Uloga društava za osiguranje u upravljanju cyber rizicima

Čurković, Daria

Sveučilište u Zagrebu

Ekonomski fakultet

Integrirani preddiplomski i diplomski sveučilišni studij

ULOGA DRUŠTAVA ZA OSIGURANJE U UPRAVLJANJU CYBER RIZICIMA

Diplomski rad

Daria Čurković

Zagreb, svibanj, 2022.

Sveučilište u Zagrebu

Ekonomski fakultet

Integrirani preddiplomski i diplomski sveučilišni studij

ULOGA DRUŠTAVA ZA OSIGURANJE U UPRAVLJANJU CYBER RIZICIMA

THE ROLE OF INSURANCE COMPANIES IN CYBER RISK MANAGEMENT

Diplomski rad

Daria Čurković, 0067552216

Mentor: Izv. prof. dr. sc. Maja Mihelja Žaja

Zagreb, svibanj, 2022.

Sveučilište u Zagrebu
Ekonomski fakultet

IZJAVA O AKADEMSKOJ ČESTITOSTI

Izjavljujem i svojim potpisom potvrđujem da je diplomski rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju korištene bilješke i bibliografija.

Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

31.5.2022. Zagreb
(mjesto i datum)

D. Dvoršak
(vlastoručni potpis studenta)

Sažetak

Napredak tehnologije i digitalizacije u današnje vrijeme brzorastući je. Svi poslovni subjekti koji žele biti u korak s vremenom, biti konkurentni na tržištu, poboljšavati svoje usluge, širiti poslovanje i napredovati, moraju se koristiti visokom razinom tehnologije i digitalizacije. Zbog toga, postaju izloženi negativnim posljedicama koje dolaze s korištenjem tehnologije. Najveća prepreka i problem su kibernetički rizici koji dolaze u paketu s digitalizacijom. Što se više razvija tehnologija, to su veće šanse nastanka cyber incidenta. Poslovni subjekti ne mogu izbjegavati kibernetičke rizike jer bi to značilo izbjegavanje korištenja tehnologije, što u današnjem vremenu nije opcija. Najbolji način upravljanja rizicima je putem osiguranja rizika. Društva za osiguranje jedan su od najvažnijih segmenata financijskog tržišta. Poslovni subjekti intenzivno osiguravaju svoje rizike putem tradicionalnih polica osiguranja, a u zadnje vrijeme povećava se i osiguranje cyber rizika. Postoje prepreke i problemi prilikom osiguravanja takvih rizika, pa to tržište još nije dovoljno razvijeno u cijelom svijetu, no definitivno će u narednom vremenu postati jedno od najznačajnijih segmenata društava za osiguranje. U radu se želi prikazati važnost efikasnog upravljanja cyber rizicima, koji su definitivno u vrhu svjetskih rizika. Postoji više načina za upravljanje tim rizicima no jedan od najvažnijih je upravo putem društava za osiguranje. Prikazat će se koja je uloga osiguranja, analizirati koliko su društva za osiguranje iskorištena u upravljanju cyber rizicima i koje su strategije upravljanja cyber rizicima. U radu će se za analiziranje i istraživanje koristiti sekundarni podaci. Koristit će se deskriptivna metoda, induktivna i deduktivna metoda, metoda komparacije, kompilacije i opisne statistike.

Ključne riječi: društva za osiguranje, cyber rizik, cyber osiguranje, cyber incident, upravljanje cyber rizikom, tehnologija

Summary

The progress of technology and digitization nowadays is fast – growing. All business entities which want to keep up with time, be competitive in the market, improve their services, expand business and progress, must use high levels of technology and digitization. Because of this, they become exposed to the negative consequences that come with the use of technology. The biggest obstacle and the problem are cyber risks that come in a digitization package. The more technology develops, the greater are the chances of Cyber incident. Business entities cannot avoid cyber risks because it would mean avoiding the use of technology, which is not an option in this days. The best way to manage risks is to secure risk. Insurance companies are one of the most important segments of financial market. Business entities are intensively providing their risks through traditional insurance policies, and recently, Cyber risk insurance has been increased. There are obstacles and problems when ensuring such risks, so this market is not yet sufficiently developed all over the world, but it will definitely become one of the most significant segments of insurance companies in the next time. The paper wants to show the importance of efficiently managing Cyber risks, which are definitely at the top of the world's risks. There are several ways to manage these risks, but one of the most important is precisely through insurance companies. It will be shown what the role of insurance is, analyzing how much insurance companies have been used in managing cyber risks and what are the cyber risks management strategies. Secondary data will be used for analyzing and research. The descriptive method, inductive and deductive method, comparison method, compilation and descriptive statistics will be used.

Key words: Insurance Companies, Cyber Risk, Cyber Insurance, Cyber Incident, Cyber Risk Management, Technology

Sadržaj

1. UVOD

1.1. Predmet i cilj rada

Današnje vrijeme je vrijeme tehnološkog rasta i napretka iz dana u dan. Kako tehnologija napreduje, gospodarski sektori to prate i koriste, kreću se u skladu s vremenom. U ovom radu objasnit će se da takav rast i napredak s jedne strane daje pozitivne efekte, a s druge negativne. Zbog većeg obujma korištenja informacijske tehnologije, elektroničke komunikacije i digitalizacije, poslovni subjekti sve su više izloženi kibernetičkim opasnostima. Cyber incidenti, kao što su cyber napadi, terorizam, cyber rat, špijunaže, prevare, krađa podataka i slično, su u samom vrhu svjetskih rizika. Svaki takav incident može imati loše i razorne posljedice za poslovne subjekte, stoga je važno efikasno upravljati cyber rizicima. U radu je objašnjeno i navedeno više načina upravljanja cyber rizicima, ali naglasak je na cyber osiguranju.

Predmet istraživanja ovog rada je utjecaj cyber rizika na poslovanje, kako se taj rizik može smanjiti i kako njime upravljati, posebice putem osiguranja tih rizika. Cilj rada je analizirati i zaključiti kolika je važnost društava za osiguranje u upravljanju cyber rizicima i borbi protiv cyber kriminala.

1.2. Izvori podataka i metode prikupljanja

Tijekom izrade diplomskog rada koristit će se znanstveni i stručni članci, knjige, izvješća, publikacije i Internet stranice te iz njih prikupljeni sekundarni podaci koji će biti analizirani i opisani. U okviru ovog rada korištene su deskriptivne metode u analizi sekundarnih podataka, deduktivna i induktivna metoda, metoda kompilacije, komparacije i opisne statistike.

1.3. Sadržaj i struktura rada

Rad se sastoji od 5 poglavlja. U uvodnom poglavlju navodi se predmet i cilj rada, izvori podataka i metode prikupljanja te sadržaj i struktura rada.

Drugo poglavlje posvećeno je društvima za osiguranje. U njemu se obrađuje teorijski dio o osiguranju, poslovanje osiguratelja, izvori sredstava i proizvodi osiguranja te se opisuju temeljne odrednice, proizvodi i prepreke cyber osiguranja. Cilj ovog poglavlja je definirati i objasniti što je cyber osiguranje i prikazati njegovo tržište.

Treće poglavlje govori o temeljnim odrednicama cyber rizika. Na početku poglavlja, dio je o informacijskoj tehnologiji, kako ona utječe na poduzeća i koja joj je uloga. Nakon toga definiraju se cyber rizici, izloženost tim rizicima te se pojašnjava zloupotreba informacijske tehnologije. Na kraju poglavlja je pregled nekih cyber incidenata iz svijeta i iz Republike Hrvatske koji su se događali u prošlosti.

U četvrtom poglavlju objašnjavat će se kako identificirati cyber rizike, navoditi načini, mogućnosti, strategije i preporuke smanjivanja rizika, prvenstveno pomoću cyber osiguranja. Uz to, analizirat će se uloga društava za osiguranje u upravljanju cyber rizicima kod poslovnih subjekata, pokazat će se koliki je njihov značaj te kako se taj značaj povećava kroz vrijeme. U poglavlju se želi zaključiti i pokazati važnost osiguratelja u sveukupnoj poslovnoj strategiji smanjivanja cyber rizika.

Rad završava zaključkom u kojem se sistematiziraju rezultati teorijske analize, iznose se najvažnije činjenice i donose zaključna razmatranja. Nakon zaključka navedeni su popis literature, popisi slika, grafikona i tablica te životopis autorice.

2. OBILJEŽJA DRUŠTAVA ZA OSIGURANJE

2.1. Teorijski okvir osiguranja

Osiguranje jest kompleksan sustav. Ekonomski, ono je instrument koji omogućuje pojedincu da zamijeni relativno malu svotu novca za relativno velik i neizvjestan financijski gubitak. Također, to je gospodarska djelatnost putem koje se pojedincu pruža ekonomska zaštita za različite rizike koji ugrožavaju pojedinca, njegov život, imovinu ili zdravlje. Osiguranje ima dva temeljna obilježja. Jedno se temelji na prijenosu rizika s pojedinca na skupinu ili zajednicu rizika, što pokazuje svijest pojedinca o ugroženosti od opasnosti od kojih će se efikasnije zaštiti ukoliko je uključen u sustav osiguranja. Drugo obilježje je raspodjela gubitaka, koja se temelji na izjednačenoj osnovici, na sve članove zajednice, što podrazumijeva podjelu nastalih gubitaka na sve osiguranike i pokriće tog gubitka iz uplaćenih premija koje su osiguranici uplatili.

Gospodarski subjekti ili pojedinci, uplaćuju premije osiguranja u ravnomjernim razdobljima kako bi se zaštitili od iznenadnih velikih gubitaka i neplaniranih troškova poslovanja. Međutim, osiguranje od rizika ne znači da neće doći do štetnog događaja i ne umanjuje vjerojatnost nastanka štete. Štoviše, osiguranici nekada mogu nenamjerno uzrokovati i inicirati rizik te štetan događaj, smanjenim oprezom i osjećajem sigurnosti zbog transferiranja rizika na osiguratelja. S druge strane, osiguranje funkcionira i omogućuje obeštećenje na racionalnim temeljima i u suštini onemogućava zloupotrebu što pojedince čini opreznijima. (Ćurak, Jakovčević, 2007.)

Osiguranje je sa stajališta pojedinca gospodarski instrument putem kojeg pojedinac vrlo malu svotu novca zamjenjuje za veliki neizvjestan gubitak koji bi postojao ukoliko ne bi bilo osiguranja. Osiguranje sa stajališta društva je gospodarski instrument za smanjivanje rizika putem kombiniranja velikog broja izlaganja istim rizicima i predviđanja gubitaka za promatranu skupinu kao cjelinu. (Klasić, Andrijanić, 2007.)

Osiguranje je, u najširem smislu, ekonomski institut u društvenom i gospodarskom životu koji zaštićuje pojedince, poslovne subjekte i gospodarski razvoj od nesretnih slučajeva i posljedica prirodnih sila. (Ćurak, Jakovčević, 2007.) Svrha osiguranja je prijenos rizika s pojedinca na osiguratelja putem ugovora o osiguranju, a premija je cijena tog osiguranja. (Rafaj, 2009.)

Sustav osiguranja ima tri temeljne funkcije, a to su: zaštitna, mobilizacijsko-alokacijska i društveno-socijalna funkcija. (Ćurak, Jakovčević, 2007.)

Zaštitna funkcija obuhvaća neposrednu (izravnu) i posrednu (neizravnu) zaštitu.

Neposredna zaštita nastoji uspostaviti efikasan sustav koji može smanjiti posljedice neželjenog događaja. Takva zaštita obuhvaća sustav preventive, koji se odnosi na prihvaćanje i primjenu svih mjera, normi, instrumenata i aktivnosti kojima je svrha ukloniti uzroke nastanka štetnog događaja. To uključuje identificiranje svih mogućih uzročnika nastanka štete, poduzimanje mjera za ograničavanje ili eliminaciju nastanka šteta i poboljšanje zaštitnih mjera za život, imovinu i zdravlje čovjeka. Preventivne mjere su na primjer tehnički pregled automobila, dizanje nasipa, uvođenje raznih standarda za različite aktivnosti i slično. S druge strane, sustav represije podrazumijeva poduzimanje mjera i aktivnosti za spašavanje ljudi i imovine. Sustav represije barem djelomično nadoknađuje slabosti sustava preventive. Primjer preventivne mjere je aparat za gašenje požara, dok su primjer represivne mjere vatrogasci. (Ćurak, Jakovčević, 2007.)

Posredna zaštita podrazumijeva ispunjavanje ugovornih obveza između društva za osiguranje i osiguranika. To uključuje isplatu odšteta koje osiguranicima isplaćuju društva za osiguranje za one rizike koji su u ugovoru o osiguranju definirani. Posredna zaštitna funkcionira na temelju prihoda koje društva za osiguranje prikupljaju putem obračuna i naplate premija osiguranja. (Hrvatska enciklopedija, 2021.) Postoje tri temeljna obilježja posredne zaštite osiguranja, a to su: stabilnost koja pokazuje da pojedinac može stabilno živjeti i poslovati u okolnosti ekonomske zaštite, sigurnost koja se pojavi kada se čovjek osjeća ekonomski zbrinutim i kontinuitet poslovanja jer se temeljem premijskih prihoda i rashoda potencijalni gubici pretvaraju u trošak osiguranika i prihod osiguratelja.

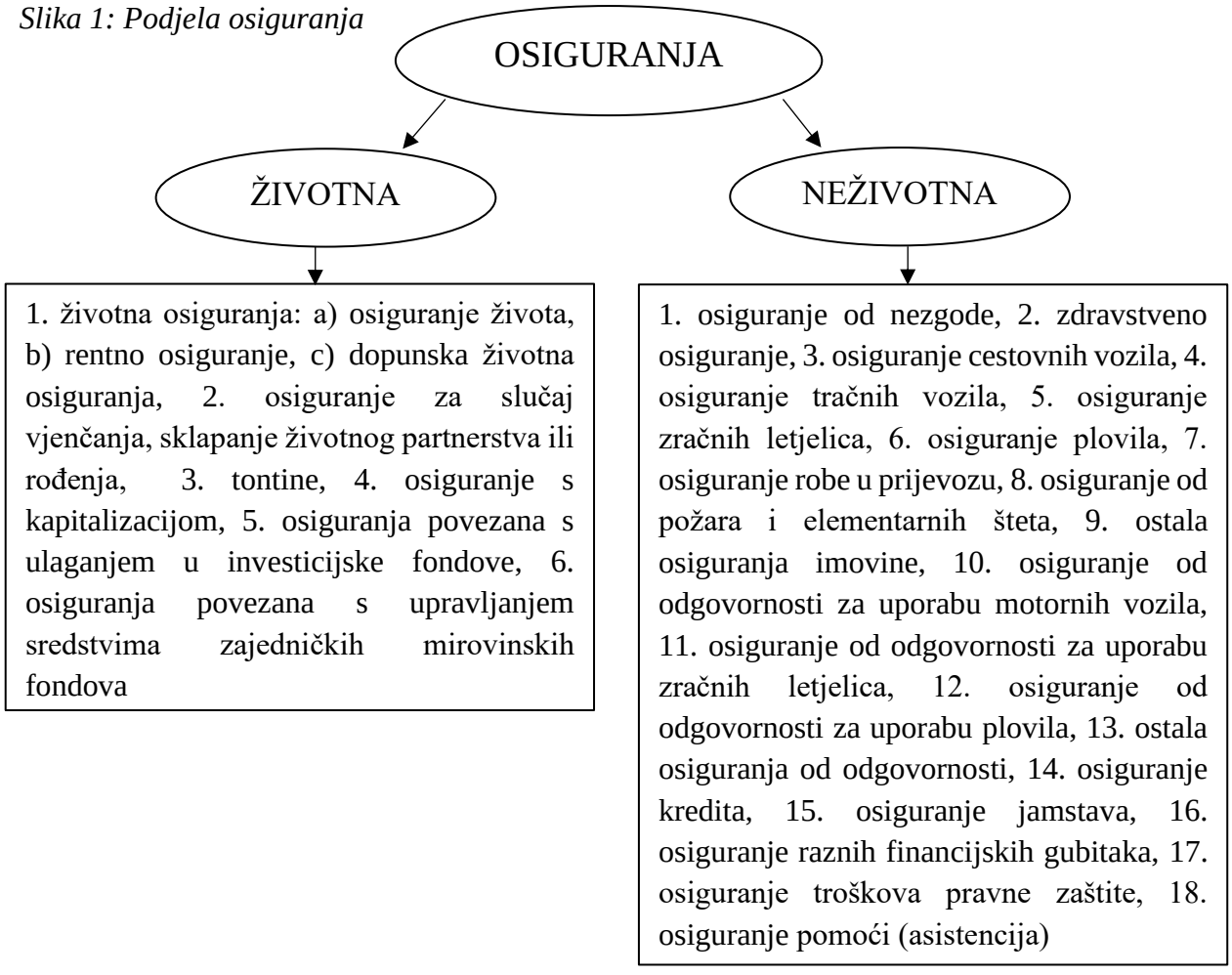
Mobilizacijsko-alokacijska funkcija je funkcija koja redistribuira štednju suficitarnih sektora i alocira ju deficitarnim sektorima putem financijskih tržišta. Društva za osiguranje putem premija osiguranja skupljaju suficitarne viškove od strane šire javnosti i na taj način potiču individualnu štednju, brigu pojedinca za budućnost i omogućavaju osiguranicima kupnju vlastite sigurnosti. Društva za osiguranje danas su vrlo važni institucionalni investitori. Uplaćene premije osiguranja predstavljaju im pasivu iz koje se oblikuje portfelj odnosno imovina društava za obveze koje su preuzete plasmanima na financijskim tržištima. S obzirom da kao institucionalni investitori alociraju plasmane gospodarski deficitarnim sektorima, pridonose razvoju financijskih tržišta, a vrijedi i naglasiti da prikupljaju veliku količinu štednje

stanovništva pa na taj način sudjeluju i utječu na dinamiku razvoja globaliziranih tržišta kapitala. Društva za osiguranje obavljajući svoju temeljnu djelatnost također ulažu i u državne i komunalne vrijednosnice pa podupiru razvojnu, zdravstvenu i socijalnu politiku, poslovno i vlasnički se integriraju s drugim institucijama te i time pridonose razvoju financijskog tržišta, razvijaju financijske proizvode pomoću vlasnički povezanih i nepovezanih financijskih institucija, pogoduju modernizaciji sustava garancija i drugo.

Društveno-socijalna funkcija osiguranja podrazumijeva ekonomsku, zdravstvenu i socijalnu zaštitu pojedinca. Odnosi se na izražen socijalni element kroz ekonomsku zaštitu, odnosno kroz materijalnu naknadu za nastale štete i isplate osiguranih svota. (Ćurak, Jakovčević, 2007.)

Klasifikacija osiguranja moguća je po raznim kriterijima. Ugrubo, po predmetu osiguranja, osiguranja se dijele na osiguranje osoba, osiguranje imovine i osiguranje od odgovornosti. (Hrvatska enciklopedija, 2021.) Prema Zakonu o osiguranju, koji je norma unutar Europske unije, osiguranja se dijele na životna i neživotna. (Zakon o osiguranju, 2020.)

Slika 1: Podjela osiguranja



Izvor: Izrada autora prema Zakonu o osiguranju, 2020.

2.2. Poslovanje društava za osiguranje

Glavna djelatnost društava za osiguranje jest pružanje usluge osiguranja, odnosno prodaja osiguranja. Ipak, svako društvo za osiguranje radi mnogo više od čiste prodaje. Kako bi osiguranje bilo dostupno široj publici, društva za osiguranje moraju odraditi širok spektar aktivnosti koje će omogućiti proces prodaje osiguranja. Ukupnost svih poslovnih operacija koje prethode i slijede sklapanju ugovora o osiguranju, preduvjet su za uspješno poslovanje društva za osiguranje. (Klobučar, 2007.)

Najvažnije poslovne aktivnosti svih društava za osiguranje su:

- utvrđivanje premijskih stopa,
- ugovaranje osiguranja,
- prodaja osiguranja,
- procjena i likvidacija šteta,
- reosiguranje i
- investicije.

Navedeno nisu svi poslovi kojima se društva za osiguranje bave – moraju se uključiti i poslovi računovodstva, pravni aspekt, kontrola i preventiva, poslovi obrade podataka i slično. (Klobučar, 2007.)

