Stručni članak
Primljeno: 31. listopada 2023.
https://doi.org/10.46672/zsl.8.9.15

Ivan Rudeš*
Ivan Pavelić**

CYBER-RIZIK, FENOMEN KOJI POSTOJI I UGROŽAVA NAS

Sažetak

Svijet i okruženje u kojem se danas živi i u kojem se obavlja veliki broj aktivnosti puni su izazova i prijetnji. Prije razvoja modernih digitalnih i komunikacijskih tehnologija pojedinci, kompanije, organizacije, davatelji javnih usluga i sl. bili su izloženi samo fizičkim (opipljivim ili vidljivim) rizicima. Unazad par desetljeća, kao i danas, pojedinci i kompanije izloženi su možda i opasnijim rizicima koji prijete u kibernetičkom (engl. *cyber*) svijetu te je potrebno naći način kako upravljati tim rizicima, poduzeti sve aktivnosti da se ti rizici svedu na minimum, a ako je to nemoguće, osigurati se s ciljem da bi se život, odnosno poslovanje moglo normalno nastaviti. U radu će se pokazati da je upravljanje *cyber*-rizicima još u ranoj fazi svog postojanja, pa mnoge kompanije i pojedinci nemaju dovoljno znanja o tome kako njima upravljati ili smatraju da je upravljanje takvim rizicima, odnosno osiguranje od takvih rizika nepotrebno. Iskustva koja su pojedine kompanije i državne institucije proživjele pokazuju da su *cyber*-rizici stvarni, te da je upravljanje tim rizicima, odnosno osiguranje od njih danas ključno u održavanju stabilnog poslovanja za sebe, ali i za sve klijente koji sudjeluju u cijelom procesu poslovanja. *Cyber*-napadi mogu paralizirati kompaniju, ponekad je čak i uništiti, te imajući to u vidu, potrebno se osigurati od takvih rizika, a isto tako osigurati i odgovornost prema klijentima kojima zbog takvih napada može nastati šteta.

Ključne riječi: kibernetički rizici, *cyber*-rizici, upravljanje rizicima, osiguranje *cyber*-rizika

1. Uvod

Sve veći utjecaj globalizacije i međusobne povezanosti u poslovanju doveo je do ubrzanog razvoja tehnologije, što je značajno povećalo kompleksnost, ali i međusobnu ovisnost različitih tehnologija. Virtualna je zaštita pod najvećim pritiskom do sada da izvršava svoju zadaću zaštite podataka, informacija itd. No, ponekad ta zaštita ne uspije odoljeti *cyber*-rizicima, te zbog toga *cyber*-osiguranja koja nude osiguravajuća društva moraju biti izrazito kvalitetna i širokih pokrića da bi se sačuvala sigurnost i

* Ivan Rudeš, bacc. oec, Zagreb, Hrvatska, ivan.rudes1@gmail.com
** mr. sc. Ivan Pavelić, Libertas međunarodno sveučilište, ipavelic@libertas.hr

stabilnost poslovanja. Da bi se u potpunosti ili djelomično ublažile posljedice štetnoga događaja (jer osiguranja, nažalost, ne mogu garantirati da se šteta neće dogoditi), osiguranje bi trebalo dati kvalitetno pokriće za takve rizike, odnosno pod određenim uvjetima preuzeti takve rizike od klijenta.

Predmet istraživanja u ovom je radu utvrđivanje aktivnosti i mjera koje se trebaju provesti s ciljem izbjegavanja štete koja može nastati realizacijom *cyber*-rizika. Menadžeri koji su poslovanje organizirali u *cyber*-području, a nisu poduzeli sve mjere zaštite u tom području, nisu svjesni kojim su sve rizicima izložili svoju kompaniju. Stoga je prvi korak prihvatiti činjenicu da *cyber*-rizici postoje, a drugi bi korak bio shvaćanje da se od takvih rizika moguće i potrebno braniti.

Stoga je postavljeno glavno istraživačko pitanje: jesu li *cyber*-rizici samo neizbježna posljedica digitalizacije na koju se moramo bespomoćno priviknuti ili su to rizici od kojih se možemo kvalitetno zaštititi procesom upravljanja takvim rizicima.

Također će se prokomentirati neki od poznatih slučajeva *cyber*-rizika, prikazati kolike su vjerojatnosti da se određeni *cyber*-rizik dogodi te koliko često su se ti rizici realizirali.

Cilj je rada doprinijeti razvoju svijesti o činjenici opasnosti od *cyber*-rizika, pokazati važnost shvaćanja da je postupak upravljanja rizikom jako bitan u svakodnevnom životu i poslovanju te analizirati koliko je osiguranje od posljedica realizacije takvih rizika bitno ako se ne zna njima upravljati. Svaka, pa i najmanja šteta koja nastane realizacijom *cyber*-rizika može biti presudna u poslovanju kompanije jer je svaka kompanija na svoj specifičan način osjetljiva na realizaciju *cyber*-rizika (stvarni i reputacijski rizik).

Tema je rada aktualna zato što, s jedne strane, većina vlasnika i menadžera u malim i srednjim poduzećima nema ni znanja za prepoznavanje rizika niti zna upravljati takvim rizicima te nemaju razvijenu svijest o načinima osiguranja od posljedica koje mogu nastati realizacijom *cyber*-rizika. S druge strane, velik dio poslovanja organiziran je putem digitalnih platformi u *cyber*-svijetu. Ovaj je rad namijenjen upravo navedenoj kategoriji menadžera, kao i studentima koji će jednog dana završiti svoje akademsko obrazovanje te se naći u situaciji upravljanja procesima, ljudima i kompanijama. Naime, proces upravljanja rizikom (u nastavku i osiguranje od rizika kojima menadžeri ne mogu ili ne znaju upravljati) iznimno je bitan, a možebitno i presudan u svakodnevnom životu i poslovanju.

U teorijskom dijelu rada pojasnit će se koncepti kao što su rizik općenito te *cyber*-rizici i posljedice koje mogu uzrokovati, zatim upravljanje rizicima i *cyber*-rizicima, kao i osiguranje *cyber*-rizika kao zadnji korak u procesu upravljanja *cyber*-rizicima.

2. Rizik

Do danas nema jedinstvene definicije rizika, nego ga svaki autor definira ovisno o djelatnosti i okolnostima u području proučavanja. Tako rizik neki autori (Matić, 2016: 205) definiraju kao opasnost od gubitka uloženih sredstava i/ili poslovnoga ugleda; drugi pak autori u prvi plan stavljaju neizvjesnost, pa rizik definiraju kao određenu i mjerljivu neizvjesnost, a treći ga definiraju kao opasnost od donošenja pogrešne odluke, odnosno kao opasnost donošenja odluke koja ne bi bila optimalna u odnosu na odabrane ciljeve.

S obzirom na to da je rad vezan za osiguranje, rizik se definira kao stanje u kojem postoji mogućnost negativnog odstupanja od poželjnog ishoda koji očekujemo ili kojemu se nadamo (Andrijanić i Klasić, 2002).

Svaka ljudska aktivnost ili situacija u kojoj se pojedinac nađe sadrži u sebi određeni rizik, a rizik sadrži i svaka poslovna aktivnost ili poslovna situacija u kojoj se poduzeće nađe. Pojedinac, naravno, može minimizirati rizike racionalnim ponašanjem ili poduzimanjem različitih radnji koje smanjuju mogućnost realizacije nekog od rizika. Ono što je potrebno jest da je ta osoba svjesna postojanja rizika i da je upoznata s procesom upravljanja njima.

Koncept rizika ima tri nužna elementa:

- percepciju o tome može li se neki štetan događaj zaista dogoditi
- vjerojatnost da će se on zaista dogoditi i
- posljedice štetnog događaja koji bi se mogao dogoditi (Kereta, 2004).

Rizik je, dakle, rezultat sinergije interakcija ovih triju elemenata.

S obzirom na to da postoji veliki broj definicija rizika, tako postoji i veliki broj podjela rizika.

