurance?, *The Journal of Risk Finance*, God. 17., Br. 5, str. 474-491
14. Gordon, L. A. i Loeb, M. P. (2002.) The economics of information security investment, *ACM Transactions on Information and System Security (TISSEC)*, God. 5., Br. 4, str. 438-457
15. Gordon, L. A., Loeb, M. P. i Sohail, T. (2003.) A framework for using insurance for cyber-risk management, *Communications of the ACM*, God. 46., Br. 3, str. 81-85
16. Harrington, S. E. i Niehaus, G. (2004.) *Risk management and insurance*, McGraw-Hill, Irwin
17. Hofmann, A. i Ramaj, H. (2011.) Interdependent risk networks: the threat of cyber attack, *International Journal of Management and Decision Making*, God. 11, Br. 5, str. 312-323
18. Huang, C. D. i Behara, R. S. (2013.) Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints, *International Journal of Production Economics*, God. 141., Br. 1, str. 255-268
19. Huang, C. D., Hu, Q., i Behara, R. S. (2008.) An economic analysis of the optimal information security investment in the case of a risk-averse firm, *International journal of production economics*, God. 114., Br. 2, str. 793-804
20. Jalali, M. S., Siegel, M. i Madnick, S. (2018.) Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment, *The Journal of Strategic Information Systems*, God. 28., Br. 1, str. 66-82
21. Lelarge, M. i Bolot, J. (2008.) A local mean field analysis of security investments in networks. In *Proceedings of the 3rd international workshop on Economics of networked systems,* str. 25-30, https://dl.acm.org/doi/pdf/10.1145/1403027.1403034 (pristup: 10.9.2020.)
22. Li, Y. i Xu, L. (2020.) Cybersecurity investments in a two-echelon supply chain with third-party risk propagation, *International Journal of Production Research*, str. 1-23
23. Madnick, S. (2017.) Preparing for the cyberattack that will knock out US power grids. *Harvard Business Review*, str. 1-10
24. Marotta, A., Martinelli, F., Nanni, S., Orlando, A. i Yautsiukhin, A. (2017.) Cyber-insurance survey, *Computer Science Review*, Br. 24., str. 35-61

25. Mayadunne, S. i Park, S. (2016.) An economic model to evaluate information security investment of risk-taking small and medium enterprises, *International Journal of Production Economics*, Br. 182., str. 519-530
26. Morgan, S. (2019.) Official Annual Cybercrime Report. Report by Cybersecurity Ventures Sponsored by Herjavec Group, https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/ (pristup: 16.8.2020.)
27. Mukhopadhyay, A.; Saha, D., Chakrabarti, B. B., Mahanti, A., i Podder, A. (2005). Insurance for cyber-risk: A Utility Model. *Decision*, God. 32., Br. 1, str. 153-169
28. OECD (2017.) Types of cyber incidents and losses. In enhancing the role of insurance in cyber risk management. OECD Publishing, https://www.oecd.org/daf/fin/insurance/Enhancing-the-Role-of-Insurance-in-Cyber-Risk-Management.pdf (pristup: 5.9.2020.)
29. Öğüt, H.; Raghunathan, S., i 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*, God. 31., Br. 3, str. 497-512
30. Phonemon Institute (2020.) Cost of Data Breach Report 2020, https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/ (pristup: 5.9.2020.)
31. Price Waterhouse Coopers (2018.) Strengthening Digital Society against Cyber Shocks: Key Findings from The Global State of Information Security ® Survey 2018, https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey/strengthening-digital-society-against-cyber-shocks.html (pristup: 18.9.2020.)
32. Qian, X.; Liu, X., Pei, J., Pardalos, P. M. i Liu, L. (2017.) A game-theoretic analysis of information security investment for multiple firms in a network, *Journal of the Operational Research Society*, God. 68., Br. 10, str. 1290-1305
33. Roy, S.; Ellis, C., Shiva, S., Dasgupta, D., Shandilya, V. i Wu, Q. (2010). A survey of game theory as applied to network security. In *2010 43rd Hawaii International Conference on System Sciences,* Honolulu, HI, str. 1-10
34. RSA (2016.) Cyber Risk Appetite: Defining and Understanding Risk in the Modern Enterprise, https://www.rsa.com/content/dam/en/white-paper/cyber-risk-appetite.pdf (pristup: 19.9.2020.)
35. Sokri, A. (2020.) Game Theory and Cyber Defense, *International Series in Operations Research & Management Science*, God. 280., str. 335-352
36. Wang, S. S. (2019.) Integrated framework for information security investment and cyber insurance, *Pacific-Basin Finance Journal*, God. 57., Br. 101173, str. 1-12
37. Wu, Y., Feng, G., Wang, N. i Liang, H. (2015.) Game of information security investment: Impact of attack types and network vulnerability, *Expert Systems with Applications*, God. 42., Br. 15-16, str. 6132-6146
38. Xu, Z. i Zhuang, J. (2019.) A study on a sequential one-defender-N-attacker game, *Risk Analysis*, God. 39., Br. 6, str. 1414-1432
39. Zhao, X.; Xue, L. i Whinston, A. B. (2013.) Managing interdependent information security risks: Cyberinsurance, managed security services, and risk pooling arrangements, *Journal of Management Information Systems*, God. 30., Br. 1, str. 123-152

Summary

CYBER SECURITY INVESTMENT

Accelerated development of technologies and their more frequent application within business organizations create numerous advantages in terms of speed of execution and automation of business processes, easier access and exchange of information, performing business activities remotely, easier access to markets, reducing business costs, etc. At the same time, business organizations are exposed to cyber risks and threats that are becoming more diverse, more complex and are growing steadily. Various forms of cyber risks are manifested through the compromise of information systems of business organizations, which can cause significant direct and indirect financial losses. Although there are growing vulnerabilities to cyber risks, especially in terms of their intensity of impact on the operations of organizations, there is still a lack of cyber security management activities. Many business organizations ignore or underestimate cyber risks or rely on generic security products. Despite the fact that cyber risks are becoming an increasingly important factor influencing the operations of organizations and their performance, research in the economic literature and in its narrower field of risk management is not adequately represented. The aim of this paper is to provide an overview of research in the field of investing in cyber security as a loss control, which is an indispensable prerequisite for confidentiality, availability and integrity of information and information systems. Furthermore, the aim of this paper is to compare investment in cyber security with the method of financial control and emphasize the importance of combining these two methods in achieving cyber security.

Keywords: *cyber security, cyber risks, security investment, loss control.*