Poslovi društava za osiguranje generalno se baziraju na preuzimanju rizika. O tome koliki rizik društvo preuzima ovisi kolika će biti premija osiguranja. Određivanjem premijskih stopa, utvrđuje se premija, tj. cijena osiguranja. Društva za osiguranje unaprijed ne znaju kolika će biti stvarna cijena osiguranja jer se ona izračunava unaprijed temeljem procijenjenih veličina (izloženost riziku, učestalost štetnih događaja, svota osiguranja itd.), a ne točnih materijalnih pokazatelja. Tek nakon isteka važenja police osiguranja društvo za osiguranje će moći utvrditi gubitke ili profit. Cilj osiguratelja jest da premije osiguranja budu dovoljne za plaćanje svih očekivanih šteta i troškova te da s druge strane daju određeni profit. U društvima za osiguranje osobe koje određuju premijske stope zovu se aktuari. Pri utvrđivanju premijskih stopa postoje kriteriji koji moraju biti uvaženi – kriterij profitabilnosti, zakonodavni i poslovni kriteriji.

Zakonodavni kriteriji:

- adekvatne premijske stope – premijske stope trebaju biti dovoljno visoke da pokriju štete (ukoliko su neadekvatne može doći do bankrota i insolventnosti osiguratelja);

- ne previsoke premijske stope – ne smiju biti veće od vrijednosti zaštite koju pružaju;
- nediskriminirajuće – premijske stope ne smiju biti znatno različite za relativno sličnu izloženost rizicima.

Poslovni kriteriji:

- jednostavnost – sustav utvrđivanja premijskih stopa mora biti razumljiv da prodavatelji osiguranja mogu utvrditi premiju osiguranja u najkraćem roku;
- stabilnost – premijske stope moraju biti stabilne u kratkom razdoblju da se zadrži zadovoljstvo osiguranika;
- prilagodljivost – promjenjiva je izloženost štetama pa sukladno tome premije moraju biti prilagodljive u cilju zadovoljenja kriterija adekvatnosti;
- poticajnost za kontrolu šteta – sustav utvrđivanja premijskih stopa mora poticati aktivnosti kontrole šteta, smanjujući njihovu učestalost i visinu. (Klobučar, 2007.)

Sljedeći važan dio poslovanja društava za osiguranje jest ugovaranje osiguranja – proces selekcije i klasifikacije budućih osiguranika i rizika kojima su izloženi. Osiguratelji odlučuju hoće li potencijalnog osiguranika i rizik prihvatiti u osiguranje ili odbiti. Prvenstveni cilj selekcije je da se u osiguranje uvedu profitabilni poslovi. Svako društvo za osiguranje mora utvrditi kriterije za ugovaranje osiguranja, a koji moraju biti u skladu s ciljevima. Na primjer, ciljevi mogu biti veliki volumen posla s malim postotkom profita ili manji volumen posla s velikim postotkom profita. Moraju biti određene vrste poslova koje su prihvatljive, granične ili zabranjene. Također, ukoliko je dostupno reosiguranje, slobodnije će se pristupati i ugovaranju osiguranja. (Klobučar, 2007.)

Poslovanje društava za osiguranje započinje prodajom osiguranja, a ne proizvodnjom kao većina drugih djelatnosti. Zbog toga, prodaja je jedna od najvažnijih funkcija osiguranja, a nerijetko je i od strane osiguratelja prodaja istaknuta kao najteži zadatak u cjelokupnoj djelatnosti. Upravo iz navedenih razloga, marketing u osiguranju zauzima važno mjesto. Marketing je širok spektar radnji koje su usmjerene na poboljšanje i povećanje obujma prodaje proizvoda osiguranja i povećanja cjelokupnog poslovanja osiguratelja te na zadovoljavanje potreba i zahtjeva tržišta. Važnost marketinga proizlazi iz stalno promjenjive potražnje za različitim proizvodima osiguranja, ali također i iz sve veće konkurencije na tržištu osiguranja. Distribucijski kanali osiguranja su načini na koje se proizvodi osiguranja prodaju. Kanali distribucije osiguranja dijele se na:

- posrednički kanal,

- bankoosiguranje i
- izravnu prodaju. (Ćurak, Jakovčević, 2007.)

Posrednički kanal je distribucijski kanal u kojem se proizvodi osiguranja prodaju putem posrednika. Takvom prodajom osiguranja ostvaruje se neizravna veza između osiguratelja i ugovaratelja osiguranja. Najčešći posrednici osiguranja su brokeri i agenti. Brokeri u osiguranju su posrednici koji su predstavnici osiguranika. Oni savjetuju osiguranike i pregovaraju o uvjetima osiguranja, a nakon sklopljenog ugovora, dobivaju proviziju od strane osiguratelja. Agenti osiguranja, s druge strane, zastupaju osiguratelje i u njihovo ime djeluju, onoliko koliko su točno ovlašteni za djelovanje (od strane osiguratelja). Proviziju također ostvaruju od strane osiguratelja. (Rejda, 2005.)

Bankoosiguranje je povezivanje banaka i osiguranja, distribucija proizvoda osiguranja putem banaka. Povezivanje banaka i osiguratelja nije dopušteno u svim zemljama, u smislu da banke proizvode osiguranja i preuzimaju obveze iz ugovora o osiguranju, ali dopuštena je distribucija proizvoda. Banke mogu biti uključene u prodaju proizvoda na temelju distribucijskih sporazuma s osigurateljem. Također, banke mogu obavljati poslove bankoosiguranja uz pomoć društva za osiguranje preko joint venture firme, u slučaju financijskog konglomerata kojem pripadaju i banka i društvo za osiguranje i slično. Glavna svrha bankoosoiguranja je bolja iskorištenost raznih kanala prodaje i smanjenje troškova te ponuda šireg izbora financijskih proizvoda na jednom mjestu što dovodi do povećanja ukupne prodaje i maksimizacije profita.

Izravna prodaja osiguranja ostvaruje se bez pomoći posrednika i banaka već se proizvodi osiguranja plasiraju kanalom izravne prodaje. Dobra strana izravne prodaje su niži troškovi kojima se ostvaruje niža cijena proizvoda osiguranja, dok su negativne strane manja prodornost i uvjerljivost te formiranje negativnog stava zbog jeftinog osiguranja. (Ćurak, Jakovčević, 2007.)

Odjel za utvrđivanje šteta ispituje sve okolnosti važne za utvrđivanje šteta i štetnog događaja,, uključujući procjenu šteta i proceduru u likvidaciji. Osnovni ciljevi u procesu likvidacije šteta su verifikacija pokrića – je li osoba ili imovina pokrivena po polici osiguranja, fer i promptno plaćanje štete i osobna pomoć osiguraniku – npr. procjenitelj šteta može pomoći osiguraniku u traženju smještaja nakon požara. (Klobučar, 2007.)

Osoba koja utvrđuje štetu je procjenitelj šteta, a postoji nekoliko vrsta procjenitelja:

- agent ili broker – ukoliko ima ovlaštenja za takve poslove, osiguranik prijavljuje štetu direktno agentu ovlaštenom za utvrđivanje štete i donošenje odluke o plaćanju do određenog iznosa;
- procjenitelj društva za osiguranje – stalni zaposlenik koji predstavlja samo to društvo za osiguranje;
- neovisni procjenitelj – pruža usluge društvima za osiguranje za proviziju ili slično;
- ured za procjenu šteta – neovisna institucija koja pruža usluge utvrđivanja šteta;
- javni procjenitelj – češće predstavlja osiguranika, a koriste se u situacijama kada se osiguratelj i osiguranik ne slažu s visinom procijenjene štete.

Postupci u utvrđivanju štete:

- obavijest o nastanku štetnog događaja,
- istraživanje i dokazivanje štete – je li nastao štetni događaj pokriven osiguranjem,
- donošenje odluke o plaćanju štete. (Klobučar, 2007.)

Osiguratelj je obvezan isplatiti naknadu iz osiguranja za štetu koja je nastala iz osiguranog slučaja, na temelju odredbi i uvjeta prema kojima je sklopljen ugovor o osiguranju. Iznos naknade koju osiguratelj plaća ne može biti veći od štete koju je osiguranik pretrpio nastupom osiguranog događaja. (Bijelić, 2002.)

Reosiguranje je jedno od važnijih koraka koje društvo za osiguranje poduzima tijekom svog poslovanja. Nakon sklapanja ugovora o osiguranju, osiguratelji se mogu osigurati reosiguranjem. Reosiguranje je osiguranje osiguranja. Dakle, reosiguranje omogućuje osigurateljima da preuzmu rizike koji prelaze njihov kapacitet – povećava se kapacitet za preuzimanje rizika. (Bijelić, 2002.) Osiguratelji moraju raspoznati rizike koje bi trebalo reosigurati, a često i značajni poslovni partneri društava za osiguranje žele znati kod kojih je reosiguratelja njihov rizik osiguran.

Investiranje društava za osiguranje donosi velik značaj u cjelokupnom poslovanju. Jedna je od najvažnijih funkcija poslova osiguranja. Prikupljene premije od strane osiguranika društva za osiguranje plasiraju na tržište putem kredita ili nekih drugih oblika investiranja sve dok nisu potrebne za likvidacije šteta i za plaćanje ostalih troškova. Fondovi koji se koriste za investiranje se, uz premije, pune i kamatama koje su ostvarene investiranjem i dospjelim investicijama koje se mogu reinvestirati. (Klobučar, 2007.)

2.3. Osiguranje kao metoda upravljanja rizicima

„Rizici su dio svakodnevnog života čovjeka i poslovnog okruženja gospodarskog subjekta.“ (Ćurak, Jakovčević, str 61.)

Svaka racionalizacija izloženosti rizicima je na individualnoj razini pojedinca. Oni koji razumiju prirodu rizika i koji su svjesni različitih posljedica štetnih događaja mogu se kvalitetno osigurati i izbjeći razne gubitke. Svijest i znanje o mogućnostima zaštite od rizika i mogućnostima upravljanja tim rizicima postali su važan dio poslovnog svijeta. Svaki poslovni subjekt sam određuje koju količinu rizika može preuzeti sam, a koju količinu rizika će transferirati na društva za osiguranje, stoga je važno usvojiti pojam rizika, shvatiti ga i definirati oblike rizične klasifikacije, kako bi se pronašao najbolji balans u preuzimanju i transferu rizika s kojima se poslovni subjekt susreće.

Treba razlikovati rizik od neizvjesnosti. Neizvjesnost je nemogućnost predviđanja budućnosti i ishoda nekog događaja. Rizik je, općenito, varijacija mogućih ishoda u nekoj situaciji u budućnosti. Objektivan rizik je varijacija ishoda nekog događaja, što bi se sve stvarno moglo dogoditi, i moguće ju je analizirati, mjeriti i procijeniti. S druge strane, subjektivan rizik je procjena osobe o nastupanju objektivnog rizika. U užem smislu, rizik je vjerojatnost odstupanja od onog što je očekivano. Temeljni pokretači rizika su razne opasnosti i hazardi. Dok je opasnost sama po sebi potencijalni uzrok nastanka štete, npr. požar, potres i slično, hazard je stanje koje izravno povećava opasnost, odnosno vjerojatnost nastanka štete. (Ćurak, Jakovčević, 2007.)

Većina pojedinaca želi izbjeći rizike, što se može nazvati averzijom prema riziku. Averzija prema riziku je najveći razlog zašto se pojedinci i poduzeća odlučuju na osiguranje, bez obzira što premije osiguranja iziskuju manje ili veće troškove. (Harrington, Niehaus, 2003.)

Da bi se nekim rizikom moglo upravljati putem osiguranja, odnosno uopće ga moći osigurati, taj rizik mora biti osigurljiv. Takvi rizici se prepoznaju i standardiziraju prema svojim obilježjima. Osigurljivi rizici su oni rizici za koje postoji osnova za utvrđivanje njihove veličine i mogućnosti pokrića. Mjerljivi su u smislu vjerojatnosti njihovog nastanka i obujma posljedica pa se može odrediti njihova cijena i prihvatljivost, kako za osiguratelja, tako i za osiguranika. U osigurljive rizike ulaze čisti rizici i u njih spadaju:

- osobni rizici,

- imovinski rizici,
- rizici odgovornosti i
- rizici nastali iz propusta drugih osoba.

Neosigurljivi rizici, s druge strane, su oni rizici za koje osiguratelj nema stvarnu osnovicu za utvrđivanje premije, nemjerljivi su i ne postoji mogućnost za diverzifikaciju rizika. Uključuju:

- špekulativne rizike,
- političke rizike i
- tehnološke rizike. (Ćurak, Jakovčević, 2007.)

Čisti rizik je posljedica slučaja, a ne svjesnog djelovanja pojedinca. (Klasić, Andrijanić, 2007.) To su rizici kod kojih postoji neizvjesnost od nastanka štetnog događaja, odnosno gubitka i ne postoji mogućnost ili situacija u kojoj bi nastupio rizični događaj, a da iz toga proizađe bilo kakva dobit. Nasuprot tome, špekulativni rizici, primjerice, su oni rizici kod kojih postoji neizvjesnost nastanka događaja koji može prouzročiti i gubitak, ali i dobitak. (Trieschman, Gustavson, 1995.) Špekulativni rizici su svjesni rizici u koje pojedinci ulaze pa se njima osiguranja ne bave. (Klasić, Andrijanić, 2007.)

Da bi rizik bio osigurljiv mora zadovoljavati sljedeće uvjete:

- mora postojati velik broj izloženih jedinica riziku,
- gubitak mora biti nenamjeran i slučajan,
- gubitak mora biti mjerljiv i odrediv,
- gubitak ne smije biti katastrofalan,
- šanse za gubitak moraju biti mjerljive i
- premija mora biti ekonomski izvodljiva. (Rejda, 2005.)

U suvremeno doba upravljanje rizicima jedno je od najvažnijih segmenata upravljanja poduzećem. Ciljevi upravljanja rizicima se svode na:

- identifikaciju i klasifikaciju,
- analizu (mjerenje kroz učestalost i jačinu),
- vrednovanje po prioritetima od značaja za poduzeće i
- odabir strategije za upravljanje rizika. (Ćurak, Jakovčević, 2007.)

Prema Vaughan i Vaughan (1995.), postupak kojim se postižu ciljevi upravljanja rizikom su:

1. utvrđivanje ciljeva

2. identifikacija rizika
3. procjena rizika
4. razmatranje alternativa i odabiranje instrumenata za upravljanje rizikom
5. primjena odluke
6. procjena i ponovno ispitivanje.

Tri osnovna načela upravljanja rizikom:

- Ne riskiraj više nego što si možeš dopustiti da izgubiš.
- Uzmi u obzir i slučajnost.
- Ne riskiraj puno za malo. (Vaughan, Vaughan, 1995.)

Metode kontrole rizika dijele se na fizičke kontrole, koje podrazumijevaju izbjegavanje rizika ili smanjenje izloženosti riziku (kontrola gubitaka, separiranje, kombiniranje i nefinancijski transferi) i na financijske kontrole koje obuhvaćaju aktivno i pasivno zadržavanje rizika te transfere rizika. Transferi rizika mogu biti neosiguranjni, npr. prijenos rizika oštećenja na proizvođača ili distributera, ili se mogu odnositi na transfer rizika na društvo za osiguranje. Takav transfer rizika je metoda koja ima najviše prednosti u odnosu na sve druge. Nakon što se poslovni subjekt odluči za transfer rizika na osiguratelja, on mora izabrati rizike koje će osigurati, odabrati osiguratelja, povremeno revidirati program svojih osiguranja, mora analizirati odnos s tvrtkom za posredovanje osiguranja, uspoređivati visinu premije s bonusima i isplaćenim štetama i decentralizirati sustav informiranja na one segmente organizacije koji su izloženi osiguranim rizicima. (Ćurak, Jakovčević, 2007.)

Osim što rizik mora biti osigurljiv, za upravljanje tim rizikom na strani osiguranika mora postojati volja da se rizik kontrolira i potpuno odsustvo namjere da se rizik ostvari.

U osiguranju je važno što točnije utvrditi veličinu rizika, tj. kvantitativno izmjeriti mogućnost nastanka štetnog događaja, a neki od faktora koji se uzimaju u obzir prilikom određivanja veličine rizika su:

- vrsta opasnosti (npr. požar, poplava..),
- fizičko – tehničke karakteristike predmeta osiguranja (razni materijali),
- veličina ili vrijednost predmeta osiguranja,
- trajanje osiguranja,
- mjesto gdje se nalazi predmet i drugo. (Bijelić, 2002.)

Poduzeća su izložena mnogim rizicima. Odabrana strategija upravljanja rizicima ovisi o karakteristikama poduzeća i izloženosti pojedinim vrstama rizika. Poslovni rizici s kojima se poduzeća susreću u prvom redu proizlaze iz njihove djelatnosti. Svaka djelatnost ima tipične rizike koji se pojavljuju tijekom poslovanja, a specifični su za određenu vrstu posla. To su na primjer promjene u navikama potrošača, sezonske oscilacije u potražnji, potreba i intenzitet kapitalnih ulaganja i slično. Generalno, rizik djelatnosti vezan je uz promjene koje nastaju zbog svjetskih trendova, promjena vezanih uz domaće tržište, navike i raspoloživ dohodak potrošača. Uz to, svaka djelatnost ovisi i o konkurenciji – novim poduzetnicima. Ukoliko se radi o djelatnosti koja donosi dobit, koja je u trendu i obećava buduće prihode, konkurencije će biti sve više. Sektori poput informacijske djelatnosti, zdrave hrane, komunikacije i drugo su sve popularniji u svijetu i sve je veći broj potrošača koji se uključuju u kupovinu takvih proizvoda. S druge strane, postoje neke tradicionalne djelatnosti koje imaju sve manje potrošača pa isto tako i konkurenata jer je profita u toj djelatnosti sve manje i sklonosti potrošača se okreću drugdje. Postoji i rizik načina poslovanja koji proizlazi iz činjenice da se svaka djelatnost može različito obavljati. Na primjer, način prodaje i kontakt s kupcima i klijentima može biti konzervativan ili može biti usmjeren novim oblicima. Rizik koji je najznačajniji za poduzeće je vezan uz donošenje poslovnih odluka – svaka poslovna odluka sa sobom donosi neku dozu rizika, a vezane su uz trenutačno poslovanje, nuđenje roba i usluga, određivanje cijene i slično. (Andrijanić, Gregurek, Merkaš, 2016.)

Klasifikacija rizika s kojima se susreću poduzeća ima više, no osnovne četiri vrste koje omogućuju daljnju detaljniju podjelu su:

- eksterni rizici – pravni, zakonski, tehnološki, politički, prirodni, tržišni, itd.,
- interni rizici – menadžerski, organizacijski, komunikacijski, kulturalni, personalni, rizici ponašanja, itd.,
- financijski – financijsko tržište, potraživanja, likvidnost, cjenovni, tečajni, itd. i
- operativni – prodaja, proizvodnja, razvoj, logistika, informacijsko-tehnološki rizici procesa itd. (Andrijanić, Gregurek, Merkaš, 2016.)

Informacijsko-tehnološki rizici zovu se i cyber rizici te su u današnjem svijetu jedni od vodećih problema većine poduzeća. To su rizici koji proizlaze iz korištenja elektroničkih podataka te korištenja telekomunikacijskih mreža i interneta, a klasificiraju se pod operativne rizike. (OECD, 2017.) Više o samim cyber rizicima je u sljedećem poglavlju.

Rizik najprije treba izbjeći – ukoliko je to moguće, a ako nije treba ocijeniti mogućnost kontrole gubitaka, zadržavanja rizika ili transfera rizika, prvenstveno putem osiguranja.

Svrha osiguranja je naknada za pretrpljenu štetu. Prilikom sklapanja ugovora, osiguranik dobiva jamstvo da će biti financijski kompenziran u slučaju nastanka osiguranog događaja. Naravno, prije isplate osigurnine, društva za osiguranje utvrđuju postojanje i visinu obveze te procjenjuju štetu, a taj postupak naziva se likvidacija štete. Nakon tog postupka, slijedi isplata osigurnine. Osigurnina je najčešće u novčanom obliku, no ugovorom o osiguranju moguće je ugovoriti i nenovčanu naknadu. Isplatom osigurnine osiguranik bi trebao biti financijski kompenziran s obzirom na štetan događaj koji je nastao, a prethodno je bio osiguran. (Ćurak, Jakovčević, 2007.)