U međunarodnom poslovanju vrlo je važna podjela rizika na prenosive i neprenosive, osigurljive i neosigurljive te subjektivne i objektivne rizike (Matić, 2004: 370).

- **prenosivi rizici** – rizici za koje je moguće utvrditi vjerojatnost nastupa i visinu štete, pa se rizik može prenijeti na druge subjekte; neki od prenosivih rizika su: valutni, transportni, ratni i politički rizik
- **neprenosivi rizici** – rizici za koje nije moguće odrediti vjerojatnost nastupa ni visinu moguće štete, stoga ih nije moguće prenijeti na druge subjekte; u neprenosive rizike ubrajamo rizike ljudskog faktora
- **osigurljivi rizici** – rizici od kojih se možemo osigurati, a u njih ubrajamo: osobni, imovinski rizik i rizik od odgovornosti za štete na imovini, zdravlju ili životu treće osobe
- **neosigurljivi rizici** – nepredvidljivi i katastrofični rizici na koje pojedinac nije mogao utjecati, pa ih ne može ni osigurati

- **subjektivni rizici** – nastaju kao posljedica subjektivne volje čovjeka, teško su predvidljivi i mjerljivi, stoga nisu osigurljivi; tipičan su primjer subjektivnih rizika spekulativni rizici
- **objektivni rizici** – rizici na koje pojedinac ne može utjecati, ali ih lako može izmjeriti, odrediti učestalost nastupa te visinu prosječne štete; to su ujedno i osigurljivi rizici.

2.1. Hazard

Hazard je, za razliku od rizika, stanje, uvjet ili ponašanje koje stvara ili povećava vjerojatnost nastanka štete (realizaciju rizika). Tako je, na primjer, hazard ako netko svjesno krši prometna pravila i vozi brzinom koja nije preporučena ili ako netko puši u prostorijama u kojima je strogo zabranjeno pušenje jer bi moglo doći do zapaljenja i eksplozije. Pojednostavljeno, hazard prethodi opasnosti koja može utjecati na pojedinca, opasnost prethodi izloženosti riziku, a izloženost riziku vodi k rizičnom događaju.

Hazard se može podijeliti u tri kategorije (Klobučar, 2007: 9):

- **fizički hazard** – predstavlja fizičke karakteristike koje povećavaju nastanak štetnog događaja; neki od primjera su zaleđena cesta koja može rezultirati klizanjem i nezgodom automobila ili neispravne električne instalacije koje mogu rezultirati požarom
- **moralni hazard** – obuhvaća sve nemoralne i nečasne radnje kojima pojedinac omogućava nastajanje štetnog događaja, odnosno svi pokušaji pojedinca da prevari osiguravajuće društvo; najbolji primjeri ovakvog hazarda su namjerno izazivanje prometnih nezgoda, nerazumni zahtjevi za isplatama šteta i sl.
- **hazard *Morale*** – iako ima sličan naziv kao prijašnja vrsta hazarda, ovaj hazard zapravo označava indiferentnost pojedinaca/osiguranika prema štetama koje im se događaju.

2.2. *Cyber*-rizici

Polazeći od navedene definicije rizika, *cyber*-rizici mogu se definirati kao rizici koji su povezani s aktivnostima na internetu, kao što su internetsko trgovanje, plaćanje internetom, ali i pohrana podataka, a koji mogu rezultirati štetom za neku kompaniju.

Razlikujemo sljedećih osam kategorija *cyber*-rizika (Olsen, 2013):

1. **hakerski napad** – svaki napad koji izvršava haker prema pojedincu ili kompaniji i kojemu je cilj prodrijeti kroz sustav zaštite da bi se na određeni način naštetilo kompaniji (krađa podataka, postavljanje virusa i sl.)
2. **povreda podataka** – svaki sigurnosni incident u kojem neovlaštena osoba ilegalnim metodama pristupa osjetljivim i povjerljivim podacima drugih osoba, kao što su brojevi bankovnih računa ili zdravstveni podaci (IBM)

3. **prijenos virusa** – proces u kojemu je namjera hakera ubaciti računalni program kojem je cilj „zaraziti" druge programe i tako im nanijeti štetu na način da se svaki program koji bude zahvaćen virusom pretvara u sam virus
4. ***cyber*-iznuda** – najjednostavnije rečeno, kriminalna radnja u kojoj napadači uspiju dohvatiti nečije osobne ili financijske podatke te prijete da će vlasnicima podataka nanijeti štetu u slučaju da ne ispunite njihove zahtjeve
5. **sabotaža zaposlenika** – najčešće je riječ o propustima zaposlenika u poslovanju i korporativna špijunaža kao jedan od mogućih rizika koji svaka kompanija može i mora očekivati da bi joj se mogao dogoditi
6. **prekid rada mreža** – vremenski period u kojem je poslovna mreža subjekta nedostupna za normalan rad i u kojoj mreža gubi svoju primarnu funkciju; pad mreže može biti uzrokovan vanjskim prijetnjama kao što je hakiranje, ali i štetom nastalom na programskoj podršci i računalnoj opremi; ovaj rizik može imati veliki utjecaj na produktivnost kompanije, ali ponajviše na nezadovoljstvo kupaca
7. **multimedijska odgovornost** – rizik u kojemu dolazi do kršenja različitih autorskih prava, plagijat, kleveta itd.
8. **ljudska greška** – rizik u kojemu zaposlenik krivom radnjom može nanijeti štetu kompaniji, a da to nije bila njegova prvotna zamisao; ljudska pogreška ne smatra se namjernim izazivanjem štete, nego nastaje kao posljedica ljudske pogrešivosti.

2.2.1. Karakteristike cyber*-rizika i postupak nastanka štetnog događaja*

Postupak nastanka *cyber*-rizika u osnovi je vrlo jednostavno opisati kao rizik koji vodi k štetnom događaju, a vezan je za digitalnu tehnologiju. Postavlja se pitanje komu je u interesu napraviti štetu nekoj kompaniji? Kao što je već navedeno, kompanije su na virtualnom tržištu izložene *cyber*-rizicima, a u virtualnom svijetu postoje pojedinci i skupine koji žele nanijeti štetu kompanijama ili pojedincima tako da ukradu privatne podatke ili virtualnu imovinu, kao što je neko intelektualno vlasništvo ili čak kriptovalute i tako u pravilu za sebe ostvaruju neku korist. Primjeri osoba koji rade takve radnje su: „haktivisti", pojedinačni hakeri i hakerske organizacije te špijuni.

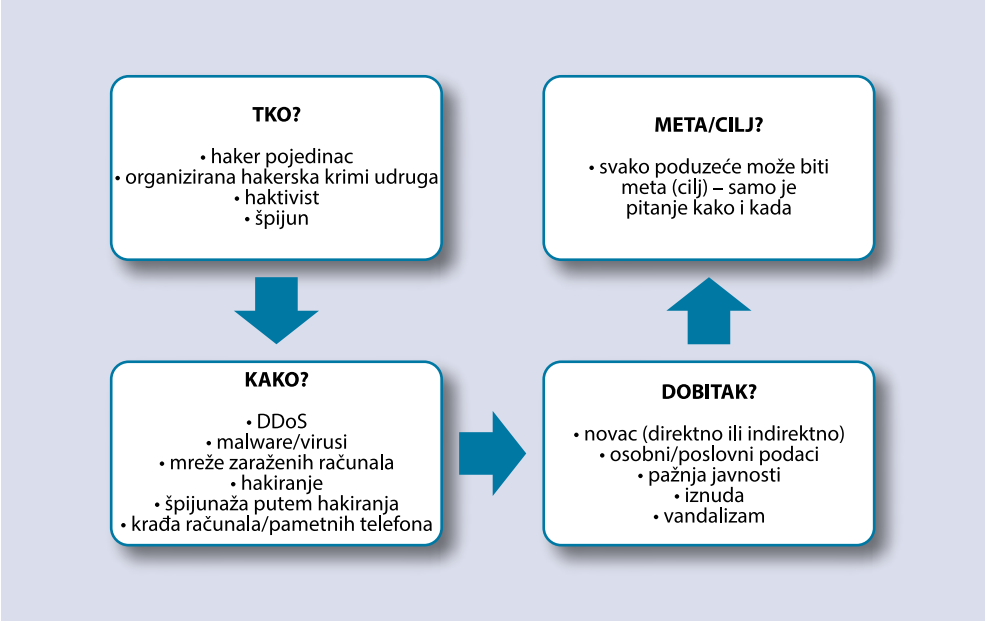
Bitno je objasniti kako nastaju štetni događaji, odnosno šteta kada dođe do realizacije nekog od *cyber*-rizika. Štetni događaji mogu nastati putem hakiranja poslovnih ili operativnih sustava. Nadalje, štetan događaj može nastati krađom računala/pametnih telefona i taj se štetni događaj može izvesti u fizičkom obliku, ali i u virtualnom jer je moguće klonirati uređaj i prenijeti sve podatke na drugo računalo (najčešće računalo hakera). Špijunaža je jedan od štetnih događaja koji može rezultirati velikim financijskim gubicima jer se vrlo lagano može doći do povjerljivih informacija kompanija, koje vrlo često vrijede veliku svotu novca. Zadnje dvije