2.4. Temeljne odrednice cyber osiguranja

Cyber osiguranje, osiguranje od cyber rizika, ili osiguranje od kibernetičke odgovornosti oblik je osiguranja koji služi za zaštitu poslovanja u modernom digitalnom dobu, u smislu zaštite od povrede podataka ili raznih hakerskih napada na računalne sustave. (Hiscox, 2022.)

Poduzeće je samostalno odgovorno za vlastitu cyber sigurnost, a kibernetički napad može dovesti i zaposlenike i klijente u opasnost. Putem osiguranja od cyber rizika poduzeću će biti pružena određena zaštita i pomoć ukoliko dođe do cyber napada. (Hiscox, 2022.) Osiguranje općenito pokriva odgovornost poduzeća za kršenje čuvanja podataka koji uključuju osjetljive podatke o klijentima, na primjer brojeve socijalnog osiguranja, brojeve kreditnih kartica, računa, vozačkih dozvola, zdravstvenih kartona i slično.

Cyber osiguranje u slučaju napada najčešće pokriva pravne, financijske i reputacijske troškove, a pomaže i u:

- obavještavanju klijenata o povredi podataka,
- obnavljanju ugroženih podataka,
- popravku oštećenih računalnih sustava,
- istrazi cyber napada,
- upravljanju ugledom,
- isplatama iznude koje traže hakeri i slično. (Nationwide, 2022.)

Ukoliko poduzeće koristi, šalje ili pohranjuje elektroničke podatke, postoje velike koristi od cyber osiguranja. Takvi podaci, bilo da pripadaju poduzeću ili su osjetljivi podaci o klijentima, ranjivi su na cyber napade, prilikom kojih bi osiguranje pomoglo s pokrivanjem troškova.

Troškovi cyber osiguranja ovise o više čimbenika. To uključuje i godišnji prihod poduzeća, industriju u kojoj poduzeće posluje, vrstu podataka koji se čuvaju i razinu mrežne sigurnosti. Određeni sektori su osjetljiviji na kibernetičke opasnosti pa će zato i zahtijevati višu razinu pokrivenosti pa ujedno imati i veće troškove osiguranja. Na primjer, sektor financija ili zdravstva, u kojem je pohranjena velika količina osobnih podataka, izložen je većem riziku od sektora ugostiteljstva ili slično. (Hiscox, 2022.)

Polica osiguranja sama po sebi naravno ne može smanjiti rizik, ali može djelovati kao mehanizam prijenosa rizika koji štiti poduzeće od velikog financijskog šoka. Većina osiguratelja koji nude police cyber osiguranja u svojoj ponudi imaju i druge usluge koje uključuju dostupnost IT stručnjaka koji pomažu prije ili poslije gubitka podataka te savjetuju o odgovarajućim postupcima i politikama koji pomažu da se održi najbolja informacijska sigurnost. (Bara, 2015.)

Prema Marshu (2018.), postoje i police osiguranja od cyber odgovornosti, koje popunjavaju nedostatke tradicionalnom osiguranju i pružaju izravnu zaštitu od gubitaka i odgovornosti od rizika koji nastaju korištenjem tehnologije i informacijskih podataka u svakodnevnom poslovanju. Takve police osiguranja su fleksibilne i omogućuju pružanje zaštite za sljedeće ključne izloženosti:

- zaštita za potraživanja koja proizlaze iz stvarnog ili navodnog neuspjeha računalne sigurnosti, da spriječi ili ublaži napad;
- zaštita za zahtjeve koji proizlaze iz otkrivanja ili pogrešnog rukovanja povjerljivim informacijama;
- pokrivenost se primjenjuje bilo da su informacije elektroničke ili tiskane;
- pokrivenost uključuje zaštitu subjekta od namjernih radnji lažnih zaposlenika;
- zamjenska odgovornost za kršenje privatnosti uzrokovano od strane dobavljača, trećih strana ili vanjskih poduzeća za poslovne procese;
- pokriće troškova povezanih s poštivanjem pravila o povredi privatnosti uključujući pravne i forenzičke troškove;
- pokriće za obranu od regulatornih mjera uključujući pokriće za procijenjene novčane kazne;

- zaštita imovine podataka – naknada za stvarne troškove nastale zbog vraćanja podataka organizacije i sredstva računalnog sustava koja su oštećena računalnim napadom;
- pokriće prekida poslovanja uključujući dodatne troškove – naknada za izgubljeni prihod, posljedice kvara tehnologije i slično;
- pokriće kibernetičke iznude – plaćanje otkupnine ili troškova istrage povezane s prijetnjom, plaćanje troškova otkrivanja, širenja, uništavanja, krađe ili upotrebe povjerljive informacije;
- pokriće fonda za kaznena djela;
- pokriće kriznog upravljanja.

Za razliku od drugih vrsta osiguranja, ne postoji standardizirani obrazac prema kojem se prodaje polica cyber osiguranja. To može uzrokovati neke izazove kod kupnje pokrića, pogotovo za one neupućene, no većinom daje pozitivne efekte zbog mogućnosti pregovora oko uvjeta cyber police. (Bara, 2015.)

Tržište cyber osiguranja za sada nije previše razvijeno, no kroz naredne godine očekuje se značajno povećanje. SAD po razvijenosti cyber osiguranja prednjači ispred Europe i Azije, no s vremenom, u Europskoj uniji očekuje se izjednačenje uvjeta. Najveći problemi za veći razvoj cyber osiguranja su nedostatak podataka i znanja o cyber rizicima, rizici konstantne promjene uvjeta, rizici akumulacije, potencijalni problemi moralnog hazarda i slično. (Eling, Schnell, Sommerrock, 2016.)

Osiguranje od cyber rizika pomaže menadžmentu za upravljanje cyber rizicima i trebalo bi biti jedna od ključnih strategija zaštite od cyber rizika. Za razliku od ostalih vrsta osiguranja, osiguranja za cyber rizike nemaju povijesnu pozadinu iz koje se mogu prikupiti podaci, pa je zato nedostatak podataka najveća prepreka u razvoju cyber osiguranja. Da bi se takva prepreka prevladala, ulogu će imati javno-privatna suradnja. (OECD, 2017.)

Općenito, zaštita informatičke infrastrukture je složen posao u kojem javni sektor bez suradnje i pomoći privatnog sektora ne može učinkovito podići razinu otpornosti, a privatni sektor bez javnih potpora bilo kroz odbitke ili druge pogodnosti, također ne može kompetentno upravljati cyber prijetnjama. Zbog toga, javno-privatna suradnja jedan je od temeljnih stupova politike cyber sigurnosti. (Cesarec, 2020.)

Prepreke tržištu cyber osiguranja:

- neizvjesnost o opsegu rizika i nedostatak aktuarskih podataka,

- neizvjesnost o tome koji se rizik osigurava,
- tehnološka evolucija – teško je biti u korak s najnovijim tehnologijama i rizicima koje nosi,
- teško je razlučiti što čini najučinkovitije mjere u upravljanju cyber rizicima,
- nedovoljno reosiguratelja i
- percepcija da postojeće osiguranje već pokriva cyber rizike. (ENISA, 2012.)

3. TEMELJNE ODREDNICE CYBER RIZIKA

3.1. Informacijska tehnologija u poslovanju

Informacije su u poslovanju jedan od ključnih resursa bez kojih je nemoguće donositi kvalitetne odluke. Za donošenje odluka nisu dovoljne informacije same po sebi, potrebno je poznavati i metode kojima se pronalaze racionalna rješenja problema, na primjer ekspertni sustavi, simulacija poslovnog procesa i slično. Kako bi se informacije kvalitetno prikupile i pohranile te učinkovito mogle pretraživati i koristiti za upotrebu različitih metoda donošenja odluka, nužna je informacijska tehnologija. (Čerić, Varga, 2004.)

Informacije se koriste na različitim radnim mjestima i u različitim odjelima u poduzeću. Velika poduzeća koja posluju u različitim gradovima ili državama moraju omogućiti većem broju ljudi korištenje i pristup bazama podataka i informacijskim sustavima, a to postižu putem računalnih mreža. Mreže računala u trenutku prenose informacije s jednog mjesta na drugo, neovisno o udaljenosti, što znatno povećava učinkovitost rada i smanjuje troškove, a ujedno omogućava i rad od kuće koji, posebice u današnje vrijeme pandemije, postaje sve popularniji. Računalne mreže omogućavaju zaposlenicima uključivanje na globalnu mrežu, Internet, te na taj način zaposleni pristupaju golemom broju izvora podataka, informacija, postižu komunikaciju s kupcima, distributerima i slično. Proizvodi i usluge se putem interneta mogu naručivati i kupovati, a mogućnost objavljivanja sadržaja i dijeljenja multimedijskih podataka s velikim brojem ljudi dovelo je do razvitka elektroničkog marketinga i drugih oblika elektroničkog poslovanja koji u današnje vrijeme prednjače. Sve navedeno dovodi do velikog napretka u odnosu na klasičan način poslovanja koji je zastario, a zaostajanje u primjeni računarskih i telekomunikacijskih sredstava znači i zaostajanje za konkurencijom što ujedno dovodi do smanjenja profita, većih troškova, gubitka dijela tržišta, a često i zatvaranja odnosno propadanja poduzeća.

Informacijska tehnologija je kombinacija mikroelektronike, telekomunikacije, softvera i računala koja omogućuje unos, obradu i distribuciju informacija. Ona prodire u sve sfere gospodarstva, znanosti, poslovnog, društvenog i privatnog života. Pojava računalnih mreža omogućila je jednostavnu i jeftinu komunikaciju te brz pristup, pretraživanje i racionalno korištenje informacija koje su smještene na različitim lokacijama. Omogućile su poduzećima komunikaciju i razmjenu informacija na daljinu što je dovelo do izuzetnog povećanja brzine i učinkovitosti rada. (Čerić, Varga, 2004.)

Informacijska tehnologija snažno je utjecala na živote i poslovanje ljudi. Elektroničko poslovanje obuhvaća elektroničko komuniciranje, rad u skupini na rješavanju zadataka, elektroničko trgovanje, multimedijsko publiciranje na internetu, korištenje elektroničkih publikacija i tako dalje. Takvo poslovanje dovodi do racionalnijeg poslovanja, do smanjenja potrebe za papirom, smanjenja troškova transporta, mogućnosti bržeg i kvalitetnijeg odlučivanja i slično, što dovodi do povećanja konkurentnosti poduzeća na tržištu.

Kako god, učinkovito obavljanje poslova zahtjeva kvalitetne informacije. Svaki poslovni sustav ima svoj informacijski sustav koji prikuplja, pohranjuje, čuva, obrađuje i isporučuje informacije važne za organizaciju, na način da budu dostupne i upotrebljive svakome kome je to potrebno. (Čerić, Varga, 2004.)

Informacijski sustavi sastoje se od ljudi, opreme, tehnologije i postupaka koji omogućuju navedeno prikupljanje i distribuciju podataka i informacija korisnicima, odnosno donositeljima poslovnih odluka. (Srića, Spremić, 2000.)

Informacijski sustav se može, ali i ne mora, koristiti informacijskom tehnologijom. (Čerić, Varga, 2004.)

IT je sredstvo konkurentske prednosti, organizacijske efikasnosti i učinkovitosti, što se može zaključiti iz sljedećeg:

- IT se istodobno pojavljuje na mjestima gdje se odvijaju procesi i nudi podršku odlučivanju većem broju ljudi koji izravno rade na tim procesima,
- odlučivanje više nije isključivo privilegija menadžera već svi zaposlenici raspolažu određenim informacijama koje im omogućuju donošenje nekih odluka,
- IT briše vremenska i zemljopisna ograničenja i omogućava rad od kud god je to potrebno,
- upotreba ekspertnih sustava zamjenjuje specijaliste generalistima,
- komunikacijska rješenja omogućuju prednosti i centralizacije i decentralizacije istodobno,
- IT omogućuje efikasnu povezanost s kupcima,
- IT se ugrađuje u proizvode čime se procesi automatski ubrzavaju, a krajnjim korisnicima se nudi kvalitetnija ponuda,
- IT podržava timski rad. (Srića, Spremić, 2000.)

Informacijska tehnologija, zaključno, omogućuje diferencijaciju proizvoda, niže cijene proizvoda ili usluga od konkurentske, ali uz istodobno povećanje kvalitete, skraćuje vrijeme razvoja, proizvodnje i distribucije proizvoda ili usluga, ili stvaranje novih, te poboljšava odnos s klijentima. Elektroničko poslovanje jest temelj modernog poslovanja i pokreće potpuno nove poslove te mijenja postojeće. (Srića, Spremić, 2000.)

Generalno, tehnologija i informacijski sustavi sami po sebi nemaju nikakve vrijednosti bez primjene na poslovanje i kreiranje novih pogodnosti i povrata na investicije (novi prihodi, profiti ili nove prilike). Zato je kooperacija između ljudi koji se bave informacijskom tehnologijom i onih koji su orijentirani na poslovanje poduzeća potrebna da bi funkcija IT-a kreirala i dodavala adekvatnu vrijednost i pomoć poslovanju. (Müller, 2001.)

IT u nekim djelatnostima ima strateško značenje dok u drugima utječe na poslovanje u smislu snižavanja troškova i povećanja produktivnosti. Na primjer, u zrakoplovnim kompanijama i bankama, IT ima stratešku važnost. S druge strane, društva za osiguranje i turističke agencije nisu strateški ovisne o IT-u, ali njegova primjena u poslovanju utječe, mijenja strukturu, nameće nove standarde i značajno unapređuje poslovne procese donoseći konkurentsku prednost. (Srića, Spremić, 2000.)

Jednako koliko informacijska tehnologija pruža mogućnosti za unaprjeđenje ljudskih djelatnosti, isto tako pruža mogućnost za razvoj različitih vrsta kriminala i zloupotrebe te povećava sigurnosne rizike poduzeća, no o tome više kasnije.

3.2. Definicija cyber rizika

Razvoj i rastuća kompleksnost, međuovisnost tehnologije i međusobna povezanost onemogućava potpunu zaštitu od cyber prijetnji. Direktor FBI-a, Robert S. Mueller, izjavio je: „postoje samo dvije vrste poduzeća: ona koja su hakirana i ona koja će biti hakirana. Pa čak i ona konvergiraju u jednu kategoriju: poduzeća koja su hakirana i ona koja će opet biti hakirana.“ (Bara, 2015.)

Pojam „cyber rizik“ odnosi se na mnoštvo različitih izvora rizika koji utječu na informacijsku i tehnološku imovinu poduzeća.

Definicija cyber rizika široka je, a može se bazirati na temelju načina na koji regulatori financijskih tržišta i tržišta osiguranja kategoriziraju cyber rizik – kao operativni rizik. No, u

fokusu je operativni cyber rizik koji se odnosi na sve rizike koji su relevantni i mogu se povezati s informacijskom i tehnološkom imovinom. Tako se cyber rizici mogu definirati kao operativni rizici za informacijsku i tehnološku imovinu koji posljedično utječu na povjerljivost, dostupnost ili integritet informacijskih sustava. Prema okvirima Basel II i Solvency II, cyber rizik dijeli se u četiri kategorije:

1. ljudske pogreške (npr. nenamjerni gubitak podataka od strane zaposlenika),
2. kvar sustava (npr. kvar hardvera),
3. neuspjeli interni procesi (npr. nedovoljno definirane odgovornosti) i
4. vanjski utjecaji (npr. požar, poplava). (Biener, Eling, Wirfs, 2014.)

Cyber rizici su, također, operativni rizici koji imaju potencijalno negativan učinak na cyber sigurnost. Spomenuta sigurnost su aktivnosti i mjere kojima se postiže cjelovitost informacija, autentičnost, povjerljivost i dostupnost podataka i infrastrukture unutar cyber prostora. Cyber prostor se može definirati kao cjelina unutar koje postoji razmjena informacija između mrežnih i informacijskih sustava. (Kovač, 2021.)

Cyber rizik je svaki rizik koji proizlazi iz korištenja elektroničkih podataka i njihovog prijenosa i transmisije i koji uključuje korištenje telekomunikacijskih mreža i interneta. Cyber rizik se, dakle, definira kao rizik koji nastaje zbog korištenja komunikacijske i informacijske tehnologije što uključuje i rizik ljudske pogreške i rizik zlonamjernog napada iz internog ili eksternog djelovanja (terorizam, hakeri, organizirani kriminal). (OECD, 2017.)

Cyber rizik najčešće je uzrokovan prirodnim katastrofama, ili zbog ljudskog djelovanja, neuspjeha ili cyber kriminala, cyber rata ili cyber terorizma. Takve rizike karakterizira međuovisnost, potencijalni ekstremni događaji, visoka nesigurnost u pogledu podataka te rizik promjene.

Pojam cyber označavaju dvije glavne komponente: elektronička komunikacijska mreža i virtualna stvarnost. Obje karakteristike razlikuju cyber rizik od drugih rizika. Virtualno označava nematerijalno, pa zato postoje poteškoće u procjeni gubitaka. Mreže su usko povezane s pojmom cyberspace, kiberprostor, koji se često koristi kao sinonim za Internet. Internet je mjesto nesigurnosti zbog javne domene, no cyberspace može biti bilo koja mreža koja povezuje IT sustave (npr. LAN, WAN, NSFNET, ARPANET). (Eling, Schnell, Sommerrock, 2016.)

„Cyberspace je skup međusobno povezanih računalnih mreža, uključujući usluge, računalne sustave, ugrađene procesore i kontrolere, kao i informacije u skladištu ili tranzitu.“ (Refsdal, Solhaug, Stolen, 2015., p. 25)

Nadalje, cyber rizici proizlaze iz korištenja cyber prostora, a prouzrokovani su cyber prijetnjom.

Cyber prijetnja sadrži komponentu vjerojatnosti – hoće li poduzeće biti meta cyber napada ili neće biti. Ta vjerojatnost može se u vremenu kretati od 0% (poduzeće nije napadnuto) do 100% (upravo to poduzeće trpi cyber napad). (Geer, Jardine, Leverett, 2020.)

U užem smislu, u nekim literaturama naglašava se da je važno razlikovati da cyber rizici nisu bilo koji rizici kojem su cyber sustavi izloženi. Na primjer, ukoliko je cyber sustav uništen zbog poplave, ne mora se definirati kao cyber rizik osim ako cyber prijetnja pridonosi uništenju. S druge strane, kršenje povjerljivosti ili gubitak dostupnosti podataka, zbog virusnih napada, su primjeri kibernetičkih rizika.

Postoje zlonamjerni cyber rizici i nezlonamjerni cyber rizici. Važno je znati razlikovati jedno od drugog, kako bi se njima uspješno upravljalo. Zlonamjerni cyber rizici su oni za koje se može potvrditi da su nastali, barem djelomično, zbog zlonamjerne prijetnje. Ukoliko nije postojala namjera i prijetnja, rizici su nezlonamjerni. Primjer zlonamjernog rizika je hakerski napad, a nezlonamjernog rizika je slučajna objava podataka na web stranicu koja je otvorena i javna. Također, neki rizici mogu biti mješavina zlonamjernog i nezlonamjernog. Na primjer, može doći do hakerskog upada u bazu podataka tijekom slučajnog kvara u sustavu. Takve situacije klasificiraju se kao zlonamjerne prijetnje i rizici jer bez zlonamjerne prijetnje ne bi došlo do gubitka. (Refsdal, Solhaug, Stolen, 2015.)

Prema Vukoviću (2012.), zlonamjerni cyber rizici proizlaze iz zlonamjernih aktivnosti kao što su:

1. cyber kriminal,
2. cyber špijunaža,
3. cyber terorizam i
4. cyber rat.

Cyber napadi se javljaju u 2 forme, ovisno o cilju – napad usmjeren na podatke i napad usmjeren na nadzorne sustave, no više o cyber incidentima u nastavku.