metode su DDoS i zlonamjerni programi (engl. *malware*). DDoS je napad s ciljem ometanja mrežnih usluga u pokušaju iscrpljivanja resursa aplikacije (Microsoft, 2023a). *Malware* se odnosi na zlonamjerne aplikacije ili kôd koji oštećuje ili ometa normalno korištenje uređaja krajnjih točaka. Kada se uređaj zarazi zlonamjernim programom, može doći do neovlaštenog pristupa, ugrožavanja podataka ili blokiranja pristupa uređaju ako ne platite otkupninu (Microsoft, 2023b).

Kao što je već navedeno, posljedica je takvih napada nastajanje štete osiguraniku. Razlozi ovakvih napada najčešće su novac, odnosno želja za zaradom s pomoću pribavljanja privatnih podataka tako da se ti podatci mogu prodati trećoj strani koja ima poslovni interes za njihovo posjedovanje. Osim toga razlog napada može biti i vandalizam, tj. isključivo izazivanje štete (bila ona fizička, digitalna ili čak reputacijska), bez obzira na korist koju napadač može imati.

Takvi se štetni događaji mogu dogoditi bilo kojoj osobi ili kompaniji, samo je pitanje kada i kako će se napad dogoditi te kakve će posljedice imati.

Shematski prikaz procesa nastanka štetnog događaja zorno je prikazan na Slici 1.



Slika 1. Prikaz nastanka štetnog događaja (izvor: Olsen, 2013)

2.2.2. Kategorije gubitaka koje mogu nastati realizacijom cyber*-rizika*

Svi gubitci koji mogu nastati prilikom nastupanja štetnog događaja dijele se u 11 kategorija (Marsh, 2015):

1. **krađa intelektualnoga vlasništva –** gubitak imovinske vrijednosti intelektualnog vlasništva, što najčešće rezultira smanjenim prihodom na tržištu ili potpunim gubitkom prihoda
2. **prekid poslovanja –** prekid poslovanja ne znači nužno zatvaranje kompanije iako to može biti posljedica *cyber*-napada ako nanesena šteta bude prevelika, ali primarno se radi o izgubljenoj vrijednosti koja nastaje prilikom napada na kompaniju i zbog koje informacijsko-komunikacijski sustav prestaje raditi (sustav uopće ne funkcionira ili se određeni podatci ne mogu dohvatiti)
3. **gubitak podataka i aplikacija –** trošak koji nastane prilikom obnavljanja pojedinih podataka ili cijeloga informacijskog sustava koji je izbrisan ili „korumpiran"
4. ***cyber*-iznuda –** ovaj gubitak podrazumijeva trošak koji kompanija ili pojedinac moraju platiti da bi vratili određene podatke/datoteke od iznuditelja, ali i sve troškove osobe/osoba koja rukovode incidentom *cyber*-iznude
5. ***cyber*-prijevara –** izravni financijski gubitak koji nastaje prilikom krađe novca (prijevare), vrijednosnih papira ili bilo koje druge imovine; ovaj gubitak podrazumijeva da se koristi računalo u izvršenju zlonamjerne aktivnosti
6. **događaj povrede privatnosti –** svi troškovi vezani za istraživanje i traženje odgovora za povredu privatnosti, uključujući informacijsko-komunikacijsku forenziku te odgovornost za potraživanja trećih strana koja proizlaze iz tog incidenta
7. **mrežne pogreške –** obveze trećih strana koje su odgovorne za sve obveze koje proizlaze iz nekih sigurnosnih događaja koji se javljaju u organizaciji informacijsko-komunikacijske mreže ili iz nje proizlaze s namjerom napada na treću osobu
8. **utjecaj na reputaciju –** svi gubitci koji nastaju nastupanjem štetnoga događaja, a koji narušavaju reputaciju kompanije i rezultiraju gubitkom baze kupaca, što za posljedicu ima gubitak ili smanjenje prihoda
9. **fizičko oštećenje imovine –** gubitak prve strane koji je rezultat *cyber*-napada
10. **smrt i tjelesna ozljeda –** odgovornosti trećih osoba za tjelesnu ozljedu ili smrt pojedinaca koje su nastale prilikom *cyber*-napada
11. **istraživanje incidenata i troškovi odgovora –** svi izravni troškovi koji su nastali istraživanjem i zatvaranjem incidenta te smanjivanje gubitka nakon incidenta; odnosi se na sve prijašnje događaje.

Nadalje je bitno napomenuti da kompanije ili državne institucije nisu jedine koje mogu biti podložne napadu jer informacije, koje hakeri mogu dobiti i od drugih, mogu biti važne neovisno o njihovoj vrsti. Štoviše, hakerima su često puno zanimljivije manje kompanije i informacije vezane za njih jer je puno veća vjerojatnost da takve pravne osobe imaju značajno manju razinu *cyber*-zaštite, odnosno nemaju razvijenu strategiju *cyber*-sigurnosti kao velike kompanije. Takve kompanije u pravilu imaju i manje razine transkripcije i manjak informacijsko-komunikacijskih stručnjaka, što

ih čini gotovo savršenim kandidatima za *cyber*-napad, ali isto tako i kandidatima za *cyber*-osiguranje.

Manje kompanije, s aspekta *cyber*-sigurnosti, mogu predstavljati veliki rizik i ozbiljan problem velikim kompanijama jer ako one u svom portfelju imaju dio poslovanja neke velike kompanije, mogu napadačima pružiti svojevrsna „stražnja vrata" za ulazak na unosnije tržište (Bara, 2015).

3. Upravljanje rizikom

Sve su pravne i fizičke osobe podložne nastanku štete putem realizacije nekog od rizika kojima je njihovo poslovanje izloženo, neovisno o tome je li riječ o velikoj ili manjoj kompaniji, pojedincu ili pak samoj državi.

Slično kao i kod definicije rizika, odnosno vrsta rizika, postoji više definicija procesa upravljanja rizikom, kao što je pregledno prikazano u Tablici 1.

Tablica 1. Različite definicije pojma upravljanja rizikom

British Standard	Steve Frostdick	College Simmons	Stipe Baljkas	Jonathan Strutt	Marko Bešker
identifikacija rizika	identifikacija rizika	identifikacija rizika	identifikacija rizika	identifikacija rizika	analiza i procjena rizika
analiza rizika	kvantifikacija rizika	procjena vjerojatnosti	procjena rizika	procjena rizika	izrada plana i priprema
postavljanje kriterija	postojanje praga tolerancije	razvoj *risk*-menadžment planova	upravljanje rizicima	postojanje praga tolerancije	implementacija plana
postavljanje praga tolerancije		praćenje *risk*-menadžment napora	kontrola rizika	iznalaženje metoda za snižavanje rizika	vrednovanje i kontrola
			završna analiza		poboljšanje procesa

Izvor: Drljača i Bešker (2020)

U upravljanju rizikom postoje četiri bitna koraka koji se moraju provesti da bi se ispravno proveo cijeli proces (Klobučar, 2007):

1. **Identifikacija potencijalnog gubitka.** U prvome se koraku istražuje koji su rizici prijetnja, odnosno koji bi rizici mogli rezultirati štetnim događajem prilikom poslovanja. Takvi gubitci mogu biti imovinske prirode, odnosno gubitak prihoda ili gubitak imovine, smrt, prijevara, gubitak i krađa informacija. Najbolji je način kako identificirati potencijalne gubitke taj da se provede inspekcija onoga što se želi osigurati, npr. zgrade, informacijskog sustava, baze i sl.

2. **Evaluacija potencijalnih gubitaka.** U ovome se koraku procjenjuje kolika je najveća moguća šteta koja bi se mogla dogoditi, odnosno analizira se koliko se neka šteta često događa (učestalost nastanka štetnog događaja) te se radi procjena koliki je iznos nastale štete (visina štete).

3. **Izbor tehnike za upravljanje rizicima.** Postoje različite tehnike ili metode kojima se, uz osiguranje, mogu izbjeći potencijalni gubici: izbjegavanje rizika, kontrola šteta ili određivanje samopridržaja:

- **izbjegavanje** je metoda kojom se nastoji u potpunosti izbjeći izlaganje kompanije nekom riziku; npr. kompanija će vrlo vjerojatno izbjeći graditi svoje postrojenje na terenu gdje su mogući potresi; ova metoda ima mogućnost svesti rizik na nulu, ali je iznimno nepraktična
- **kontrola šteta** metoda je u kojoj se nastoji smanjiti mogućnost nastanka štetnog događaja: kompanija prihvaća da ne može u potpunosti ukloniti rizik, ali poduzima aktivnosti kojima smanjuje mogućnost njihovog nastanka
- **određivanje samopridržaja** metoda je kojom kompanija odlučuje u kojem će postotku sudjelovati u štetnom događaju ako se on dogodi; ova se metoda može poistovjetiti s franšizom, međutim, da bi se koristila, potrebno je zadovoljiti tri bitna uvjeta: kada gotovo sa sigurnošću možemo predvidjeti kada će se štetni događaj dogoditi, kada nijedna druga tehnika nije dovoljno dobra te kada je najveća moguća šteta minimalna (Klobučar, 2007: 47).

4. **Implementacija programa pokrića rizika.** Ovaj se korak realizira kada su definirani svi prethodni koraci u procesu upravljanja rizikom.

Na Slici 2 prikazana je matrica upravljanja rizikom koja je iznimno korisna, ako se želi vidjeti koliko se često neka šteta može dogoditi i koji je intenzitet tog rizika, jer pruža uvid u odabir koju je vrstu upravljanja rizikom najbolje poduzeti.

MATRICA PROCJENE RIZIKA

ozbiljnost / vjerojatnost	katastrofalan (1)	kritičan (2)	marginalan (3)	neznatan (4)
čest (A)	visok	visok	ozbiljan	srednji
vjerojatan (B)	visok	visok	ozbiljan	srednji
povremen (C)	visok	ozbiljan	srednji	nizak
slab (D)	ozbiljan	srednji	srednji	nizak
nevjerojatan (E)	srednji	srednji	srednji	nizak
eliminiran (F)	eliminiran			

Slika 2. Matrica procjene rizika (izvor: obrada autora)

Ako je šteta niskog intenziteta i njezina visina je niska, tada bi najbolja tehnika bila samopridržaj jer nije učinkovito osiguravati rizik koji se ne događa često.

Ako je učestalost štete niska, ali je njezina visina visoka, tada bi najlogičnije bilo odlučiti se za ugovaranje osiguranja. Ako je i učestalost i visina štete velika, onda bi se trebala primijeniti tehnika izbjegavanja.

Cyber-kriminal ima veliki utjecaj na organizacije jer je problem *cyber*-sigurnosti prerastao informacijsko-komunikacijski odjel, koji je sve donedavno bio isključivo nadležan za poslove *cyber*-sigurnosti te je postao jedan od strateških rizika za koji izvršni menadžment mora preuzeti odgovornost (Bara, 2015).

S obzirom na navedeno, svaka uspješna, ozbiljna kompanija danas bi trebala imati razvijenu strategiju za upravljanje *cyber*-rizicima kako bi mogla nastaviti uspješno poslovanje, tj. da bi sačuvala svoju infrastrukturu, osigurala opstanak na tržištu i kontinuiranu sigurnost.

Ako se navedeno kvalitetno provede, *cyber*-osiguranje može biti dio cjelokupne strategije smanjivanja rizika jer u trećem koraku upravljanja rizikom (izbor tehnika za upravljanje rizicima), nakon što se iskoriste mjere izbjegavanja, kontrole i određivanja samopridržaja, osiguranje rizika jest metoda koju bi svakako trebalo koristiti i to na način da se te metode nadopunjavaju. Istovremeno se postavlja pitanje pruža li osiguranje adekvatnu zaštitu, odnosno pokrivaju li osiguravajuća društva zaštitu stvarnih rizika u *cyber*-sferi, a što će biti obrađeno u drugom dijelu ovog rada.

3.1. Osiguranje rizika

Subjekti koji razumiju prirodu rizika i razlikuju posljedice štetnih događaja mogu se kvalitetno zaštititi i osigurati od gubitaka i šteta raznih vrsta i oblika (Ćurak i Jakovčević, 2007: 61).

Iako postoje i druge metode kojima se može zaštiti, odnosno pomoću kojih se može upravljati određenim rizikom, osiguranje je jedna od bitnih metoda zaštite pojedinca ili kompanije od određenog rizika. Shodno tomu, upravljanje rizikom može se definirati kao metoda kojom se upravlja čistim rizikom kojemu su izloženi pojedinci ili kompanije (Klobučar, 2007: 40).

Najbitnije pitanje upravljanja rizikom jest kako uklopiti sam proces pri ugovaranju osiguranja, odnosno treba li osiguranik uopće raditi analizu rizika kojima je izložen te, ako treba, u kojoj su mjeri klijenti izloženi riziku, a zatim procijeniti koji su potencijalni gubitci i kolika je njihova izloženost.

Vrlo bitnu ulogu u ovom procesu imaju posrednici unutar cijelog sustava osiguranja ili, drugim riječima, brokeri koji najčešće za klijente odrađuju proces upravljanja rizikom jer ni kompanije ni osiguravajuća društva taj proces ponekad ne rade ili ne rade dovoljno ozbiljno. U ovom je procesu iznimno bitan izvještaj o osiguranju (engl. *underwriting report*) ili dokument koji osiguratelju i osiguraniku služi za ocjenu izlo-

ženosti potencijalnim štetama koje mogu osigurati te izračuna najveće vjerojatne štete kojoj klijent odnosno osiguratelj može biti izložen (Klobučar, 2007: 41).

Iz navedenog se može zaključiti da je ovaj proces jako sličan procesu ocjene rizika u osiguranju, ali se radi o rizicima iz različitih djelatnosti i o *cyber*-riziku koji je prisutan radi objektivnih okolnosti ili upravljanja rizicima preuzetih iz osiguranja (Klobučar, 2007: 41).

Upravljanje rizikom jest proces koji kompaniji daje pregled o svim štetama koje bi se mogle dogoditi subjektu (prikazuje izloženost štetama) tijekom poslovanja, a tijekom pregleda tog procesa donose se odluke koji će se rizici pokrivati/osigurati ili će se na neki drugi način ograničiti njegova štetnost.

4. Osiguranje *cyber*-rizika

U današnje doba digitalizacije gotovo da i ne postoji kompanija koja svoje poslovanje ne obavlja u digitalnom odnosno virtualnom svijetu. To čini u obliku komunikacije s klijentima i poslovnim partnerima, zatim pohranjivanjem podataka klijenata, kao i provođenjem internetskih plaćanja te svojom osobnom prezentacijom na internetskim stranicama. Samim time, kao i u pravom svijetu, kompanijama i pojedincima prijete različiti oblici *cyber*-kriminala, kriminalnih napada i prijevara te *cyber*-špijuniranja. Sve navedeno može imati iznimno velike posljedice na poslovanje kompanije, i to ne samo za pojedinu kompaniju nego i na sve dionike kojima je u interesu da poslovni subjekt dobro posluje.