3.3. Izloženost cyber rizicima i zloupotreba informacijske tehnologije

Računalni kriminal postoji od samih početaka suvremenog računarstva. Primjeri računalnog kriminala su masovne krađe podataka, probijanje zaporki za pristup računalima korporacija ili vladinih organizacija, presretanje poruka pojedinaca i iz njih uzimanje podataka poput brojeva kreditnih kartica i slično. Neprekidno se pojavljuju i novi računalni virusi koji nakon aktivacije mogu izbrisati ili izmijeniti podatke, slati poruke onima koji su u sustavu računala i tako dalje. Kriminalci, ali i poduzeća, ugrožavaju privatnost pojedinaca na različite načine. Primjerice, mogu se prikupiti različite informacije o pojedincima koje kriminalcima omogućuju da troše tuđi novac ili koriste te informacije protiv pojedinaca. Organizacije često ugrožavaju privatnost svojih zaposlenika na način da pregledavaju njihovu elektroničku poštu, prate što gledaju i pretražuju na internetu i slično. Vladine organizacije također mogu pratiti privatne podatke pojedinaca, no to je najčešće u svrhu borbe protiv terorizma i kriminala. Ugrožavaju se autorska prava tako što se sadržaji besplatno objavljuju i koriste, a velik broj poduzeća neovlašteno prikuplja informacije o pojedincima pa ih kasnije preprodaje onima koji žele oglašavati putem interneta. (Čerić, Varga, 2004.)

Važno je uspostaviti i održavati različite sigurnosne sustave i zaštitne mehanizme koji omogućuju sigurnost informacijskih sustava. Sigurnosni sustavi usmjereni su na očuvanje podataka i informacija, odnosno na sprečavanje njihova uništenja, krađe, oštećenja ili neovlaštene uporabe. Osnovni sigurnosni zahtjevi su:

- sigurnost podataka i informacija,
- dostupnost podataka i informacija samo ovlaštenim korisnicima,
- tajnost podataka.

Mjere sigurnosti podataka uključuju fizičko osiguranje uređaja i nositelja podataka, planove aktivnosti u iznimnim okolnostima, instalaciju pričuvne opreme, arhiviranje podataka i tako dalje. Koriste se različiti alati za kriptiranje podataka, autentifikaciju korisnika, detekcije napada, ispitivanje stabilnosti i sigurnosti računalnih sustava i mreža, zaštite od virusa, zaštite prijenosa podataka, zaštita za pravo pristupa određenim podacima i slično. (Srića, Spremić, 2000.)

Da bi se smanjila izloženost cyber rizicima potrebno je provoditi 4 temeljne aktivnosti u poslovanju:

1. priprema – potrebno je razumjeti kritičnu imovinu poduzeća, razviti sposobnosti za rješavanje različitih rizika, utvrditi sklonost riziku i ugraditi upravljanje rizicima u cijelo poduzeće,
2. zaštita – osigurati cyber pripravnost, ocjenjivanje prijetnji i kontrola, osigurati provjeru procesa za treće osobe, osnažiti upravljanje incidentima,
3. detekcija – razviti sposobnost otkrivanja i kontinuiranog praćenja za rješavanje nepravilnosti,
4. poboljšanje – izgraditi sveobuhvatnu bazu podataka sigurnosnih incidenata i omogućiti oporavak od incidenta u što kraćem periodu. (Bara, 2015.)

Tablica 1: Gubici koji proizlaze iz cyber napada i IT propusta

GUBITAK	OBJAŠNJENJE
Cyber kriminal	Financijski gubitak kojeg je poduzeće pretrpjelo, a proizašlo je iz korištenja računala i mreža u svrhu prevare i krađe novca, vrijednosnih papira i slično.
Krađa intelektualnog vlasništva	Gubitak imovine u smislu gubitka intelektualnog vlasništva što dovodi do gubitka prihoda zbog smanjenog udjela na tržištu.
Prekid poslovanja	Gubitak prihoda zbog prekida rada IT sustava kao posljedice cyber napada.
Cyber iznuda	Trošak za rukovanje cyber incidentom, u kombinaciji s plaćanjem otkupnine.
Mrežne pogreške	Obveze prema trećim stranama ukoliko dođe do napada na treću stranu putem napada kroz IT sustav poduzeća.
Utjecaj na reputaciju	Gubitak koji proizlazi zbog smanjenja udjela kupaca ili transakcija, a izravno je povezano s objavom o povredi sigurnosti.
Fizičko oštećenje imovine	Gubitak koji nastaje zbog uništenja fizičke imovine zbog cyber napada.
Povreda privatnosti	Trošak istraživanja i odgovora na događaj povrede privatnosti trećih osoba, uključujući i kazne regulatora.
Smrt i tjelesna ozljeda	Odgovornost trećih osoba za smrt i tjelesne ozljede proizašle iz cyber napada.

Istraživanje incidenta	Troškovi nastali istraživanjem incidenta i smanjivanje gubitaka nakon incidenta.
Gubitak podataka i aplikacija	Trošak rekonstrukcije softvera i aplikacija koji su izbrisani ili korumpirani.

Izvor: Izrada autora prema Bara (2015.)

Industrije koje su najviše pogođene cyber napadima su:

- zdravstvo,
- proizvodnja,
- transport,
- financijske institucije i
- vlada. (Marsh, 2018.)

Povećanje međusobne povezanosti i globalizacija te komercijalizacija cyber kriminala dovode do sve većih i češćih cyber incidenata.

Važno je obratiti pozornost na činjenicu da nisu jedino velika poduzeća podložna cyber incidentima i napadima. Ono što privlači hakere su privatni podaci, vrijedne informacije, intelektualno vlasništvo i slično, a ne veličina poduzeća. Mala poduzeća za hakerske napade dosta su atraktivna, većinom zbog toga što nemaju tolike resurse kao velike tvrtke pa nemaju dovoljno dobru strategiju i zaštitu od cyber napada. Mala poduzeća često se više koriste online poslovanjem i različitim internetskim uslugama, zbog nižih troškova poslovanja. Imaju slabiju sigurnosnu zaštitu i osjetljivije su na širok raspon cyber napada. Slabosti malih poduzeća, zbog kojih postaju privlačnija hakerima (Bara, 2015.), jesu:

- nedostatak vremena, stručnosti i novaca za provedbu sveobuhvatnih sigurnosnih mjera,
- nedostatak IT stručnjaka,
- nedostatak svijesti o cyber rizicima,
- nedovoljna obuka zaposlenika,
- neuspjeh instaliranja i ažuriranja sigurnosne zaštite,
- outsourcing sigurnosnih mjera nekvalificiranim izvođačima i
- neuspjeh osiguranja krajnjih točki.

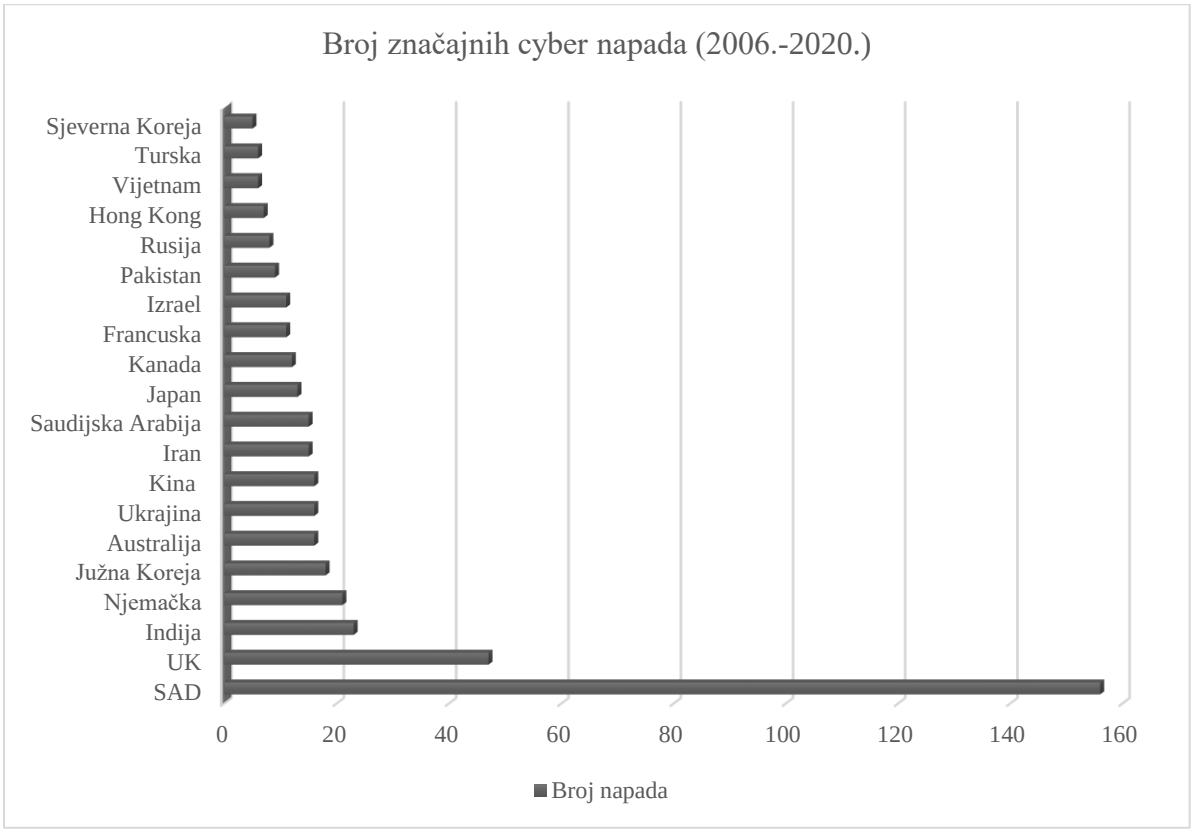
Hakerima je najprivlačnija situacija u kojoj je malo poduzeće, putem različitih složenih mreža i mobilnih veza, povezano s velikim poduzećem, kao npr. partnerom ili kupcem, pa im omogućava ulazak u unosnije tržište na „stražnja vrata.“ (Bara, 2015.)

3.4. Pregled cyber incidenata u svijetu, u Republici Hrvatskoj i odabranim zemljama

Cyber sigurnost u posljednjem je desetljeću, a i duže, postala jedna od vodećih briga u svijetu. Napadi i incidenti događaju se sve češće.

U sljedećem dijelu teksta navodit će se zemlje koje su najvećim dijelom pogođene i koje su doživjele najviše „značajnih“ cyber incidenata između 2006. i 2020. godine. „Značajni“ cyber incident ili napad može se definirati kao napad na državnu agenciju, vladu, obrambena i visokotehnološka poduzeća ili na napade koji su povezani s gospodarskim gubitkom većim od milijun dolara.

Grafikon 1: Broj značajnih cyber napada od 2006. do 2020. godine



Izvor: Specops (2020.)

Na grafikonu 1 vidljivo je da su Sjedinjene Američke Države doživjele najviše značajnih cyber incidenata, ukupno 156 u navedenom razdoblju. U 2018. bilježi se najveći broj napada, 30. Jedno od najnovijih problema u SAD-u otkrila je Agencija za nacionalnu sigurnost u svibnju

2020. godine. Naime, ruski hakeri koristili su tzv. „bug“ u e-pošti kako bi došli do osjetljivih podataka američkih organizacija.

Nakon SAD-a, Ujedinjeno Kraljevstvo je država s najviše značajnih cyber napada, prema Specopsu, njih 47. Taj broj uključuje i cyber napade velikih razmjera raspoređenih na digitalne platforme Laburističke stranke na izborima 2019. godine.

Na trećem mjestu je Indija, s 23 značajna cyber napada kroz navedeno razdoblje. Jedan od većih cyber napada na Indiju bio je u lipnju 2020. godine – napad na aktiviste i borce za ljudska prava kroz zlonamjerni softver koji je bilježio njihove pritiske tipki, snimao zvuk i krao osobne podatke.

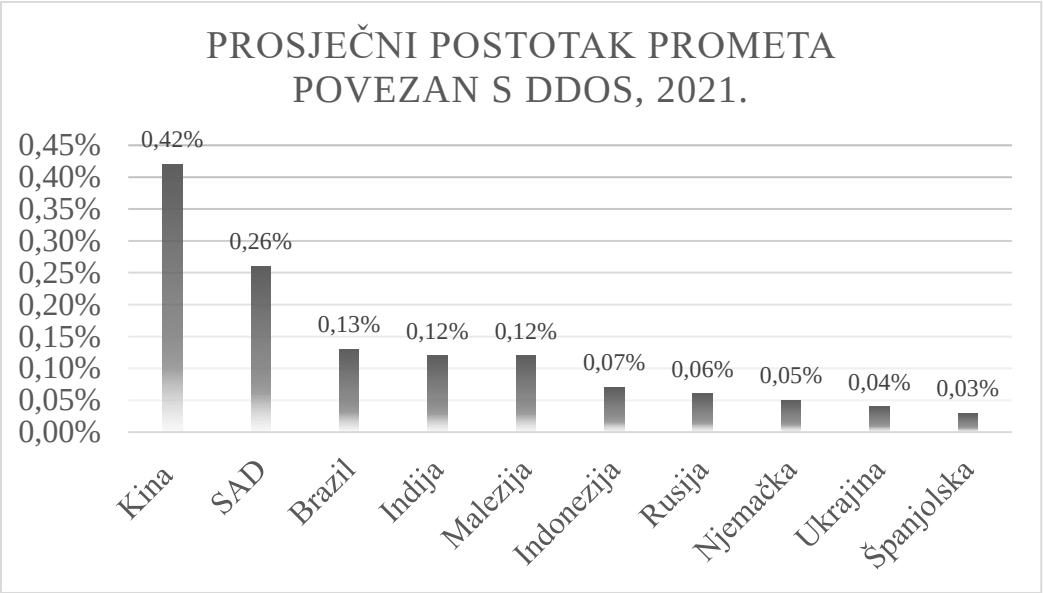
Njemačka broji 21 napad, Južna Koreja 18, a Australija na šestom mjestu, 16 napada. U Australiji je 2020. godine premijer Scott Morrison upozorio da su australijske tvrtke i usluge, kao i vladine agencije, na meti velikih i sofisticiranih hakerskih napada. Nakon Australije i Ukrajine, koja broji jednak broj napada koliko i Australija, slijede Kina, Iran i Saudijska Arabija s 15 značajnih napada, Japan s 13 te Kanada s 12. Francuska i Izrael broje samo 11 značajnih cyber napada u razdoblju od 2006. do 2020. godine, Pakistan 9, Rusija 8, Hong Kong 7, Turska i Vijetnam po 6. Sjeverna Koreja, za razliku od Južne Koreje, ima izrazito manji broj napada, njih 5. (Specops, 2020.)

U sljedećem dijelu teksta navest će se države iz kojih potječe najveći broj hakerskih napada uskraćivanja usluga – tzv. DDoS napada. DDoS napad, Distributed Denial-of-Service, je klasični cyber napad, relativno jednostavan za počinitelja. On uključuje usmjeravanje velike količine prometa na određeni sustav, kako bi se nadjačao njegov kapacitet i spriječilo daljnje obavljanje funkcija. Najjednostavniji primjer za DDoS napad je slučaj u kojem hakeri preplave web stranicu prometom pa je legitimni korisnici ne mogu učitati.

Prema Cloudflare-u, top 10 zemalja koje prednjače u DDoS napadima su: Kina, SAD, Brazil, Indija, Malezija, Indonezija, Rusija, Njemačka, Ukrajina i Španjolska. (Miller, 2022.)

Na grafikonu 2, podaci mjere postotak ukupnog prometa u zemlji povezanog s DDoS napadima.

Grafikon 2: Prosječni postotak prometa povezan s DDoS napadima



Izvor: Miller (2022.)

Vidljivo je da Kina prednjači s 0,42%, nakon nje SAD s 0,26%, Brazil s 0,13% te Indija i Malezija s 0,12%. Nakon prvih pet država dolaze Indonezija s prosječnim postotkom od 0,07%, pa Rusija s 0,06%. Zadnje tri su Njemačka s 0,05%, Ukrajina s 0,04% i Španjolska s 0,03%. Vrijedi napomenuti da navedeni popis država koje prednjače u DDoS napadima odražava većinu zemalja s najvećim brojem stanovnika u svijetu, izuzev Malezije, Ukrajine i Španjolske koje imaju relativno malu populaciju u usporedbi na ostale hakerske države.

Ostale zemlje koje su ušle u top 10 barem jedno tromjesečje u 2021. godini su Francuska, Argentina, Ujedinjeno Kraljevstvo i Tajland.

Zemlje koje također nisu na popisu, a Akamai (vodeća američka tvrtka za kibernetičku sigurnost) ih je u prošlosti svrstavao među najaktivnije hakerske zemlje na svijetu su Turska, Tajvan, Rumunjska, Italija i Mađarska. (Miller, 2022.)

3.4.1. Cyber incidenti u svijetu

U travnju 2021. podaci više od 530 milijuna korisnika Facebooka objavljeni su na internetu. Podaci su uključivali imena i prezimena, datume rođenja, status veze i Facebook ID-eve.

Audi i Volkswagen otkrili su povredu podataka, u lipnju 2021., koja je utjecala na više od 3 milijuna kupaca i potencijalnih kupaca, prvenstveno sa sjedištem u SAD-u. Za povredu je navodno kriv povezani dobavljač, koji je razotkrio podatke između kolovoza 2019. i svibnja 2021. godine.

Telekomunikacijska tvrtka T-mobile, u kolovozu 2021. pretrpjela je kibernetički napad koji je doveo do krađe podataka od oko 50 milijuna klijenata i potencijalnih klijenata. 21-godišnjak koji je izveo napad tvrdi da je skupio oko 106 GB informacija koje uključuju brojeve vozačkih dozvola, adrese klijenata i brojeve socijalnih osiguranja.

Tijekom 2020. usluge koje pruža Zoom aplikacija doživjele su veliki porast korištenja s obzirom na COVID-19 i rad od kuće, sastanke putem kamera, online nastavu i slično. U travnju 2020. dogodio se cyber incident nazvan Zoombombing koji je omogućio cyber kriminalcima da upadaju u privatne sastanke, pristupaju razgovorima, dijele uvredljive slike, videozapise i ekrane. Nakon toga Zoom je ažurirao aplikaciju s boljom sigurnosnom zaštitom.

Jedan od najznačajnijih cyber napada iz 2020. godine učinio je haker poznat pod imenom ShinyHunters. Haker je ukrao oko 386 milijuna korisničkih zapisa iz 18 različitih tvrtki od početka godine do srpnja. Napadač je objavio poveznice za baze podataka tih tvrtki, učinio ih besplatnim za preuzimanje i prodao podatke na internetu.

2013. u listopadu softverska tvrtka Adobe je pretrpjela cyber napad u kojem su hakeri ukrali podatke o kreditnim karticama od oko 3 milijuna njihovih korisnika. U napadu su također ukradeni podaci vjerodajnica za prijavu, korisnička imena, lozinke, a kasnije je otkriveno da su bili ukradeni i podaci o imenima korisnika, identifikacijski podaci te lozinke i podaci debitnih kartica. Adobe je platio korisnicima milijun dolara kao financijsku nagodbu zbog kršenja zakona od evidenciji kupaca i loše poslovne prakse. Također, nagodba je uključivala i odredbu da Adobe treba provesti sigurnosne mjere i dostaviti rezultate sigurnosne revizije.

LinkedIn je hakerska meta mnogih kriminalaca koji pokreću napade na društvene mreže. 2012. godine dogodio se prvi napad na LinkedIn kada su hakeri ukrali oko 6,5 milijuna lozinki koje su kasnije objavili na ruskom hakerskom forumu. Kasnije je otkrivena prava širina napada kada je uhvaćen haker koji je prodavao oko 165 milijuna lozinki i adresa e-pošte za 5 bitcoina koji je tada iznosio oko 2000 dolara. LinkedIn je potvrdio incident i poništio lozinke svim korisnicima koji su bili pogođeni.

Zynga, programer igara, u rujnu 2019. pretrpjela je cyber napad od strane pakistanske grupe hakera GnosticPlayers. Pristupili su bazi podataka Zynga igara te kompromitirali adrese e-pošte, lozinke, telefonske brojeve i korisničke ID-eve Facebooka i Zynge 218 milijuna ljudi. (Fortinet, 2022.)

U veljači 2022. godine više naftnih terminala u Belgiji i Njemačkoj bilo je žrtvom cyber napada. Nisu mogli obraditi dolaznu robu zbog soja „ransomware-a" – ucjenjivačkog softvera koji korisniku uskraćuje pristup računalnim resursima i traži plaćanje otkupnine za uklanjanje ograničenja, pa energetske tvrtke nisu uspjele obraditi plaćanja.

Kineski hakeri u prosincu 2021. provalili su u četiri američka obrambena i tehnološka poduzeća, i u jedan u studenom. Dobili su podatke i lozinke za pristup sustavima poduzeća te pokušali presresti osjetljivu komunikaciju.

Europska unija u rujnu 2021. službeno je okrivila Rusiju za sudjelovanje u cyber napadu „Ghostwriter", koji je ciljao na izbore i političke sustave nekoliko država članica. Od 2017. ruski operateri hakirali su račune državnih službenika na društvenim mrežama i web stranice s vijestima, s ciljem stvaranja nepovjerenja u američke i NATO snage. (CSIS, 2022.)

Još u 2011. nekoliko tvrtki koje pružaju sigurnost brodovima koji plove kroz „područje visokog rizika" bilo je podvrgnuto hakerskim napadima. Pirati su uspješno pristupili osjetljivim podacima o kretanju broda, teretima i njihovom osiguranju. Na takav način, mogli su planirati svoje daljnje radnje i tražiti otkupninu. Koristili su se zlonamjernim programima „key log" koji snimaju svaki pritisak na tipkovnicu i šalju informacije na e-poštu pirata, odnosno hakera.

Luka Antwerpen u Belgiji bila je pod hakerskim napadima od 2011. do 2013. koje su izveli sofisticirani krijumčari droge koristeći zlonamjerni softver, a i druge metode. Hakeri su uspješno otkrivali gdje se nalaze kontejneri s narkoticima te su slali vlastite vozače da pokupe robu prije nego bi pravi vlasnik došao po kontejner. Vlasti su shvatile da se nešto događa kada su počeli nestajati cijeli kontejneri.

U lipnju 2017. najveći kontejnerski operater Maersk pretrpio je ogroman cyber napad. Zlonamjerni softver „NotPetya" izazvao je potrebu za reinstalacijom više od 4.000 servera i 45.000 računala. Tvrtka je bila prisiljena transportirati i raditi 10 dana bez IT podrške. (Mraković, Vojinović, 2019.)

Prvi zabilježeni cyber napad dogodio se 1988. godine kada je diplomirani student na Sveučilištu Cornell, Robert Tappan Morris, razvio program za crve koji bi indeksirao web na način da

izbroji koliko je računala spojeno na Internet. Međutim, crv se instalirao na jedno od sedam računala te i natjerao ih da se sruše, zbog čega je nenamjerno postao prvi napad uskraćivanja usluge (DDoS). Crv je oštetio oko 6000 računala, što je tada činilo oko 10% cjelokupnog interneta.

Pojedinačni cyber napadi danas redovito kradu podatke stotina milijuna ljudi. (Fortinet, 2022.)

3.4.2. Cyber incidenti u RH

Poduzeća koja rade u Republici Hrvatskoj također nisu imuna na cyber napade. U RH prije ulaska u EU postojali su slučajevi cyber napada, no ulaskom u EU taj broj se značajno povećao, a napadi su postali veći i sustavniji. 2014. godine, nakon šest mjeseci uzastopnih cyber napada na korisnike internet bankarstva u Hrvatskoj, HNB je objavio da je prema dostupnim podacima otuđeno i plaćeno manje od 6% od potencijalno neovlaštenih transakcija u ukupnom iznosu od gotovo 1,8 milijuna kuna. (Bara, 2015)

U Republici Hrvatskoj, prema Hlača (2018.), u 2017. godini zabilježeno je 755 cyber incidenata u nadležnosti MUP-a i 732 incidenta u nadležnosti CERT-a. Svaki incident imao je izvorište napada u hrvatskoj domeni.

2015. godine dogodio se napad na Ministarstvo vanjskih i europskih poslova, prema podacima CERT-a. Napadači nisu došli do nikakvih povjerljivih podataka, no sam čin smatra se ozbiljnim ugrožavanjem nacionalne sigurnosti.

U 2019. godini vodeći tipovi cyber incidenata bili su krađa identiteta i web defacement – kompromitirano web sjedište s izmijenjenim izgledom ili sadržajem web stranice.

Također, trajala je phishing kampanja prema korisnicima jedne banke kada su na mail dolazile poveznice koje bi vodile na lažne stranice banke i tamo navodile klijente da se prijave u sustav. Nakon toga, uslijedio je e-mail phishing Hrvatske pošte.

U veljači 2020. godine dogodio se veliki napad na INU koja je bila meta zlonamjernog softvera koji je interno značajno utjecao na poslovanje. INA je imala problem s izdavanjem bonova za mobitele i elektroničkih vinjeta te naplate komunalnih računa. Neslužbena je informacija da su hakeri INU ucjenjivali s iznosom od 1500 Bitcoina, preračunavajući u domaću valutu, oko 100 milijuna kuna. (Tintor, 2020.)

Najnoviji hakerski napad u RH je onaj na drugog najvećeg telekomunikacijskog operatera u Hrvatskoj, A1. Napad se dogodio u veljači 2022. godine, a kompromitirani su osobni podaci od otprilike 200.000 građana. Haker je upao u središnji korisnički sustav A1 Hrvatska, u kojem operater pohranjuje sve podatke o svojim korisnicima. Haker je ucijenio A1 rekavši da će, ukoliko mu ne uplate pola milijuna dolara u kriptovalutama, objaviti podatke na dark webu. Treba napomenuti da je haker maloljetnik, a također i da je izjavio kako je A1 bio svjestan da je hakiran, ili da barem netko pokušava hakirati, minimalno 6 do 7 dana, bez da su išta poduzeli.

4. UPRAVLJANJE CYBER RIZICIMA

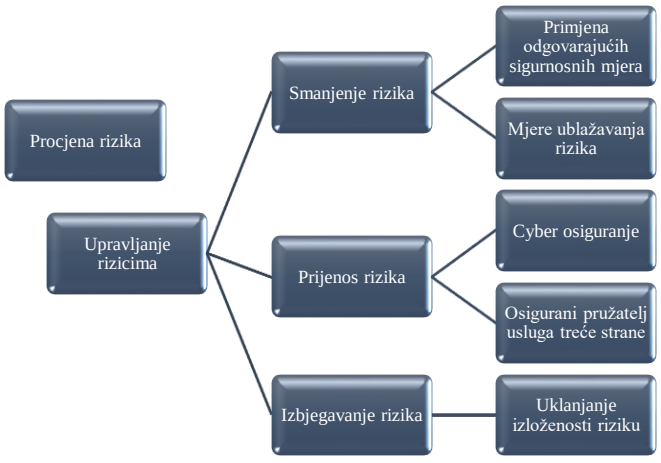
Cijeli proces upravljanja kibernetičkim rizicima obuhvaća primjenu metoda fizičke kontrole koja se odnosi na smanjivanje rizika kroz poduzimanje mjera kibernetičke sigurnosti. Metode fizičke kontrole inače uključuju i izbjegavanje rizika, no u slučaju kibernetičkih, to nije moguće. Naime, izbjeći takve rizike značilo bi provođenje poslovnih aktivnosti bez tehnologije i tehnoloških rješenja, što bi smanjilo efikasnost organizacije. S druge strane, upravljanje cyber rizicima obuhvaća i financijske metode koje uključuju zadržavanje rizika odnosno prijenos rizika na društva za osiguranje. Proces uključuje aktivnosti: identifikacija, kvantifikacija, integracija, prioritizacija, izbor i primjena metoda upravljanja rizicima te nadzor. (Kovač, 2021.)

Upravljanje cyber rizicima uključuje strategiju za koju se očekuje da je svi, odnosno većina implementiraju (Protrka, Marić, Plećaš, 2017.):

1. zaštita podataka,
2. tehnička koordinacija u obradi računalnih sigurnosnih incidenata,
3. međunarodna suradnja,
4. obrazovanje, istraživanje, razvoj i povećana svijest o sigurnosti u cyber prostoru.

Upravljanje cyber rizicima i sigurnošću jesu, prema Solar (2020.), radnje i politike koje usvajaju svi sudionici koji se koriste tehnologijom, civili, vojska, industrija, vlada i privatni sektor kako bi zaštitili digitalni prostor.

Slika 2: Upravljanje cyber rizicima



Izvor: Izrada autora prema Kopp, Kaffenberger, Wilson (2017.)

4.1. Identifikacija cyber rizika

Pod identifikacijom rizika podrazumijevaju se aktivnosti kojima je cilj identificirati, opisati i dokumentirati rizike i moguće uzroke rizika. Rizik je uvijek povezan s incidentom. Postoje tri elementa bez kojih ne može biti rizika – imovina, ranjivost i prijetnja. Bez imovine nema onoga čemu bi se moglo naštetiti, bez ranjivosti nema mogućnosti i načina nanošenja štete, a bez prijetnje nema uzroka štete. Dakle, identificiranje rizika provodi se identificiranjem prijetnje u odnosu na imovinu i razumijevanje kako prijetnja može dovesti do incidenta iskorištavanjem ranjivosti. (Refsdal, Solhaug, Stolen, 2015.)

Važno je naglasiti kako prilikom procjene rizika najviše zabrinjavaju sredstva poput informacija, informacijske strukture, mreža i usluga, a manje ono što dolazi kasnije, kao daljnja posljedica – reputacija, imidž, prihodi, tržišni udjeli ili zakonske usklađenosti, na primjer zaštita podataka i privatnost. Iako se kibernetički prostor i sustavi najčešće vežu uz virtualno i nematerijalno, važno je osvijestiti da cyber incidenti mogu utjecati i na zdravlje, život, okoliš. (Refsdal, Solhaug, Stolen, 2015.)

Identifikacija cyber rizika može se podijeliti na dvije glavne grane. S jedne strane, identifikacija zlonamjernih cyber rizika, i s druge strane identifikacija nezlonamjernih cyber rizika.

Identifikacija zlonamjernih cyber rizika dijeli se na:

- Identifikaciju izvora prijetnje – izvori prijetnji najčešće su ljudi, no postoje i neljudski napadi kao na primjer računalni virusi. No, i tada postoji svrha, namjera i motiv jer se takvi izvori prijetnji uvode namjerno. Kada postoji zlonamjerni softver koji je razvijen posebno za određeni napad, tada se osoba koja je razvila softver smatra izvorom prijetnje, ali inače je izvor prijetnje upravo zlonamjerni softver. Najčešće izvori dolaze izvana, no nekada mogu biti i interni.
- Identifikaciju zlonamjerne prijetnje – za svaki od izvora zlonamjerne prijetnje nastavlja se identificiranje prijetnje koja može proizaći iz tog izvora i izazvati štetu.
- Identifikaciju ranjivosti – istražuje se kontrola i obrambeni mehanizmi kako bi se utvrdila njihova snaga i primjerenost s obzirom na određene prijetnje. Također, provode se i testiranja koja provjeravaju može li, i koliko ozbiljno, izvor prijetnje pokrenuti napad i koji su mogući incidenti.
- Identifikaciju zlonamjernog incidenta – zapravo se identificira incident i posljedice koje će taj incident ostaviti na imovinu. (Refsdal, Solhaug, Stolen, 2015.)

Identifikacija nezlonamjernih cyber rizika je ponešto drugačija. S obzirom da ne postoji namjera ili motiv iza nezlonamjerne prijetnje, nije uobičajeno da se prvo identificira izvor prijetnje. Naprotiv, počinje se identifikacijom sredstava i imovine koja se može oštetiti i načini na koji može doći do oštećenja. Nakon toga identificiraju se ranjivosti i prijetnje koje mogu uzrokovati incident i na kraju se identificira nezlonamjerni izvor prijetnje.

- Identifikacija nezlonamjernog incidenta – primjerice, kod informacijske imovine treba istražiti kako su informacije pohranjene, kako se obrađuju u sustavu i cyber prostoru, kako se prenose, tko im ima pristup i tako dalje. Korisno je istražiti prijašnje incidente, nenamjerne štete i kako je do njih došlo, da bi se u budućnosti to izbjeglo.
- Identifikacija nezlonamjerne ranjivosti – potrebno je istražiti tehnički dio organizacije, kulturu, rutine, svijest, znanje i slične stavke u organizaciji i među zaposlenicima. Također, treba provjeravati i aktualizirati sigurnosne i obrambene mehanizme.
- Identifikacija nezlonamjernih prijetnji – koji nenamjerni događaji mogu prouzrokovati identificirani incident zbog utvrđenih ranjivosti, i kako? Također, važno je obratiti pozornost na vanjske sustave koje organizacije koriste, a mogu biti prijetnja ukoliko u njima dođe do štete.
- Identifikacija izvora prijetnje – odvija se na sličan način kao i identifikacija prijetnje. Tko su korisnici sustava i kako mogu uzrokovati nenamjerne ili slučajne događaje koji dovode do štete? Uz to, mora se obratiti pozornost i na neljudske izvore prijetnji, kao što su kvar hardvera ili drugih tehničkih problema, trošenja ili prirodnih katastrofa. (Refsdal, Solhaug, Stolen, 2015.)

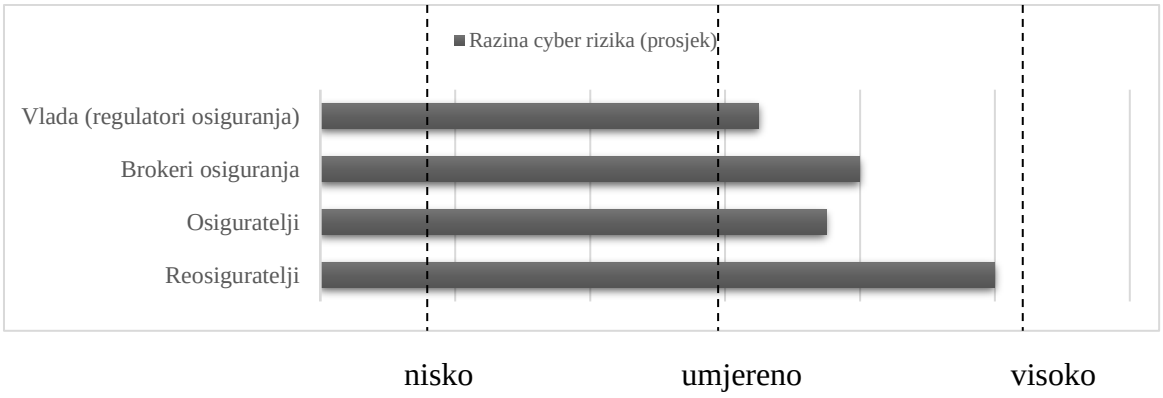
Cyber rizici i prijetnje iz dana u dan postaju sofisticiranije i obuhvaćaju nekoliko jurisdikcija zbog čega ih je teže pratiti i istražiti. Kod cyber napada u novo vrijeme postoji podjela poslova, odnosno može se reći da su cyber napadi industrijalizirani – za neke operacije postoji točna podjela posla, na primjer tržište za usluge hakiranja, tržište za razmjene podataka, za specijalizirane operatere i slično. Napadači surađuju i prekogranično pa dodatno otežavaju zaustavljanje napada ili pronalaske počinitelja. (Adelmann, Elliot, Ergen, Gaidosch, Jenkinson, …, Wilson, 2020.)

Slika 3: Upravljanje cyber rizicima

Izvor: Izrada autora prema Mraković, Vojinović (2019.)

Podaci ankete OECD-a iz 2016. godine o osiguranju cyber rizika:

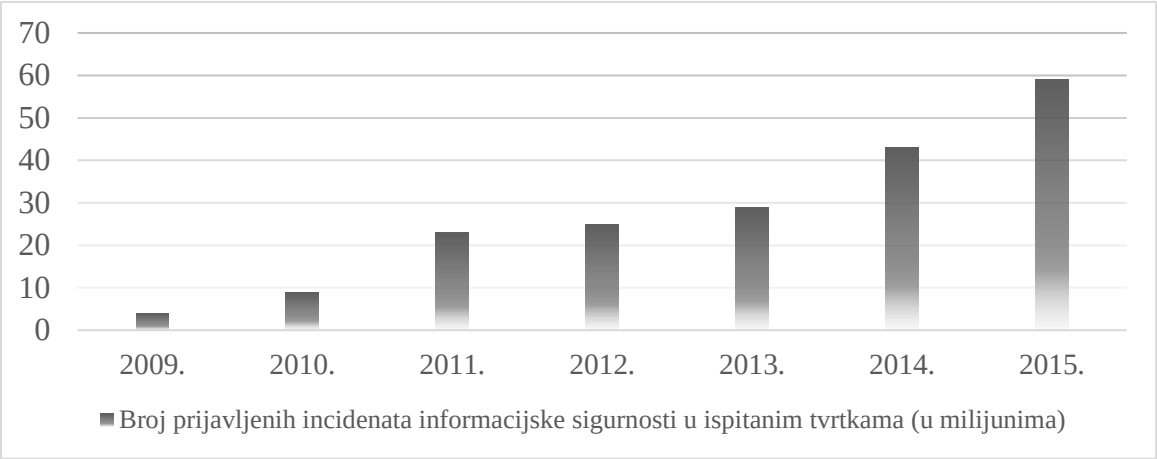
Grafikon 3: Percepcija o razini cyber rizika



Izvor: OECD, (2017.)

Ispitanici OECD-ovog upitnika o osiguranju cyber rizika općenito smatraju da su njihove zemlje i poduzeća suočena s umjerenom do visokom razinom cyber rizika i incidenata. U anketi nitko nije naveo da cyber incidenti ne predstavljaju rizik za njihove zemlje. (OECD, 2017.) Na grafikonu 3 vidljivo je da je među ispitanicima percepcija o razini cyber rizika najviša među reosiguratelјima i brokerima osiguranja, a najniža među regulatorima osiguranja.

Grafikon 4: Sve veća učestalost cyber incidenata

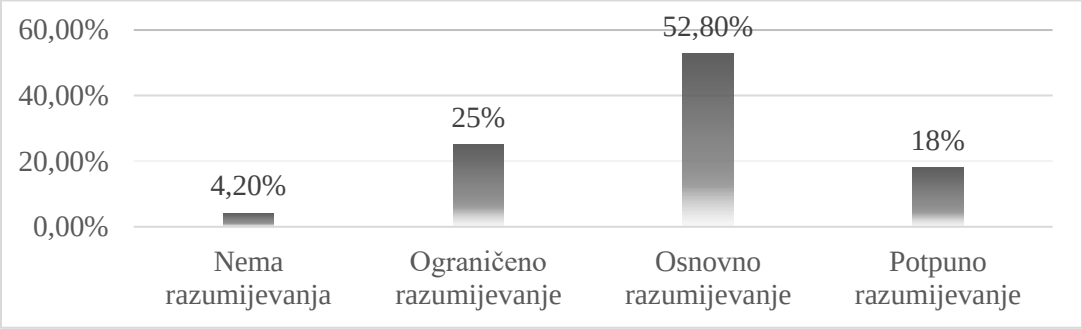


Izvor: OECD (2017.)

Oko 80% ispitanika smatra da se učestalost cyber incidenata i napada povećavala posljednjih godina. Na grafikonu 4 prikazan je broj incidenata koji se povećavao za prosječno 60% godišnje od 2009. godine – to je vjerojatno uključivalo kako stvarni porast incidenata, tako i poboljšanja u otkrivanju incidenata. (OECD, 2017.)

Podaci Marsha (2015.), prikupljeni u Ujedinjenom Kraljevstvu od strane stručnjaka za rizike i financijskih direktora velikih i srednjih organizacija:

Grafikon 5: U kojoj mjeri organizacija jasno razumije svoju izloženost cyber riziku?