Posljedice ovakvih napada mogu biti gubitak ekonomske vrijednosti, krađa povjerljivih podataka, smanjenje reputacije robne marke i slično.

Što je osiguranje *cyber*-rizika?

Danas se *cyber*-način poslovanja smatra glavnim izvorom rizika za kompanije. No, nije rijetka pojava da se *cyber*-osiguranje pogrešno shvaća zbog razloga kao što su: iznimno kompliciranа stručna terminologija koja je vezana za osiguranje, ali i *cyber*-svijet, kao i zbog same vrste ovog osiguranja koja se vrlo brzo mijenja, odnosno evoluira. Također, danas se *cyber*-rizici više ne smatraju rizicima u nastajanju, pa bi svaka kompanija trebala uzeti u obzir njihov utjecaj na financijsko poslovanje.

Cyber-osiguranje može se definirati kao vrsta imovinskog osiguranja koje štiti poslovanje društava od financijskih gubitaka uslijed ostvarenja *cyber*-rizika (Lesić, 2023).

Cyber-rizici su svi oni rizici koji su u direktnoj vezi s internetskim aktivnostima: kupovanje na mreži, pohrana podataka i slično. Sukladno s tim, *cyber*-osiguranjem osiguravaju se štete koje nastaju kao posljedica hakerskih napada, pokušaja iznude, napada virusima, ljudske pogreške i sve ono što je u vezi s *cyber*-rizicima.

Treba napomenuti da u najboljem slučaju *cyber*-napad može pokazati koji su nedostatci obrambenog sustava informacijsko-komunikacijske kompanije koji se daju jednostavno korigirati/ispraviti, ali u najtežim slučajevima može doći do potpunog prestanka operacija kompanije zbog krađe osjetljivih i povjerljivih podataka kompanije, ali i njezinih klijenata.

Sve navedeno govori da su *cyber*-osiguranja iznimno bitna u današnjem svijetu.

Glavno je pitanje koje potencijalni klijenti postavljaju kada bi neko društvo moralo biti zabrinuto zbog izloženosti *cyber*-rizicima te je odgovor na to pitanje kada:

- kompanija prikuplja, obrađuje i pohranjuje osobne podatke fizičkih osoba
- subjekti imaju visok stupanj ovisnosti o elektroničkim procesima i računalnim mrežama
- subjekti su obveznici regulatornih zahtjeva
- surađuju s pružateljima računalnih usluga
- zabrinuti su u pogledu potencijalnih odštetnih zahtjeva s naslova imovinskih i/ili neimovinskih šteta koje mogu biti posljedica *cyber*-napada (Lesić, 2023).

4.1. Pokrića koja pokriva *cyber*-polica osiguranja

Kao i svaka vrsta osiguranja, tako i *cyber*-polica osiguranja ima određena pokrića kojima štiti osiguranika od štetnoga događaja. No, nameće se pitanje zašto je *cyber*-polica uopće potrebna korisnicima. Ne može li osiguranik jednostavno ugovoriti neku opću policu osiguranja koja bi ujedno pokrivala i sve štete koje nastaju kao posljedica štetnih *cyber*-događaja?

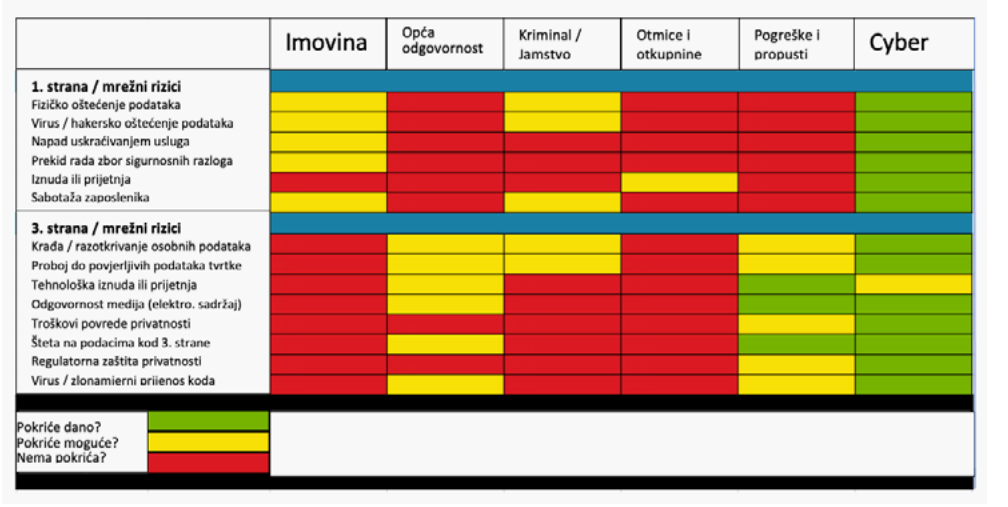
Cyber-police osiguranja upravo su zato napravljene jer standardna pokrića koja nude osiguratelji gotovo da i ne pokrivaju specifične rizike koji su vezani za digitalni svijet i zbog toga se moraju ugovarati *cyber*-police osiguranja.

Neki su od primjera (Lesić, 2023):

- **osiguranje opće odgovornosti** – osigurava se građanskopravna izvanugovorna odgovornost osiguranika za štetu koja je nastala prema trećim osobama koja može biti u obliku ozljede, gubitka/uništenja stvari ili, u najgorem slučaju, smrti
- **osiguranje profesionalne odgovornosti** – pruža pokrića za sve ekonomske štete koje su nastale iz propusta ili nenamjernih pogreški prilikom pružanja profesionalnih usluga te se najčešće isključuju one štete u kojima dolazi do povrede osobnih podataka
- **osiguranje imovine** – pruža pokriće i zaštitu za svu osiguranu materijalnu imovinu u slučaju fizičke opasnosti ili rizika; čest je problem da se ovo osiguranje ne odnosi na podatke ili zapise jer se oni ne smatraju materijalnom imovinom te su izloženi raznim rizicima koji nisu fizičkog karaktera, pa možemo reći da su izloženi rizicima „virtualnog" karaktera, kao što je npr. zlouporaba internih podataka

- **osiguranje pronevjere i računalnog kriminala** – ovo se pokriće u pravilu odnosi samo na zaposlenike te pronevjeru novca ili neke druge materijalne imovine, ali ne i na virtualnu imovinu.

Zbog navedenih nedostataka došlo je do razvoja *cyber*-polica osiguranja koja imaju striktno definirane rizike koje pokrivaju tako da klijent može biti siguran da su njegovi rizici posebno definirani, a što se može jasno vidjeti na Slici 3.



Slika 3. Prikaz pokrića po policama osiguranja (izvor: *AON Risk Solutions*, 2014)

4.2. Podjela *cyber*-pokrića i njihov opseg

Cyber-pokrića mogu se podijeliti na dvije vrste: osiguranje samog osiguranika (*first-party insurance*) i osiguranje trećih strana (*third-party insurance*).

Osiguranje samog osiguranika zapravo pokriva sve štete koje nastaju osiguraniku, a koje su nanesene od strane hakera i drugih subjekata kojima je interes nanijeti štetu samom osiguraniku.

Osiguranje trećih strana su sva ona pokrića koje zahvaćaju odgovornosti prema trećim osobama te se ta vrsta pokrića još naziva pokrićem odgovornosti prema trećim osobama.

Pojednostavljeno, pokrića treće strane zapravo služe da bi se osiguranik osigurao od štete koju je izazvao trećim osobama prilikom realizacije nekog *cyber*-napada.

Pokrića kojima se osiguranik može osigurati jesu (*BIBA*, 2022):

- **financijska naknada** – podložno gubitku koji je nastao kod subjekta nakon završetka *cyber*-napada i prilikom nastupa štete, a osiguranik ima pravo na financijsku isplatu novčanih sredstava od osiguravajućeg društva

- **nadoknada gubitaka zbog prekida poslovanja –** nakon što je *cyber*-napad izvršen, moguće je da dođe do pada cijelog informacijsko-komunikacijskog sustava i samim time onemogućuje se uredno poslovanje kompanije i izvjestan je gubitak prihoda; police *cyber*-odgovornosti mogu pokriti gubitak koji kompanija pretrpi prilikom napada
- **osiguranje u slučaju povrede podataka –** u slučaju da se izvrši *cyber*-napad i nastane štetni događaj, kompanije su dužne po zakonu obavijestiti sve treće strane s kojima posluju da se napad odvio; to može značajno povećati troškove povrede podataka i to ponajviše u smislu zaštite od krađe identiteta za sve one osobe koje su pogođene tim napadom; ovo pokriće uključuje i pravnu zaštitu koja bi trebala kompaniji i samim time štiti podatke od *cyber*-rizika
- **naknada od *cyber*-iznude –** ovo pokriće pokriva slučaj u kojemu napadač postavi *ransomware* ili neki drugi zlćudni program koji je specijaliziran za krađu podataka od kompanija, a funkcionira na principu ucjene, odnosno kompanija mora platiti veliku svotu novaca da bi joj se vratila ukradena informacija; s obzirom na to da su ovakvi napadi sve češći, iznimno je važno ugovoriti ovakvo pokriće
- **forenzička podrška –** prilikom nastanka *cyber*-napada neminovno je da će organizacija morati utvrditi kako se napad dogodio i koji je opseg prodora koji je izvršen i što je dovelo do toga; ovo pokriće omogućuje osiguraniku da mu se cijela forenzička podrška isplati, tj. bude pokrivena i najčešće u sebi sadrži i cjelodnevnu *cyber*-podršku
- **pravna podrška –** ovo pokriće pokriva sve troškove pravne podrške; nakon nastanka napada, tj. štetnog događaja u pravilu se kontaktiraju pravne službe da bi se kompaniji pomoglo u daljnjim koracima, a ta je podrška najčešće iznimno skupa; ovo pokriće pokriva sve troškove koji nastaju prilikom *cyber*-napada.

Uz pokrića koja su standardna za svaku *cyber*-policu osiguranja, mogu se ugovoriti i dodatna pokrića kao što su (*BIBA,* 2022):

- **pokriće *„bricking*"** – pokriće koje pokriva zamjenu računalne opreme oštećene prilikom *cyber*-napada
- ***cyber*-zločini** – pokriva sve one gubitke koji su rezultat prijevare koju su počinili zaposlenici, a to su, na primjer, krivotvorenje i sve ostale kriminalne aktivnosti
- **odgovornost prema medijima** – ovo pokriće pokriva optužbe protiv klevete, raznih omalovažavanja, krađa autorskih prava, ali uvjet je da su nastale kao rezultat pogreške ili propusta
- **gubitak PCI – DSS –** ovo pokriće obuhvaća pokrića procjene, novčanih kazni koje su izrekle banke ili druge kartične kuće zbog nepoštivanja standarda sigurnosti podataka industrije platnih kartica**.**

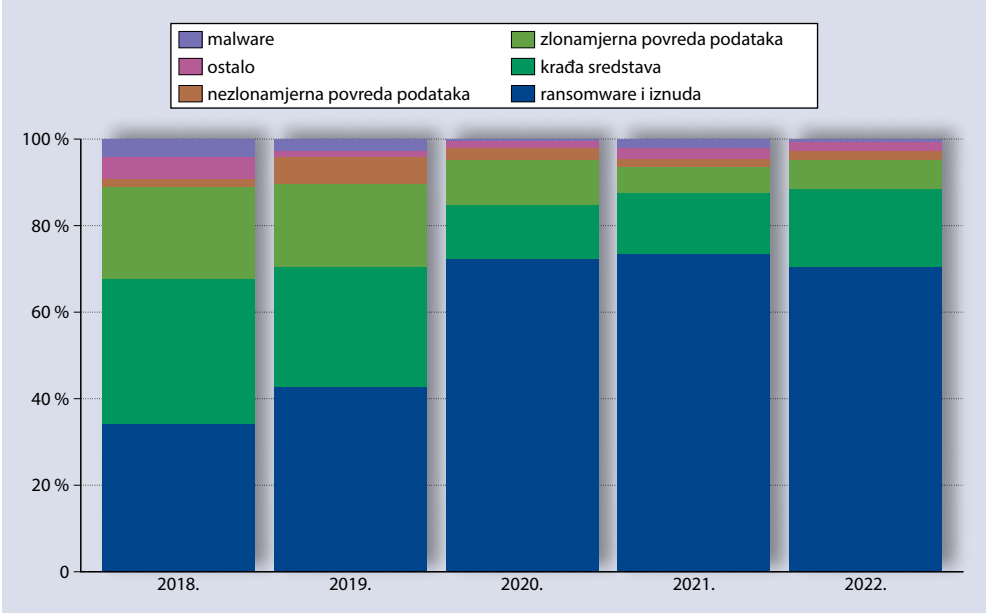
4.3. Dosadašnja iskustva s realizacijom *cyber*-rizika

Britansko udruženje brokera u osiguranju provelo je istraživanje o rizicima koji su najveća moguća prijetnja klijentima te kako se njihov udio mijenjao od 2018. do 2022. godine (BIBA, 2022). Rezultati su prikazani na Grafikonu 1, odnosno na grafikonu je prikazano šest najzastupljenijih rizika, od kojih je najviše zastupljena iznuda.

Iz Grafikona 1 zaključujemo da se već u razdoblju od dviju godina (2018. – 2020.) učestalost rizika iznude povećao čak 100 %, odnosno dvostruko, što je značajan porast za jedan rizik. Krađa novčanih sredstava zauzima drugo mjesto, a trend u grafikonu pokazuje da se taj rizik isprva smanjivao u promatranom razdoblju, ali kasnije i rastao, što ga čini rizikom kojeg je potrebno osigurati. Zanimljivo je da je malware najmanje zastupljen rizik na tržištu te se njegov rizik smanjivao tijekom godina, pa se sada gotovo i ne bilježi kao rizik.

Grafikon također opisuje koje alate najviše koriste „napadači" na osiguranike. Kao što je već navedeno, iznuda je omiljen instrument kojim se radi šteta kompaniji, te se od tog rizika najviše isplati osigurati. Također je važno napomenuti da je taj rizik daleko najzastupljeniji, pa će premija osiguranja biti najskuplja jer postoji najveća šansa da se šteta dogodi. Ovaj grafikon dobar je primjer kakvu bi policu cyber-osiguranja potencijalni osiguranici trebali ugovoriti jer daje jasne podatke koji su rizici najozbiljniji te koji bi se mogli realizirati.

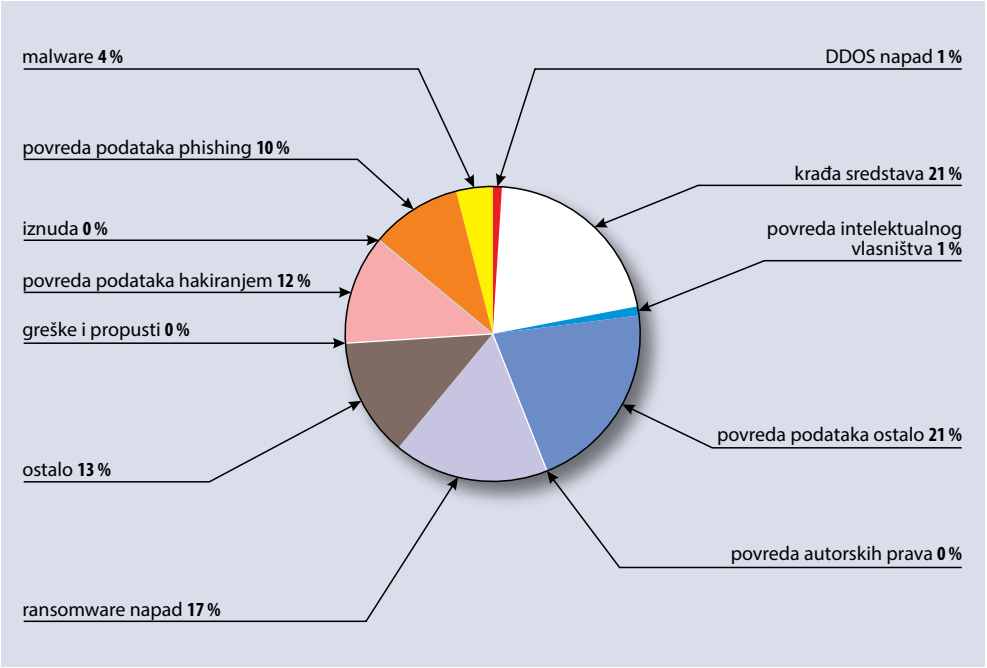
Grafikon 1. Potraživanja klijenata za štete



Izvor: *BIBA* (2022)

U Grafikonu 2 prikazuje se postotak realizacija pojedinih rizika.