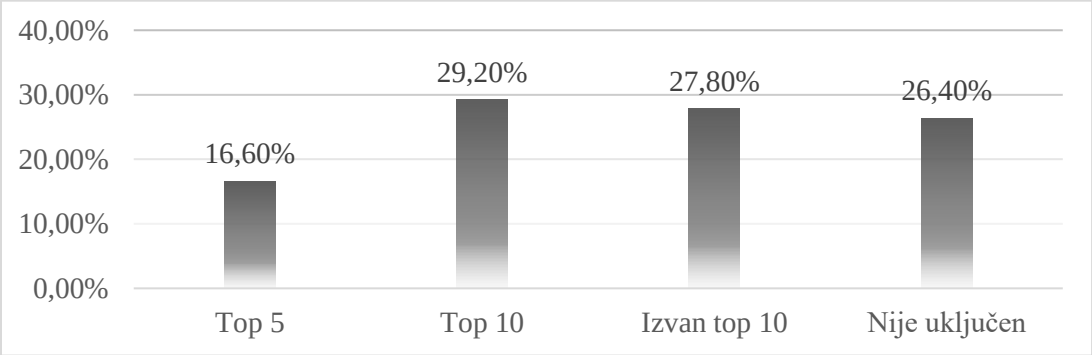


Izvor: Marsh (2015.)

Na grafikonu 5 prikazano je razumijevanje izloženosti cyber riziku od strane organizacije. U odnosu na prethodnu godinu, došlo je do pada postotka ispitanika koji smatraju da organizacija ima „potpuno razumijevanje“ o izloženosti cyber riziku; s 34% na 18%. (Marsh, 2015.) 52,8% ispitanika smatra da postoji „osnovno razumijevanje“ o izloženosti, 25% smatra da postoji „ograničeno razumijevanje“, a 4,20% je onih koji smatraju da razumijevanja uopće nema. Iz

priloženog je jasno da je potrebno više smjernica i pomoći za shvaćanje cyber rizika i izloženosti.

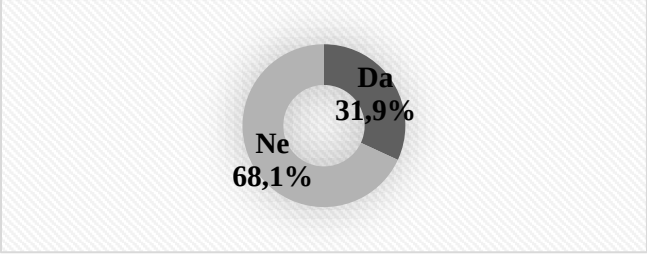
Grafikon 6: Gdje se nalazi cyber rizik u registru rizika u organizaciji?



Izvor: Marsh (2015.)

Samo 16,60% ispitanika stavlja cyber rizik u top 5 rizika u registru rizika, 29,20% u top 10, a ostatak izvan top 10. 26,40% ispitanika ni ne uključuje cyber rizik u registar rizika. Podaci su iznenađujući s obzirom da Nacionalna strategija sigurnosti Ujedinjenog Kraljevstva stavlja cyber rizik kao prvi stupanj prijetnje poduzećima. (Marsh, 2015.) Registar rizika jest dokument koji se koristi kao alat u upravljanju rizicima za prepoznavanje potencijalnih zastoja unutar organizacije i za cilj ima identificiranje, analizu i rješavanje rizika prije nego postanu problemi i poremete željene rezultate. (Ray, 2021.)

Grafikon 7: Je li identificiran jedan ili više cyber incidenata koji bi mogli najviše utjecati na organizaciju?



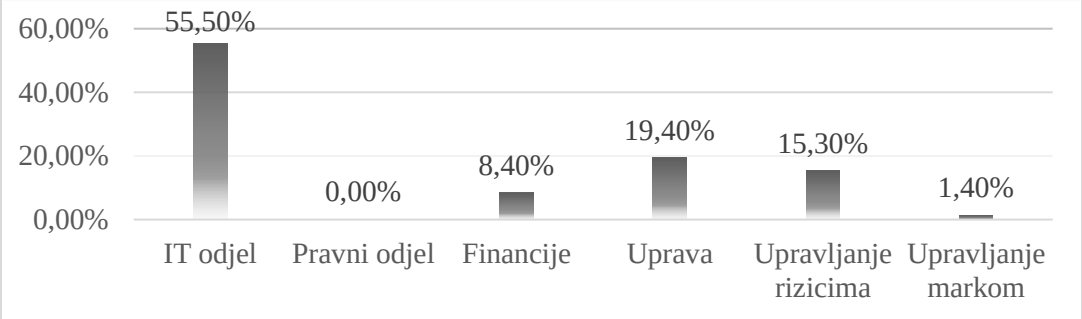
Izvor: Marsh (2015.)

Na grafikonu 7 vidljivo je da je 31,9% ispitanika, manje od trećine, identificiralo jedan ili više cyber incidenata koji bi najviše utjecali na njihovu organizaciju, a čak 68,1% nije.

Iz prethodnih grafikona vidljiv je nedostatak razumijevanja važnosti cyber rizika i štete te opasnosti koje oni mogu prouzročiti. S obzirom da je cyber rizik poslovni rizik, a ne samo

tehnički problem, potrebno je povećavati svijest o posljedicama incidenata uzrokovanih cyber rizicima, i ne samo od strane IT stručnjaka koji mogu i znaju implementirati kibernetičku sigurnost, već i od strane ostalih odjela organizacije kao i najviših razina.

Grafikon 8: Koji od sljedećih odjela preuzima primarnu odgovornost za pregled i upravljanje cyber rizicima?

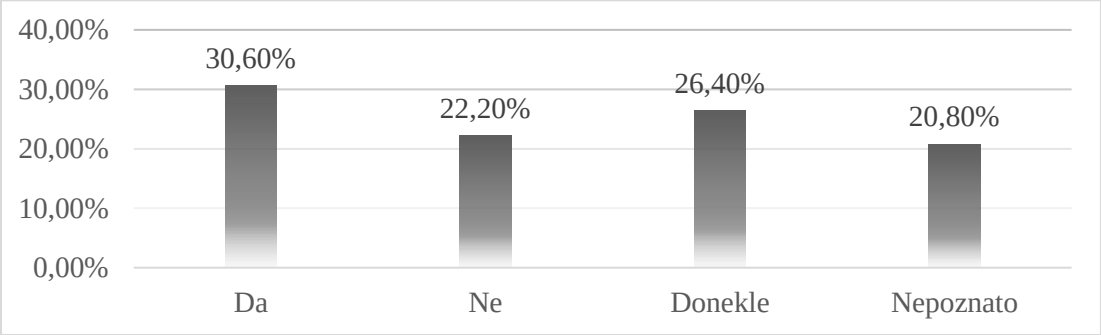


Izvor: Marsh (2015.)

Prema grafikonu 8, odgovornost za cyber rizik 2015. godine na razini uprave postoji u 19,40% britanskih organizacija, u skladu s rezultatima od prethodne godine (20%) što je poprilično niska razina. IT odjeli preuzimaju najveću odgovornost za cyber rizike, 55,50%. Upravljanje rizicima preuzima cyber rizik u samo 15,30% poduzeća, iako je cyber rizik postao sve više prepoznat i kao poslovni rizik. Odjel financija preuzima odgovornost za cyber rizik u 8,40% poduzeća, a upravljanje markom u 1,40%. (Marsh, 2015.)

Grafikoni 9 i 10 prikazuju u kolikoj su mjeri organizacije u Ujedinjenom Kraljevstvu 2015. godine bile pripremljene na cyber napade i incidente te se prikazuju očekivani izvori prijetnji koje bi najviše naštetile organizaciji. Iz navedenog može se uvidjeti identifikacija cyber rizika od strane britanskih organizacija i svijest o opasnosti koju uzrokuju.

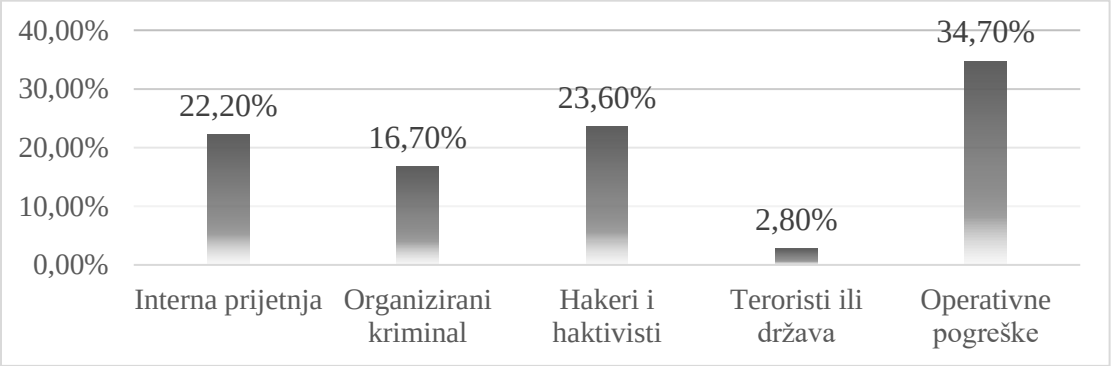
Grafikon 9: Posjeduje li organizacija plan odgovora i oporavka za moguće cyber napade?



Izvor: Marsh (2015.)

30,6% organizacija posjeduje plan odgovora i oporavka za potencijalni cyber incident, a čak 22,20% organizacija ne posjeduje uopće.

Grafikon 10: Odakle proizlaze najveće cyber prijetnje za organizaciju?



Izvor: Marsh (2015.)

Najveće cyber prijetnje za britanske organizacije, na temelju upitnika iz 2015. godine, proizlaze iz operativnih pogrešaka, čak 34,70%. Hakeri i interne prijetnje predstavljaju sljedeće najveće cyber prijetnje, nakon njih dolazi organizirani kriminal, a teroriste ili državu najvećom cyber prijetnjom smatra samo 2,80% ispitanika.

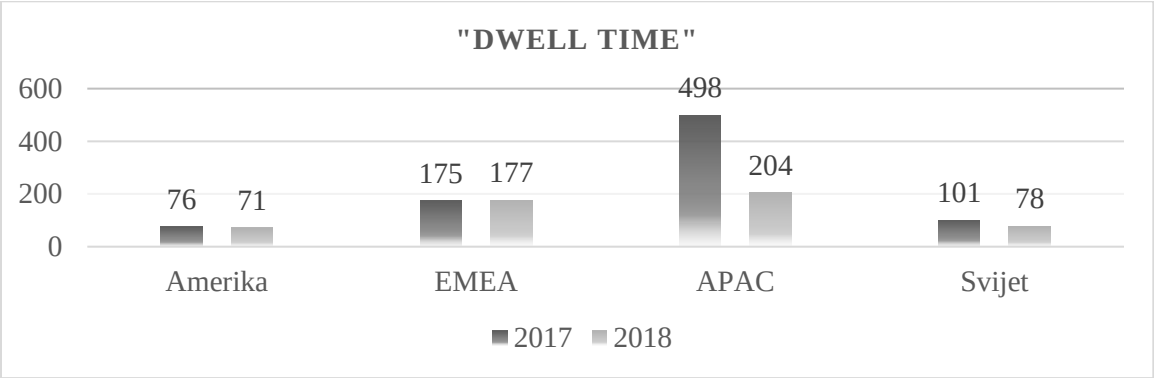
Istraživanje u 2016. godini, za europske zemlje, pokazalo je da postoji napredak u razumijevanju i u razumijevanju važnosti i problematičnosti cyber rizika, no i dalje ostaje nisko. 2015. postotak organizacija koje tvrde da razumiju svoju izloženost cyber riziku iznosio je 21%, dok 2016. iznosi 31%. Također, postotak organizacija koje cyber sigurnost stavljaju među top 5 rizika, povećao se sa 17% u 2015. na 32% u 2016, a postotak organizacija koje ne uključuju cyber rizik u svoj registar rizika smanjio se s 23% u 2015. na 9% u 2016. godini. Unatoč tom napretku, Europa, kao i ostale zemlje svijeta imaju dugačak put da dođu u korak s vremenom u kojem najviše prijete kibernetički napadi.

Vrijedi napomenuti da je situacija u Europi lošija nego u SAD-u. Europskoj uniji potrebno je tri puta više vremena od globalnog prosjeka da bi otkrili cyber napad. „Vrijeme zadržavanja“ odnosno „dwell time“ – vrijeme od napada do otkrivanja napada – u Europi trajalo je u prosjeku 469 dana, za razliku od globalnog prosjeka od 146 dana. Važno je da se vrijeme identifikacije svede na što manje razdoblje, jer dugo vrijeme zadržavanja hakerima omogućava otvaranje drugih vrata u sustavima koji su napadnuti. Naravno, prilikom identifikacije napada, sustav će odmah biti isključen, pa će se onemogućiti daljnji incidenti. Za usporedbu, europska poduzeća otkrivala su oko 12% upada u sustave s vanjske strane, dok su američka poduzeća, njihove

tvrtke za kibernetičku sigurnost i tajne službe, otkrile oko 53% hakerskih napada. (Marsh, McLennan, 2017.)

Na grafikonu 11 prikazano je „vrijeme zadržavanja“ u Americi, Europi, Bliskom istoku i Africi (EMEA), Aziji i Pacifiku (APAC) i u svijetu. Uspoređene su 2017. i 2018. godina. Vidljivo je da je u svijetu situacija u 2018. godini bolja s obzirom na 2017.; sa 101 dana, „dwell time“ smanjio se na 78 dana. Azija i Pacifik imaju vrijeme zadržavanja od 204 dana u 2018. godini, najduže od svih regija u svijetu, no vrijedi naglasiti da se s obzirom na 2017. godinu i 498 dana, to vrijeme znatno smanjilo.

Grafikon 11: Situacija u 2018., prema istraživanju Yeo, Ende (2019.), popravlja se:



Izvor: Yeo, Ende (2019.)

Kibernetički trendovi i statistike prema Softactivity-u u 2022. godini:

- tržište cyber sigurnosti globalno raste prema ukupnoj godišnjoj stopi rasta za 10,9%;
- pandemija COVID-19 u 2020. godini izazvala je velik porast kibernetičkog kriminala i phishing napada – rad od doma i nedovoljni sigurnosni protokoli takvog rada su najvjerojatniji razlozi povećanja napada;
- zdravstvo je najugroženija industrija za povredu podataka – u 2020. zdravstvo je izgubilo oko 7,18 milijuna dolara;
- potrebno je u prosjeku oko 280 dana da se otkrije, identificira i zaustavi cyber napad;
- oko 95% cyber incidenata posljedica je ljudskih pogrešaka;
- Google je otkrio više od 2 milijuna stranica za krađu identiteta u 2020. godini. (Softactivity, 2022.)

S obzirom na sve navedeno, zaključuje se važnost pravovremene identifikacije rizika, efikasno upravljanje tim rizicima i zaštita. S vremenom, iz godine u godinu, poduzeća i ljudi u globalu počinju uviđati moguće katastrofalne posljedice koje cyber prijetnje i incidenti mogu

prouzrokovati. Zbog toga, poduzeća počinju cyber rizike svrstavati među najvažnije i najveće rizike s kojima se danas susreću, a strategije i upravljanja takvim rizicima postaju česte teme brojnih znanstvenih članaka i literatura. U upravljanju cyber rizicima društva za osiguranje definitivno su jedan od najvažnijih načina za što bolju zaštitu od cyber napada odnosno od posljedica koje taj napad donosi. U narednom dijelu teksta govorit će se o ulozi koju društva za osiguranje imaju u upravljanju cyber rizicima i koliko je, te je li dovoljno, takav način osiguranja iskorišten, koliki je značaj i uloga društava za osiguranje u cyber incidentima te na koje načine se cyber rizici mogu smanjiti i cyber incidenti ublažiti pomoću osiguranja.

4.2. Preporuke i strategija smanjivanja rizika cyber osiguranjem

Osiguranje imovine i odgovornosti dostupno je u većini zemalja i na svakom tržištu osiguranja diljem svijeta. Takva osiguranja generalno pokrivaju štetu većinom samo na fizičkoj imovini, proizvodnom pogonu i slično, te isključuju cyber rizike. Kao odgovor na takvu situaciju, pojavilo se specijalizirano tržište upravo za cyber rizike, najvećim dijelom u SAD-u. Za sada još uvijek osiguranja za cyber rizike nisu pretjerano popularna i iskorištena, no iz godine u godinu postaju sve poželjnija. U 2014. godini, u Europi je postojalo čak 25% poduzeća koja nisu bila ni svjesna da osiguranja za cyber rizike postoje, a samo je 10% poduzeća u svom poslovanju koristilo i kupovalo police osiguranja za takav rizik. (Biener, Eling, Wirfs, 2014.)

Postojale su brojne prepreke i problemi za razvoj cyber osiguranja u prošlosti:

- Razvoj učestalosti i težine gubitaka: prije 2000. godine gubici zbog cyber rizika bili su relativno niski, ponajviše zbog ograničenih mogućnosti korištenja digitalizacije i tehnologije. Tokom godina, razvojem tehnologije, povećavali su se gubici nastali zbog kibernetičkih rizika pa se povećavala i potreba za osiguranjem.
- Udruživanje rizika: korelacija između kibernetičkih rizika relativno je visoka u odnosu na ostale rizike – diverzifikacija rizika je problematična i teško ostvariva.
- Manjak podataka: glavni problem kod osiguranja cyber rizika je nedostatak podataka i nedostatak razumijevanja takvih rizika. Problem proizlazi i zbog visoke razine neizvjesnosti za osiguratelja, pa ujedno nude nisko maksimalno pokriće što rezultira neprivlačnim policama osiguranja za menadžere.
- Rizik promjene: cyber rizici veoma su dinamični, promjene su često drastične i brze pa su i analize povijesnih podataka često nesigurne s obzirom na moguće značajne

promjene u riziku. Brojni su tehnički aspekti, napredak u hardveru i softveru, korištenje novih mreža i slično, koji mijenjaju cyber rizike.

- Informacijske asimetrije: negativna selekcija i moralni hazard često su smatrane primarne prepreke za razvoj tržišta cyber osiguranja. Međusobno povezana priroda informacijskih sustava otežava otkrivanje, a još više dokazivanje izvora gubitaka i identiteta počinitelja, što smanjuje ulaganje poduzeća u samozaštitu od cyber rizika. Dokazano je da poduzeća koja su doživjela cyber napad radije kupuju osiguranja nego što ulažu u samozaštitu, što dodatno povećava negativnu selekciju.
- Vrijednost proizvoda: police cyber osiguranja sadrže značajna isključenja kao što su samonaneseni gubitak, pristup nesigurnim web stranicama, isključuju se neizravni troškovi, na primjer gubitak ugleda. Zbog toga, mnogi korisnici preispituju vrijednost i svrhu tog osiguranja. (Biener, Eling, Wirfs, 2014.)

Zaključno, važno je uspostaviti minimalne standarde o ograničenjima pokrića, procjenu rizika prije pokrića, kao i jasnije definicije cyber rizika. Usluge savjetovanja i procjene rizika od strane osiguratelja, prije ponude za osiguranje cyber rizika povećat će potražnju. Navedeno bi trebalo smanjiti, ako ne i eliminirati barem neke od najčešćih i najvećih problema osiguranja cyber rizika. (Biener, Eling, Wirfs, 2014.)

Prema Insurance Europe (2019.) najveće prepreke cyber osiguranju pri postajanju mainstream proizvod su:

- teško je kvantificirati i procijeniti cyber rizike,
- neizvjesnost potencijalnih budućih gubitaka i teško procjenjivanje mogućih gubitaka nastalih iz cyber incidenta,
- visoko povezani rizici zbog raširene uporabe određenih operacijskih sustava,
- malo dostupnih podataka; osiguratelji koriste aktuarske i povijesne podatke da bi modelirali gubitke, ali u slučaju cyber rizika i incidenata, takvih podataka je malo, ili ih nema,
- veliki nematerijalni gubici – teško je kvantificirati štetu koja je povezana s npr. gubitkom ugleda.

Koje su najvažnije predispozicije za održivost osiguranja od cyber rizika?

- Na izvoru rizika mora biti dovoljno otpornosti, tj. moraju biti provedene određene mjere zaštite. Da vlasnici ne zaključavaju kuću u kojoj žive, ne bi mogli osigurati krađu. Dakle, da bi cyber rizik mogao biti osiguran, potrebno je provesti tri glavna koraka:

procjena, mjerenje i upravljanje. Višak rizika, koji preostane nakon poduzetih mjera, može se osigurati.

- Osiguratelji moraju ostvariti prihvatljiv povrat kapitala – zahtijeva opširnu procjenu rizika.
- Kapital mora biti dovoljan da nakon napada osigura adekvatne naknade osiguranicima. (Stajšić Golijanin, 2020.)

Tržište cyber osiguranja u novije vrijeme postalo je specijalizirano i inovativno. Uključeni su proizvodi za mala i srednja poduzeća, za srednje tržište, ali i za velike multinacionalne korporacije. Većina cyber proizvoda ima slične karakteristike, ali na tržištu postoji veliki raspon ponuđenih proizvoda, kao i politike ograničenja (koliko se cyber osiguranja može kupiti). Nedostatak standardizacije cyber osiguranja pokazuje da je cyber osiguranje relativno novije osiguranje, pokazuje njegovu evoluciju iz postojećih proizvoda i konkurentsku prirodu poslovanja. U većinu polica osiguranja uključeno je pokriće za izloženost prve i treće strane (gubitak ili oštećenje digitalne imovine), oporavak podataka, prekid poslovanja, troškove obavijesti, odgovornost za povrede podataka, multimedijsku odgovornost, nepoštenje zaposlenika, cyber iznudu i regulatorne troškove obrane. Također, osiguratelji nude i niz usluga svojim korisnicima, kao što su krizni menadžment, forenzički IT, sigurnosne savjete i pravne konzultacije. Već spomenuto, osiguratelji i regulatori dovode u pitanje potencijal za agregiranje cyber rizika, odnosno sistemski rizik, pri čemu jedan događaj izaziva višestruke gubitke za više društava za osiguranje. Posebnu zabrinutost iz perspektive agregacije izazivaju aktivnosti napadača koje sponzorira država ili terorističkih napadača, koji možda nisu motivirani novčanom dobiti, već željom da prouzrokuju štetu i poremećaje nacionalnoj infrastrukturi i gospodarstvu. (Camillo, 2017.)

Prijenos rizika je, dakle, moguć kupnjom ugovora o osiguranju. No, najvažniji dio strategije i planiranja upravljanja rizikom je smanjenje i ublažavanje rizika, a onda u kombinaciji s time, prijenos rizika. Kao što je već rečeno, izbjegavanje rizika kao način upravljanja rizikom, u slučaju cyber rizika nije moguć, jer bi to značilo da se poduzeća moraju odreći korištenja tehnologije i digitalizacije, što bi svakako rezultiralo puno većim gubicima nego što je „suživot“ sa cyber rizikom. Osiguratelji neće pristati na ugovaranje osiguranja ukoliko nema politike smanjivanja rizika i zaštite sustava od strane potencijalnog korisnika osiguranja. Prilikom ugovaranja osiguratelji će analizirati, procijeniti i provjeriti učinkovitost takvih alata. Te procjene mogu povećati svijest o cyber rizicima i koliko su velik i važan dio ukupnog portfelja rizika.

Poduzeća se mogu odlučiti i za strategiju samoosiguranja. U tom slučaju, poduzeće će samo plaćati štetu i gubitke. Tada kapital mora biti uštеđen unaprijed i služiti kao zaštita. Osim akumulacije kapitala, potrebno je uspostaviti smjernice za hitne slučajeve te kontinuirano pratiti rizike. Učinkoviti plan za upravljanje krizom jedan je od glavnih preduvjeta za uspješno i adekvatno rješavanje problema nastalih zbog cyber rizika. Strategije cyber napada stalno se mijenjaju pa je od strane menadžmenta potrebna prilagodba. Razmjena informacija, temeljita komunikacija, povećanje znanja i svijesti o cyber rizicima i sigurnosti te prihvaćanje stalne promjene procesa upravljanja tim rizicima, temelj su dobrog upravljanja njima. (Eling, Schnell, Sommerrock, 2016.)

Da bi se cyber rizici smanjili zbog korištenja cyber osiguranja, trebalo je popularizirati takva osiguranja te omogućiti osigurateljima što lakše poslovanje s obzirom na prepreke koje postoje pri osiguranju cyber rizika.

Preporuke za poboljšanje i povećanje tržišta cyber osiguranja i smanjivanje cyber rizika:

- Što osiguratelji mogu učiniti:
    - udruživanje osiguratelja cyber rizika u „pool“-ove (akumuliranje rizika iste vrste u jednom portfelju, dijeljenje podataka i stručnosti, udruživanje resursa i preuzimanje teških rizika...),
    - uspostavljanje anonimiziranih podatkovnih „pool“-ova (prikupljanje podataka od prijašnjih cyber napada, prikupljanje znanja i načina rješavanja incidenata, itd.),
    - organiziranje reosiguravajućih „pool“-ova,
    - suradnja s drugim dioničarima na podizanju svijesti o potrebi osiguranja cyber rizika,
    - provoditi analize scenarija, pratiti tehnološki razvoj (npr. block chain tehnologija, računalstvo u oblaku i slično), poboljšati vlastite analitičke vještine, napraviti vlastiti IT otpornijim,
    - prodaja i upravljanje rizicima trebaju steći specifično tehničko informatičko znanje kako bi se cyber rizik razumio – nedostatak razumijevanja, kako na strani potražnje, tako i na strani ponude, je glavna prepreka razvoja tržišta cyber osiguranja.
- Što vlade mogu učiniti:
    - boriti se s kibernetičkim kriminalom međunarodnom suradnjom,

- pokrenuti globalne pokrete usmjerene na ograničavanje i sprečavanje cyber ratova,
- povećavati otpornost IT-a,
- podržati razvoj cyber baza podataka i uvesti zahtjeve za izvješćivanje,
- uvesti minimalne standarde za smanjenje rizika,
- stvarati javno-privatna partnerstva između vlade i osiguratelja kao osiguratelje u krajnjoj nuždi (za ekstremne scenarije),
- potaknuti razvoj anonimizirane baze podataka,
- olakšati razvoj tradicionalnog i alternativnog mehanizma prijenosa rizika. (Eling, Schnell, Sommerrock, 2016.)

Strategije vlade na nacionalnoj razini trebaju potaknuti standardne sigurnosne prakse koje trebaju koristiti vladine agencije, poduzeća i građani u svakodnevnom korištenju kibernetičkog prostora. Ciljevi takvih strategija trebali bi definirati nedostatke, pronalaziti rješenja za te nedostatke, procijeniti napredak i ponavljati to. Strategija vlade ne bi smjela biti usmjerena na kontroliranje razine sigurnosti na internetu od strane vlade, jer od toga nema velike koristi. Treba se usredotočiti na elimininiranje ili zaštitu ranjivosti koje omogućuju napade i na pokušaj što boljeg rješenja situacije kada dođe do incidenta – putem osiguranja. I Republika Hrvatska je 2015. godine donijela Nacionalnu strategiju o cyber sigurnosti. (Galinec, Možnik, Guberina, 2018.)

Cyber osiguranje ima veliki potencijal da na razini Europske unije poveća cyber elastičnost – u SAD-u je cyber tržište puno razvijenije nego u Europi, pa je u zemljama Europe potrebo veće ulaganje u takvo osiguranje. Preporuke za kreatore politike EU, prema Insurance Europe (2019.):

- promicati podizanje svijesti,
- podrška javno-privatnim suradnjama za katastrofalne rizike,
- poticanje država članica da djeluju na povećanje cyber sigurnosti,
- podrška nastojanjima da podaci o cyber incidentima budu dostupni – na takav način se osigurateljima olakšava poslovanje i povećava se ponuda cyber osiguranja.
- ne uvoditi standardizaciju koja može naštetiti i kupcima i osigurateljima,
- ne uvoditi obvezno osiguranje za kibernetičke rizike jer bi to bilo kontraproduktivno.

Cyber osiguranje, kao zaključak svega navedenog, ima puno prepreka za puno ostvarenje, no u zadnjim godinama i potražnja i ponuda takvog osiguranja raste, informacije se prikupljaju, a

znanje i analize se povećavaju. Postoji sve više stručnjaka, na primjer brokera takvih osiguranja koji procjenjuju, analiziraju i pomažu osiguratelјima i korisnicima pri odabiru i slaganju individualnog cyber osiguranja. Cyber osiguranje jedna je od važnijih strategija prilikom „borbe“ protiv kibernetičkih rizika, uz mjere smanjivanja rizika i zaštite od tih rizika. Zaštita je dobar preventivni način obrane i upravljanja rizikom, no kad-tad do incidenta će doći, a tada je potrebno određeno osiguranje da bi se spasilo što se spasiti može i da poduzeće dobije barem dio onoga što je izgubilo, u materijalnom smislu, te na taj način bude manje oštećeno. Veliki troškovi proizlaze iz cyber napada te je osiguranje kao strategija upravljanja važan faktor.

4.2.1. Ponuda cyber osiguranja

Ponuda cyber osiguranja danas još uvijek nije dovoljna s obzirom na učestalost cyber incidenata u svijetu. Društva za osiguranje osvješćuju potrebu za prodajom polica cyber osiguranja, no u puno zemalja to nije doseglo zadovoljavajuće razine. Police cyber osiguranja, već rečeno, nisu standardizirane već ovise o potrebama kupaca, no postoje neki standardni obrasci koje svako osiguranje može pratiti i omogućiti kupcima barem djelomično osiguranje od cyber rizika.

U nastavku teksta navode se primjeri ponuda osiguranja odabranih društava za osiguranje iz svijeta, dostupnih na internetskim stranicama.

Allianz Global Corporate & Specialty (AGCS) ima dugogodišnje iskustvo u cyber osiguranju, zaštiti organizacija od cyber kriminala i digitalnih prijetnji. Vrste rizika koje AGCS pokriva su gubitci prve strane i gubitci treće strane:

- odgovornost za povredu osobnih i korporativnih podataka,
- troškovi povrede podataka,
- odgovornost za sigurnost mreže za hakirane ili ugrožene sustave, uključujući napade uskraćivanjem usluge,
- medijska odgovornost za digitalne publikacije,
- prekid poslovanja uzrokovan cyber incidentom,
- troškovi obnove podataka i programa koji su rezultat cyber incidenta,
- IT podrška za komunikaciju u kriznim situacijama za ublažavanje štete po ugledu,
- krizno komuniciranje za ublažavanje reputacijske štete.

Također, ACGS klijentima nudi i usluge prevencije i pomoći u poboljšanju cyber otpornosti te ublažavanju negativnih učinaka nakon incidenata. Pristup IT forenzičkim stručnjacima ili pravnoj ili kriznoj komunikacijskoj podršci klijentima je omogućen 24/7. (AGCS, 2022.)

Berkshire Hathaway pruža mogućnost uzimanja sveobuhvatne police osiguranja koja služi za zaštitu cjelokupnog poslovanja manjih poduzeća, a ne samo dijela poslovanja (THREE by Berkshire Hathaway). Takva jedinstvena polica kombinira pokrića kritična za poslovanje, a cyber osiguranje u nju je uključeno. Cyber osiguranje u takvoj polici pokriva sljedeće rizike:

- povreda podataka,
- ransomware (štetan softver koji korisniku uskraćuje pristup računalnim resursima i traži plaćanje otkupnine za uklanjanje ograničenja),
- cyber odgovornost,
- phishing (krađa podataka putem e-maila),
- računalna prevara. (THREE, 2022.)

AIA Insurance Agency naglašava da agenti u osiguranju rade police cyber osiguranja isključivo prema potrebama klijenata, a ne standardizirane, no većina polica uključuje sljedeća pokrića:

- upravljanje krizom povrede podataka/privatnosti,
- pokriće medijske odgovornosti,
- pokriće štete treće strane,
- pokriće odgovornosti za iznudu,
- odgovornost za sigurnost mreže.

Kao ono najvažnije, naglašavaju da polica cyber osiguranja štiti poduzeće od odgovornosti u slučaju povrede podataka u kojoj su osobni podaci klijenata ukradeni ili izloženi. (AIA Insurance Agency, 2022.)

AXA XL provodi modularnu politiku cyber zaštite i zaštite podataka koja je osmišljena da bude prilagođena potrebama određenog industrijskog sektora – za odgovornost prema trećim stranama i za gubitke prve strane. Pokrivenost je opsežna i fleksibilna te se može isporučiti niz usluga koje mogu spriječiti cyber napade ili odgovoriti na njih brzo i učinkovito ako se napad dogodi. Polica osiguranja svakako pokriva:

- prekid poslovanja i trošak,
- gubitak/uništenje elektroničke imovine,
- odgovore na incidente,

- regulatorne troškove zaštite privatnosti i pokriće regulatornih kazni te kazne (gdje je to moguće osigurati zakonom) koje proizlaze iz nezakonite radnje u vezi s privatnošću ili sigurnošću,
- obnavljanje podataka,
- cyber iznudu.

Kao dio cyber pokrivenosti, omogućen je pristup specijaliziranim timovima dostupnima 24/7 koji su spremni pomoći pri cyber incidentu. (AXA XL, 2022.)

Munich Re je vodeći svjetski reosiguratelj cyber rizika. Nudi cyber pokrića za poduzeća sa značajnim ograničenjima. Police osiguranja su modularne i kreću se od tradicionalnih pokrića povrede sigurnosti podataka i pokrića troškova za plaćanje otkupnine u cyber iznudi, do pokrića prekida poslovanja zbog fizičke cyber štete ili nekog operativnog poremećaja. Ovisno o individualnim profilima rizika, Munich Re integrira inovativne koncepte cyber osiguranja kao što su pokriće za štetu po ugledu, zaštita od osobne i materijalne štete te kazne ili jamstvena plaćanja, ako ih prouzrokuje cyber napad.

Proizvodi i usluge u polici cyber osiguranja:

- pokriće za prekid poslovanja, uključujući troškove forenzike,
- pokrivenost cyber kriminala i cyber iznude,
- narušavanje ugleda i izvještavanje medija,
- pokriće štete na digitalnoj imovini i troškovi zamjene hardvera,
- pokriće odgovornosti za tehnologiju, mrežnu sigurnost i privatnost,
- regulatorna pokrivenost,
- bliska suradnja s pružateljima usluga prije i nakon incidenta,
- upravljanje cyber incidentima,
- prilagođeni proizvodi i usluge cyber osiguranja. (Munich Re, 2022.)

Društvo za osiguranje Zurich smatra da je za poduzeća veće pitanje kada će se dogoditi ozbiljan cyber napad, a ne hoće li se dogoditi. Polica cyber osiguranja nudi pokrića prve i treće strane.

Pokrića:

- troškovi kršenja podataka,
- gubitak poslovnih prihoda i dodatni troškovi incidenta,
- trošak zamjene digitalnih sredstava,
- cyber prijetnje iznudom,

- kvar sustava,
- cyber prevare,
- hitni troškovi nastali zbog incidenta,
- odgovornost za sigurnost i privatnost,
- troškovi obrane u regulatornom postupku,
- građanske kazne i kazne povezane s platnim karticama. (Zurich, 2022.)

Generali grupa surađuje s klijentima diljem svijeta i nudi širok spektar osiguranja od cyber rizika, prilagođavajući proizvode kako bi odgovarali specifičnim potrebama i situacijama klijenata. Dizajniraju se rješenja koja izravno rješavaju probleme poput krađe podataka i oporavaka sustava te prekida poslovanja. Stručnjaci rade izravno s poduzećima te prilagođavaju cyber proizvode i usluge specifičnim potrebama. Cyber zaštita nudi niz komplementarnih usluga uključujući:

- sprječavanje gubitaka – pružanje preventivne zaštite, jačanje cyber obrane prije nego dođe do napada i omogućavanje poduzeću da u potpunosti izbjegne štetu;
- smanjenje gubitaka – financijska potpora u slučaju da je poduzeće oštećeno napadom;
- usluge nakon incidenta – niz usluga pomoći za poduzeće, što je brže moguće nakon napada, uključujući zaštitu od dodatnih napada i vraćanje ugleda što je brže moguće. (Generali, 2022.)

Cyber Lev Insurance je društvo za osiguranje koje također nudi individualizirane i prilagođene police osiguranja, a pokrića koja uključuje cyber polica za velike korporacije su pokrića prema prvoj i prema trećoj strani.

- Pokrića prema prvoj strani:
    - oštećenje digitalne imovine,
    - prekid poslovanja zbog cyber napada,
    - cyber ucjena i ograničenje pristupa,
    - odgovor na incident,
    - cyber terorizam,
    - pokriće za narušavanje osobnog ugleda.
- Pokrića prema trećoj strani:
    - privatna odgovornost,
    - odgovornost za internetske medije,
    - troškovi povezani sa standardima sigurnosti,

- obrana i sankcije od strane regulatornih tijela. (Cyberlev, 2022.)

4.3. Analiza uloge i značaja društava za osiguranje u upravljanju cyber rizicima

Pregled tržišta cyber kriminala i rizika, prema Marshu (2015.):

- procijenjeni godišnji trošak cyber kriminala na globalnu ekonomiju iznosio je 445 milijardi dolara;
- očekivana veličina globalnog tržišta cyber sigurnosti iznosila je 120 milijardi dolara;
- broj ljudi u SAD-u kojima su hakeri ukrali osobne podatke u samo 2014. godini jest 40 milijuna;
- procijenjena veličina globalnog tržišta cyber osiguranja iznosila je 2 milijuna;
- godišnja stopa rasta tržišta cyber osiguranja iznosila je 50-100%.

Cyber osiguranja omogućavaju zaštitu od velikog cyber rizika, ali koji se može odrediti, industrije poput financijskih institucija koriste cyber osiguranje kako bi ispunile regulatorne zahtjeve, a osiguranje je korisno i za zaštitu od lako vrijednih gubitaka kao što su regulatorne kazne i kršenje privatnosti podataka. (Chabrow, 2012.)

Industrija osiguranja, prema Insurance Europe (2019.), ima ključnu ulogu i značaj u pomaganju Europskoj uniji u naporima da se poveća cyber otpornost i konkurentnost. Osiguratelji mogu osigurati kontinuitet poslovanja pomažući poduzećima da se brže oporave od cyber napada, mogu povećati svijest pojedincima i poduzećima o cyber rizicima kojima su izloženi i ponuditi učinkovitu zaštitu od njih. Također, mogu savjetovati europske i nacionalne kreatore politike o cyber rizicima i kako mogu bolje upravljati njima i ublažiti ih. Osiguranje djeluje kao mehanizam transfera rizika i osigurava poduzećima gubitke koji se ne mogu u potpunosti spriječiti. U slučaju cyber rizika, industrija osiguranja osiguranicima nudi i savjetovanja, pomoć pri sprečavanju cyber napada, a na kraju i ublažavanje posljedica ako se cyber incident dogodi. Osiguranja pokrivaju razne posljedice cyber rizika, kao što su phishing, zlonamjerni softveri, kršenje podataka. Pružaju pokriće za prvu stranu, za štetu na digitalnu imovinu, troškove prekida poslovanja i slično već navedeno u tekstu. S druge strane, cyber osiguranja pružaju i pokriće treće strane, u smislu odgovornosti vezane za privatnost i povjerljivost. Neke police osiguranja nude osiguranicima usluge procjene potencijalne izloženosti te tehničku i pravnu pomoć, kao i pomoć u odnosima s javnošću prilikom incidenta. Cjelokupna ponuda pomaže poboljšati cyber otpornost osiguranicima i pomaže u ublažavanju posljedica u slučaju incidenta.

Pokrića se razlikuju ovisno o potrebama kupaca, o izloženosti rizicima i vrsti cyber rizika kojima su izloženi, razini digitalizacije i veličini i vrsti usluga koje osiguranici pružaju.

Osiguratelji i reosiguratelji aktivno uče o cyber rizicima pa time i proces osiguranja postaje bolji. Kako tržište sazrijeva, kapital tržišta može pomoći i u proširenju kapaciteta za cyber reosiguranje. S druge strane, treba naglasiti da oslanjanje isključivo na osiguranje i mogućnost reosiguranja može dovesti do negativnih posljedica, na primjer stvaranje moralnog hazarda, smanjenja poticaja za aktivno upravljanje rizikom i napadom. Dakle, kao što je već navedeno, cyber osiguranje je pozitivan, koristan i važan faktor u procesu upravljanja cyber rizicima, no ostali načini upravljanja ne smiju ostati zanemareni, jer samo tako upravljanje cyber rizicima može biti uspješno. U slučaju cyber ratovanja i terorizma, pogotovo onim koje sponzorira vlada, potrebna je javna pomoć i rješenje, pa u takvom slučaju često vlada preuzima odgovornost reosiguratelja u krajnjoj nuždi. (CRO Forum, 2014.)