Grafikon 2. Postotak realizacije *cyber*-rizika



Izvor: *BIBA* (2022)

Usporedbom Grafikona 1 i 2 može se zaključiti da se najviše realiziraju krađe novčanih sredstava te povrede podataka odnosno krađe podataka. Razlog je tomu činjenica da danas kompanije posluju u virtualnom okruženju i mogu elektronički obavljati novčane transakcije, što značajno olakšava zlouporabu financijskih sredstava. Danas su svima poznate prijevare koje kruže digitalnim svijetom kao jedan od načina kako osiguranik može biti oštećen. Prema podatcima iz Grafikona 2, krađa podataka također je zastupljena, kao i krađa novca, a razlog je jednostavan: danas informacija može vrijediti više od novca. Jedan od primjera ovakvih krađa jest krađa identiteta, koja je zadnjih nekoliko godina dosegla rekordne brojke.

Treći je najveći ostvareni rizik iznuda koja se može definirati i kao nanošenje štete digitalnoj imovini. Iznuda je iznimno zastupljen rizik jer su kompanije danas nevjerojatno ovisne o svojim sustavima, a hakeri znaju da lako mogu iznuditi sredstva od kompanija koje imaju vitalni interes u funkcioniranju i zaštiti svog sustava.

Ranjivost industrijskih kontrola i njihova izloženost *cyber*-napadima predstavljaju ozbiljan rizik i prijetnja su za svaku državu. U svijetu je zabilježeno nekoliko slučajeva manipulacije centrifugama u nuklearnim elektranama, što predstavlja ozbiljan rizik za cijelu populaciju, a ne samo za industriju (Bara, 2015). Primjer *cyber*-napada

slučaj je Stuxneta i iranskog nuklearnog programa (Bara, 2015). Stuxnet je bio pokušaj američke vlade da napadne i onesposobi sve nuklearne elektrane u Sjevernoj Koreji, no napad je bio neuspješan. Ovakvi napadi mogu se vrlo lako klasificirati kao *cyber*-ratovanje, čak i kao *cyber*-terorizam, ali su direktan pokazatelj da je ukupna svjetska populacija izložena *cyber*-napadima i da jedan takav napad može imati goleme posljedice za veliki dio čovječanstva. Svakako treba spomenuti vjerojatno jedan od najvećih incidenata u svijetu. Godine 2015. u svijetu je odjeknuo incident *cyber*-sigurnosti OPM (2015). Ovaj se incident zapravo sastojao od dvaju različitih incidenata pa je u većemu od njih došlo do krađe osobnih podataka više od 21 milijuna državnih službenika, a u manjem su otkriveni osobni podatci oko 4,2 milijuna ljudi.

Uz ova dva velika incidenta 2015. godine dogodili su se mnogi *cyber*-incidenti koji su nanijeli goleme štete u gospodarstvu. Allianzovo izvješće (*Allianz,* 2015) pokazalo je da su takvi incidenti globalno prouzročili gotovo 450 milijarda dolara štete, a čak 50 % ukupno nanesenih šteta snosi deset najvećih svjetskih gospodarstava.

Prema izvješću Willis Towers Watsona iz 2020. godine (WLTW je vodeća globalna tvrtka za savjetovanje, posredovanje i rješenja koja pomažu klijentima diljem svijeta pretvoriti rizik u put rasta), koje su proveli u 14 zemalja i u kojem su analizirali više od 1150 šteta nastalih realizacijom *cyber*-rizika u razdoblju od 2013. do 2019. godine, prosječna je naknada po šteti iznosila 4,88 milijuna USD, uz eksponencijalan rast u tom razdoblju (*Willis Towers Watson,* 2020).

Prema izvješću za 2023. godinu kompanije Coalition Inc. iz San Francisca (tvrtka specijalizirana za *cyber*-rizike koja kombinira sigurnost i *cyber*-osiguranje da bi klijentima pomogla uočiti i spriječiti *cyber*-rizik prije nego što se dogodi putem proizvoda „Aktivno osiguranje"), najvažnija lekcija iz 2022. jest da je *cyber*-rizikom moguće upravljati (*Coalition,* 2023). Većina incidenata koje su uočili mogla se spriječiti prikladnim sigurnosnim kontrolama i aktivnim pristupom upravljanju kibernetičkim rizikom, što ilustrira razloge bliske suradnje sa svakim svojim osiguranikom. Personaliziranim nadzorom i namjenskim timovima za odgovor na incidente „Aktivno osiguranje" pomaže ublažiti rizike i spriječiti napade prije nego što se dogode, što je rezultiralo da su osiguranici Coalitiona doživjeli 64 % manje šteta od prosjeka industrije (u SAD-u).

Prema istom izvješću (*Coalition,* 2023), *cyber*-trendovi u 2022. jesu:

- *cyber*-potraživanja su se stabilizirala, ali *cyber*-rizik nije nestao
- neriješene ranjivosti dovele su do češćih *cyber*-napada i
- programska podrška na kraju životnog vijeka (EOL) učinila je organizacije lakom metom.

Stručnjaci za *cyber*-sigurnost očekuju daljnji rast prijetnji *cyber*-sigurnosti uz pomoć novih i razrađenijih metoda i alata. Razlog zašto će se *cyber*-rizik često realizirati, osim njegove financijske isplativosti, jest taj da je vrlo malo vjerojatno da će osobe koje su skrivile takav napad biti uhvaćene i kažnjene (Schrader, 2015).

5. Zaključak i preporuke

Kao što je u radu prikazano i objašnjeno, *cyber*-rizici nisu samo neizbježna posljedica digitalizacije na koju se moramo bespomoćno priviknuti nego svakodnevica visokotehnološkog pristupa poslovanju s kojom se susreće svaki pojedinac, kao fizička osoba ili kao predstavnik pravne osobe. Drugim riječima, većina poslovnih pojedinaca susreće se s tim rizicima, pa onda mora naći i načina kako zaštititi od rizika sebe i kompaniju za koju je osoba odgovorna.

Jedini je način na koji se to može postići taj da se tim rizicima upravlja procesom upravljanja rizicima. S obzirom na to da postoji slaba educiranost o tom području, potrebno je iskoristiti sve resurse znanja koji su dostupni da bi se proces upravljanja rizikom organizirao na najbolji mogući način. U radu se naglašava da je osiguranje jedna od opcija u procesu upravljanja rizikom, pa bi onda kroz tu prizmu trebalo sagledati i upravljanje *cyber*-rizikom. Naime, tim bi rizikom trebalo upravljati kao i bilo kojim drugim rizikom, pod uvjetom da postoji dovoljno znanja da se njime upravlja.

Ako postoji interno znanje u kompaniji vezano za *cyber*-rizike, tada bi njih u svakom slučaju trebalo upotrijebiti za tu namjenu, a ukoliko ih nema, tada bi trebalo angažirati specijaliste kojima je to područje poznato. Naravno, uz razumno prihvatljiv trošak.

Ono što u ovom procesu zaštite od *cyber*-rizika u Republici Hrvatskoj djelomično stvara probleme jest, s jedne strane, niska averzija prema riziku odgovornih u kompanijama, a s druge strane, slaba aktivnost osiguravajućih društava za osiguranje *cyber*-rizika.

Provedeno je i istraživanje na uzorku od 79 menadžera velikih hrvatskih poduzeća, a rezultati pokazuju da veći dio ispitanika ima veliku sklonost riziku (59 %), u odnosu na ispitanike s niskom sklonošću riziku (41 %), što je karakteristično za neuređeno tržište. Nadalje su muškarci skloniji riziku (75 %) u odnosu na žene (25 %). Istovremeno je u vrhovnom menadžmentu 75 % muškaraca u odnosu na samo 25 % žena (Prester, 2004).

S druge strane, većina osiguravajućih društava u Republici Hrvatskoj trenutno u svojoj ponudi ne nudi *cyber*-osiguranje ili ga nude uz ograničena pokrića. Postoji nekoliko razloga za to. Jedan je od njih da nema dovoljno potencijalnih klijenata jer osiguranje kao djelatnost ima svoje zakonitosti, a jedna od njih je i dovoljan broj klijenata sa sličnim ili istim rizikom. Nameće se pitanje kako riješiti taj problem. Jedno od potencijalnih rješenja su *brokeri* u osiguranju, odnosno specifično međunarodni *brokeri* u osiguranju, jer bi oni u načelu trebali imati dovoljno znanja za realizaciju takve vrste osiguranja, a u slučaju da ta znanja nemaju, oni su dio mreže *brokera* posredstvom koje mogu dobiti odgovore na postavljena pitanja (slično se dogodilo kada se u Republici Hrvatskoj počelo razvijati tržište kapitala, pa se znanje „uvozilo" s onih tržišta koja su već bila razvijenija).

Stoga se može zaključiti da *cyber*-osiguranje zbog rizika koje osigurava ima značajnu ulogu u očuvanju pojedinih dijelova gospodarstva jer povećava sigurnost poslovanja. To znači da u slučaju velike štete na nekom velikom gospodarskom subjektu osiguranje može pokriti nastalu štetu da bi kompanija nastavila daljnje poslovanje.

Treba napomenuti da su hrvatski stručnjaci za sigurnost i forenziku među najboljima u Europi (Ivezić, 2014) i shodno tomu te bi stručnjake trebalo uključiti u pitanja *cyber*-sigurnosti tako da klijentima pruže najbolju moguću zaštitu u *cyber*-osiguranju, za kojom definitivno u suvremenom svijetu postoji potreba.

Literatura

1. *Allianz* (2015). A guide to Cyber Risk: Managing the impact of Increasing Interconnectivity. https://commercial.allianz.com/news-and-insights/reports/a-guide-to-cyber-risk.htm (10. kolovoza 2023.)
2. Andrijanić I. i Klasić K. (2002). *Tehnika osiguranja i reosiguranja*. Zagreb: Mikrorad.
3. *AON Risk Solutions* (2014). Europe's Digital Transformation, The Risk/Return Trade-off. https://www.aon.com/cyber-solutions/?s=Europe%E2%80%99s+Digital+Transformation%3A+The+Risk%2FReturn+Trade-off (6. kolovoza 2023.)
4. Bara, D. (2015). Uloga cyber-osiguranja u upravljanju i prijenosu rizika cyber sigurnosti. U M. Ćurković, S. Dobrić, J. Horvat Martinović, J. Krišto i T. Šker (ur.), *Zbornik radova s međunarodne znanstveno-stručne konferencije „Dani hrvatskog osiguranja"*, str. 127. – 138.
5. *BIBA – British Insurance Brookers´ Association* (2022). A guide to cyber insurance. https://www.cfc.com/media/5279/biba-cyber-guide_2022_digital.pdf (11. kolovoza 2023.)
6. *Coalition* (2023). *2023: Cyber Claims Report*. https://info.coalitioninc.com/download-2023-cyber-claims-report-mid-year-update.html (18. listopada 2023.)
7. Ćurak M. i Jakovčević D. (2007). *Osiguranje i rizici*. Zagreb: RRiF plus.
8. Drljača, M. i Bešker, M. (2010). Održivi rizik i upravljanjem rizicima poslovanja. *Kvalitet*, 7/8. https://bib.irb.hr/datoteka/520678.9._Odrivi_uspjeh_i_upravljanje_rizicima_poslovanja.pdf (30. listopada 2023.)
9. Ivezić, B. (2014, 30. lipnja). HNB: Sumnja se da su cyber kriminalci Hrvatima ukrali 1,8 milijuna kuna". *Poslovni dnevnik*, 2014. https://www.poslovni.hr/sci-tech/manje-napada-cyber-kriminalaca-ali-opasnost-i-dalje-postoji-27446 (10. kolovoza 2023.)
10. Kereta, J. (2004). *Upravljanje rizicima*. RRiF, 8, 48–53.
11. Klobučar, D. (2007). *Risk management i osiguranje*. Zagreb: Tectus.
12. Lesić, T. (2023). Cyber, ANO insurance solutions 2023. *LinkedIn*. ANO Insurance Solutions on LinkedIn: Tvrtke koje su izvoznici u IT industriji pametno upravljaju rizicima i… (19. kolovoza 2023.)
13. Marsh (2015). UK cyber Security: The Role of Insurance in Managing and Mitigating the Risk. HM Government 2015., Marsh Ltd. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf (2. kolovoza 2023.)
14. Matić, B. (2004). *Međunarodno poslovanje*. Zagreb: Sinergija d.o.o.

15. Matić, B. (2016). *Međunarodno poslovanje – institucije, pravila, strategije*. Zagreb: Ekonomski fakultet Sveučilišta u Zagrebu.
16. Microsoft (2023a). Što je DDoS napad? https://www.microsoft.com/hr-hr/security/business/security-101/what-is-a-ddos-attack (30. listopada 2023.)
17. Microsoft (2023b). Što je zlonamjerni softver? https://www.microsoft.com/hr-hr/security/business/security-101/what-is-malware; (30. listopada 2023.)
18. Olsen, T. (2013). Insurance cyber risk. Willis. https://docplayer.net/amp/23894325-Insurance-cyber-risk-tine-olsen-willis.html (2. kolovoza 2023.)
19. *OPM* (2015). Information about OPM Cybersecurity Incidents. https://www.opm.gov/cybersecurity (10. kolovoza 2023.)
20. Prester, J. (2004). Sklonost riziku hrvatskih managera. *Slobodno poduzetništvo*, 4, TEB, Zagreb.
21. Schrader, C. (2015). Small Business Cyber Security Threats. http://www.nationalcybersecurityinstitute.org/small-business/2015-small-business-cyber-security-threats/ (10. kolovoza 2023.)
22. *Willis Towers Watson* (2020). *Cyber*-claims analysis report. https://www.wtwco.com/en-gb/insights/2020/07/cyber-claims-analysis-report (30. listopada 2023.)

Cyber-risk, a phenomenon that exists and endangers us

Abstract

The world in which we live today, engaged in numerous activities, is full of challenges and threats. Before the development of modern digital and communication technologies, individuals, companies, organizations, public service providers, and others were exposed only to physical (tangible and visible) risks. Over the past few decades, however, individuals and companies face potentially more dangerous risks in the cyber world, requiring finding ways to manage those risks, and taking all necessary actions to minimize them. If that proves impossible, measures need to be taken to ensure that life and business can continue normally. This paper demonstrates that cyber risk management is still in its early stages, leaving many companies and individuals with insufficient knowledge or awareness of how to manage them. Some even consider managing such risks or insuring against them as unnecessary. Experiences of certain companies and state institutions demonstrate the reality of cyber risks and the criticality of managing them and insuring against them to maintain stable operations, not only for themselves but also for all clients involved in the business process. Cyber-attacks can paralyze a company and sometimes even destroy it. With this in mind, it is necessary to safeguard against such risks and ensure accountability towards clients who may suffer damage due to such attacks.

Keywords: cyber risks, risk management, cyber risk insurance