Na tržištu cyber osiguranja vjerojatno nema osiguratelja koji nudi isti broj i vrstu pokrića u svojoj ponudi. Zato prilikom uzimanja osiguranja, treba dobro procijeniti što i kako se želi osigurati i prema tome izabrati osiguratelja koji nude te usluge.

Tablica 2: Vrste pokrića osiguranja koje su najčešće na tržištu

Vrsta pokrića	*% proizvoda koji sadrže ovo pokriće (26 uzoraka)*
Kršenje privatnosti	92%
Gubitak podataka i softvera	81%
Troškovi odgovora na incident	81%
Cyber iznuda	73%
Prekid poslovanja	69%
Multimedijska odgovornost	65%
Regulatorni i obrambeni troškovi	62%
Narušavanje ugleda	46%
Odgovornost za mrežne pogreške	42%
Prekid poslovanja zbog vanjskih uzroka	33%
Odgovornost za tehnološke greške i propuste	27%
Odgovornost za greške i propuste u profesionalnim uslugama	23%
Financijska krađa i prevara	23%

Krađa intelektualnog vlasništva	23%
Oštećenje fizičke imovine	19%
Smrt i tjelesne ozljede	15%
Cyber terorizam	12%
Odgovornost za direktore i službenike	13%
Odgovornost za proizvod i poslovanje	8%
Oštećenje okoliša	4%

Izvor: Izrada autora prema Cambridge Centre for Risk Studies (2016.)

Modeliranje fizičkih rizika je, već objašnjeno, dobro uspostavljeno s obzirom da postoje povijesni podaci na temelju kojih se mogu vršiti procjene za budućnost. Za cyber rizik, ne postoje povijesni podaci pa se za procjenu takvih rizika osiguratelji moraju oslanjati na stručnjake koji donose pretpostavke o mogućim cyber incidentima i njihovom obujmu. S obzirom na takve poteškoće, poduzeća ne mogu kvalitetno kvantificirati svoj rizik pa je alternativni pristup koncentrirati se na ukupni izloženost i kapacitet. U 2014. godini, ukupna globalna izloženost industrije osiguranja cyber rizika (kvantificiran ukupnim prodanim ograničenjem samostalne kibernetičke odštete) iznosila je oko 100 milijardi funti.

Tablica 3: Usporedba izloženosti cyber osiguranja prema globalnom osiguranju

Ukupna vrijednost izloženosti industrije osiguranja cyber rizika	100 milijardi funti
Maksimalni globalni kapacitet (re)osiguranja za bilo koji događaj prirodne katastrofe	65 milijardi funti
Maksimalni globalni kapacitet (re)osiguranja za nuklearnu energiju, za gubitak prve strane	3 milijarde funti
Raspon mogućeg maksimalnog gubitka za portfelje nekretnina	0,15% – 20%
Raspon mogućeg maksimalnog gubitka za cyber incidente	150 milijuna funti – 20 milijardi funti

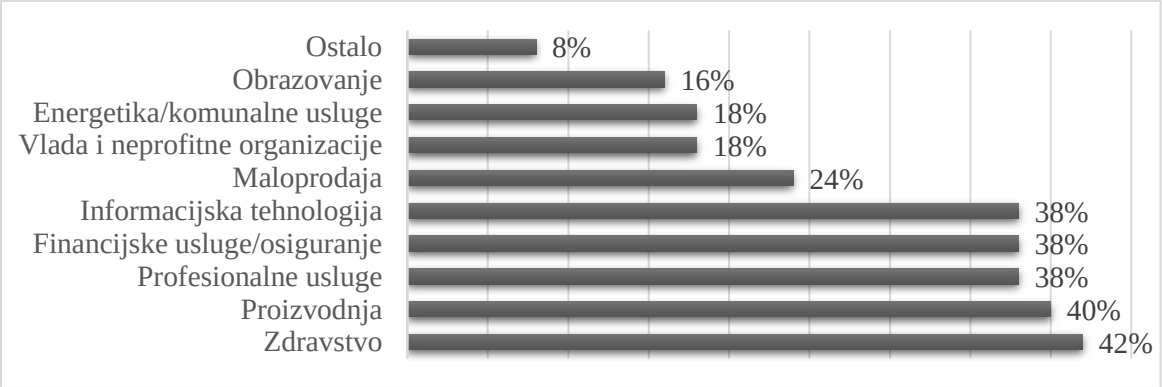
Izvor: Izrada autora prema podacima Marsha (2015.)

Ako se uzme u obzir da bi se cyber tržište osiguranja od 2014. na dalje moglo utrostručiti u narednih 3 do 5 godina, maksimalni mogući gubitak za cyber rizike mogao bi premašiti globalni maksimalni kapacitet osiguranja za, na primjer, nuklearnu ili prirodnu katastrofu. Navedeno

dovodi do zaključka da osiguratelji uspješno upravljaju cyber rizicima te da se osiguranje razvija još od prošlog desetljeća. (Marsh, 2015.)

Podaci iz grafikona 12, 13 i 14 izvučeni su iz ankete, PartnerRe i Advisen (2018.), trendovi na tržištu cyber osiguranja. Ispitano je 270 brokera i 70 osiguratelja iz cijelog svijeta, većinom iz Sjeverne Amerike. Važno je napomenuti da je 2018. godina kompetitivnija od 2017., što je potvrđeno od 90% ispitanika.

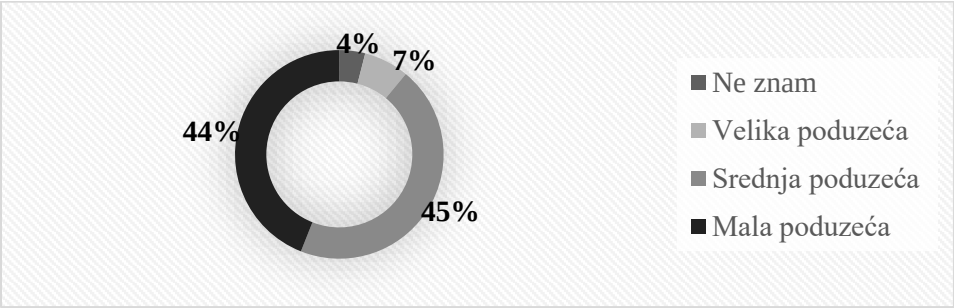
Grafikon 12: Koje industrije (top 3) donose najviše novih kupaca cyber osiguranja?



Izvor: PartnerRe i Advisen (2018.)

Prema ispitanicima, zdravstvo donosi najviše novih kupaca cyber osiguranja, no i industrije proizvodnje, financijskih i profesionalnih usluga, osiguranja i informacijske tehnologije ne zaostaju puno. Proizvodnja je s petog mjesta prethodne godine dospjela na drugo mjesto. Neki ispitanici naglasili su da se povećala potražnja iz građevinskog sektora i hotelijerstva. (PartnerRe i Advisen, 2018.)

Grafikon 13: Novi kupci cyber osiguranja



Izvor: PartnerRe i Advisen (2018.)

Većina novih kupaca osiguranja su srednja poduzeća, čiji godišnji prihodi variraju između 50 milijuna i 1 milijarde dolara, i mala poduzeća čiji su prihodi manji od 50 milijuna dolara. To se

može objasniti jer velike korporacije i poduzeća već imaju cyber osiguranja u svojem portfelju i cyber rizici su im visoko pozicionirani u registru rizika. Ovo je pozitivan trend s obzirom da ukazuje na suočavanje i bolje razumijevanje cyber rizika od strane malih i srednjih poduzeća. (PartnerRe i Advisen, 2018.)

Grafikon 14: Koje su najveće prepreke (top 3) za prodaju police osiguranja?

Izvor: PartnerRe i Advisen (2018.)

Na grafikonu 14 navedene su najveće prepreke za prodaju police cyber osiguranja. Bez obzira na napredak postignut na tržištu cyber osiguranja, ostaju prepreke koje stoje na putu prema kupnji osiguranja. Primarna prepreka je nedostatak razumijevanja o izloženosti, a druga najveća prepreka nedostatak razumijevanja za pokrivenost.

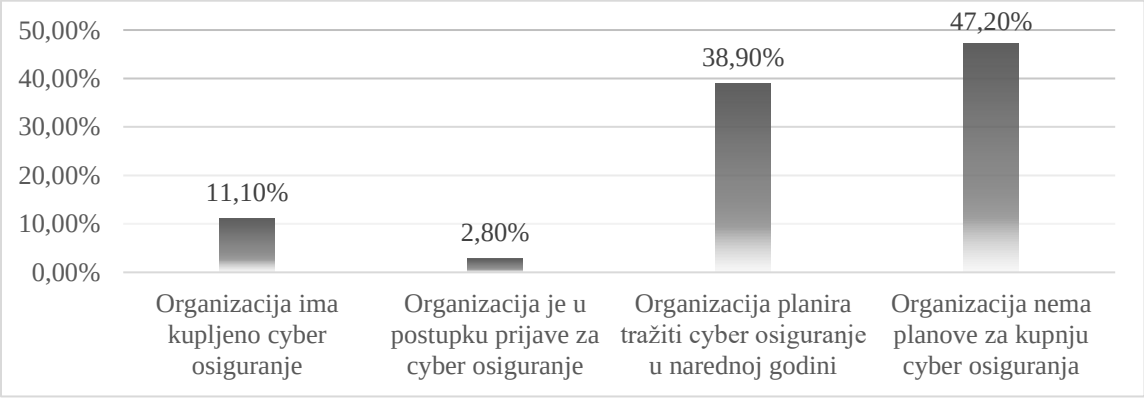
Amerika je puno naprednija u otpornosti prema cyber rizicima i u cyber osiguranju od Europe. Kako god, unatoč svim navedenim preprekama, industrija cyber osiguranja mogla bi imati ključnu ulogu u pružanju pomoći Europskoj uniji u naporima da poveća cyber otpornost i konkurentnost. Osiguratelji bi jamčili nastavak poslovanja pomažući poduzećima da se brže oporave od napada, povećali svijest građana o opasnosti od cyber rizika i pružili im djelotvornu zaštitu te savjetovali europske i nacionalne politike o tome kako se cyber rizici mogu ublažiti ali i bolje upravljati njima. Već je više puta navedeno da standardizacija polica osiguranja ne bi bila produktivna u cyber osiguranju. Također, niti uvođenje obveznog cyber osiguranja ne bi pomoglo u razvoju tog tržišta i većoj otpornosti ili konkurentnosti. Glavni razlozi za to su činjenice da se tržište osiguranja neprekidno razvija, pa bi standardizirane police ubrzo postajale zastarjele. Isto tako, negativno bi djelovalo na osiguranike i osiguratelje jer bi osiguranici morali kupovati police koje nisu točno prilagođene za njihove rizike i potrebe, već bi plaćali nešto što im ni ne treba, a osiguratelji ne bi mogli točno napraviti policu koja odgovara njihovim klijentima. Najveći problem cyber osiguranja je svakako nedostatak podataka koji su

potrebni osiguratelji ma da mogu kreirati cijenu police, no s vremenom je sve više stručnjaka koji procjenjuju rizike i izloženost poduzeća, pa se tržište povećava. (Gajski Kovačić, 2020.)

Allianz Global Corporate & Specialty ima zabilježen porast potreba za cyber osiguranjem u zadnjim godinama. Žele pružiti pomoć svojim klijentima u boljem razumijevanju i većoj otpornosti na cyber rizike, ali važno je reći da velik dio zaštite od cyber rizika leži u dobroj IT infrastrukturi, zaštiti osobnih podataka, suzdržavanja od dijeljenja informacija na internetu, uporabe antivirusnih softvera i njihovom redovnom ažuriranju, korištenju lozinki značajne zaštite (velika i mala slova, brojke, znakovi). Nakon toga, dolaze police osiguranja koje omogućuju još puno veću zaštitu. Do 2020. godine procijenjeno je da će biti 50 milijardi uređaja koji će razmjenjivati informacije. Zbog ogromnog porasta uređaja spojenih na internet i sve većeg korištenja digitalizacije i razvoja tehnologije, rast će i cyber napadi pa i potreba za cyber osiguranjem. Premije za cyber osiguranje će globalno rasti od tadašnjih 2 milijarde dolara, u 2017. godini, na 20 milijardi dolara, kroz narednih 10 godina, s porastom od 20%. Također, povećano korištenje interneta dovest će i pojedince u rizik od cyber napada, za koje društva za osiguranje još nemaju adekvatnu ponudu osiguranja. Očekuje se da će taj segment tržišta osiguranja također značajno porasti. Osiguranje od cyber rizika je u posljednjih 20 godina diljem svijeta poraslo s od oko 10 osiguratelja do otprilike 50 osiguratelja koji nude police za cyber rizike. Prema Moody's-u 2017. godine su bruto prodane premije iznosile oko 2,75 milijardi dolara, a 2016. oko 2 milijarde. Pwc je procjenjivao da će se do 2020. premija cyber osiguranja povećati na 7,5 milijardi dolara. (Protrka, Marić, Plećaš, 2017.)

Prema anketi Marsha (2015.) u Ujedinjenom Kraljevstvu, otkriveno je da je više od polovice (52,8%) ispitanih poduzeća na neki način angažirano na tržištu osiguranja.

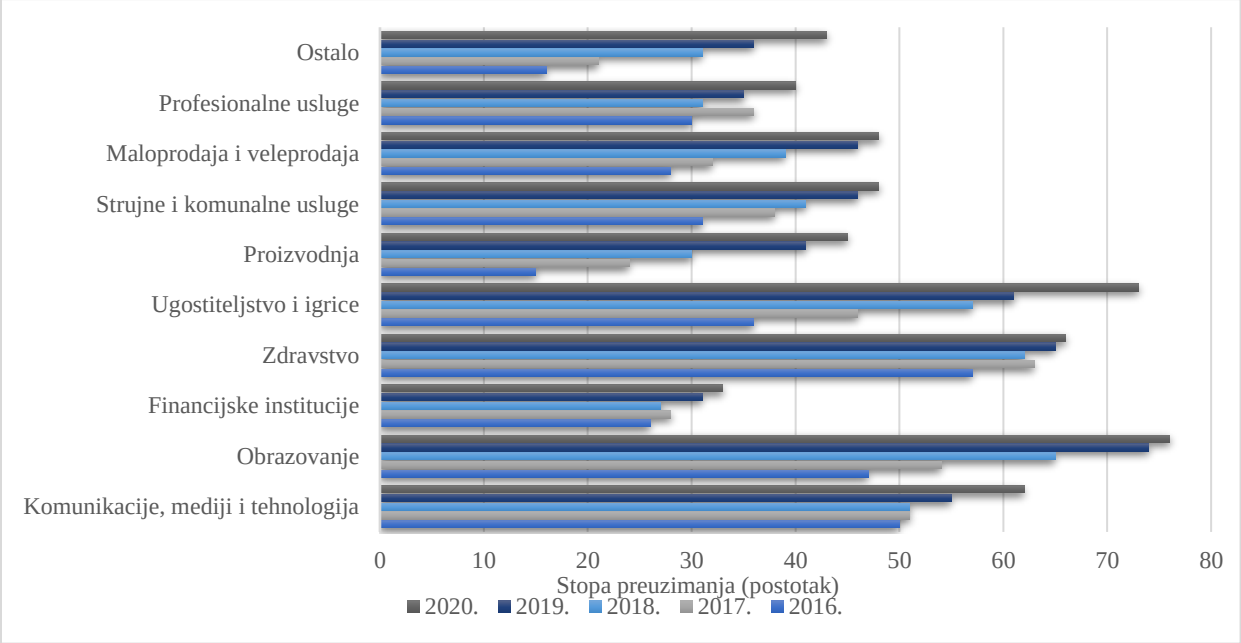
Grafikon 15: Trenutni status organizacije u pogledu cyber osiguranja



Izvor: Marsh (2015.)

Na grafikonu 15 prikazano je da je 52,80% ispitanika na neki način angažirano na tržištu osiguranja – no samo 11,10% ima kupljeno cyber osiguranje. Ostatak poduzeća planira tražiti cyber osiguranje, a 2,80% je već u procesu prijave za cyber osiguranje. 47,20% ispitanika nema planove za kupnju cyber osiguranja što znači da nije angažirano na tom tržištu.

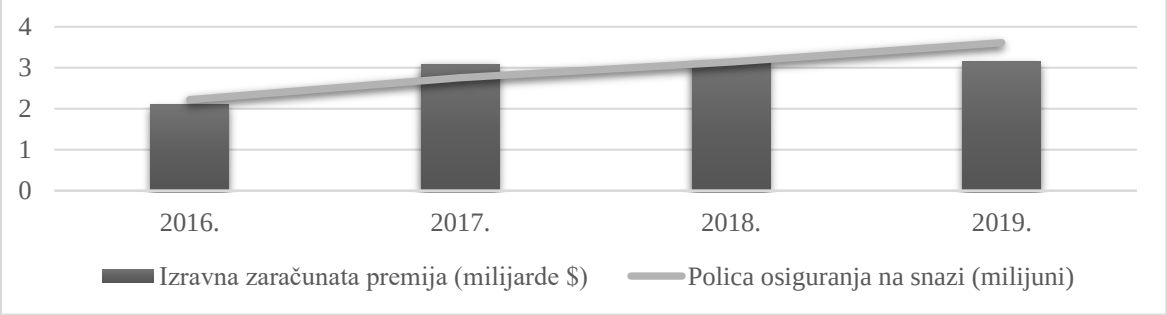
Grafikon 16: Stopa preuzimanja cyber osiguranja po djelatnostima, 2016. – 2020.



Izvor: GAO (2021.)

Grafikon 16 pokazuje da se stope preuzimanja cyber osiguranja razlikuju ovisno o industrijama. Industrijski sektori s najvećim stopama preuzimanja u razdoblju od 2016. do 2020. godine uključivali su obrazovanje i zdravstvo – industrije koje koriste velike količine osobnih podataka i zaštićenih informacija. Ugostiteljstvo i maloprodaja su sektori koji se koriste podacima s platnih kartica pa u novije vrijeme sve više koriste cyber osiguranja.

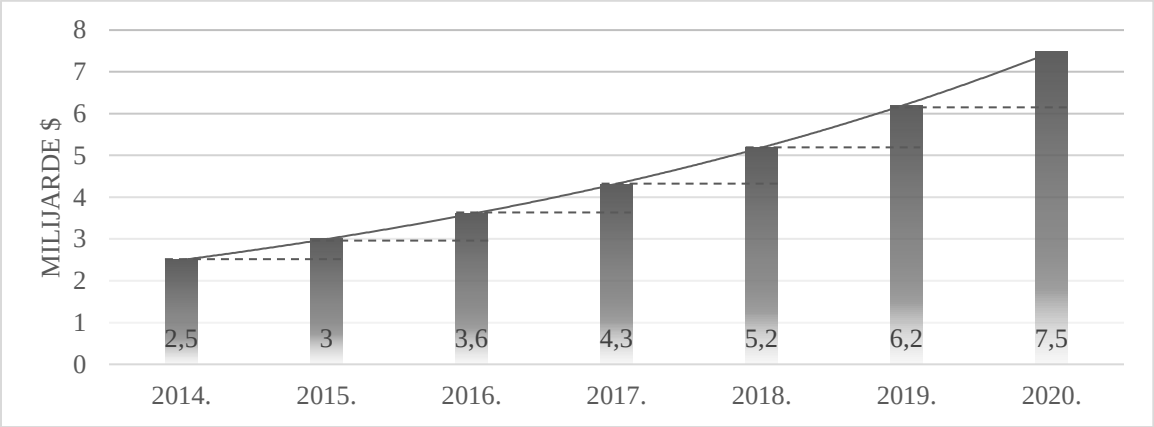
Grafikon 17: Izravne zaračunate premije i police na snazi za cyber osiguranje, 2016. – 2019.



Izvor: GAO (2021.)

Potražnja za cyber osiguranjem kroz godine raste što pokazuje da subjekti bolje razumiju i odgovaraju na sve veće cyber rizike. Na grafikonu 17 vidljivo je povećanje polica osiguranja na snazi od 2016. do 2019. godine – broj važećih polica povećao se s oko 2,2 milijuna na više od 3,6 milijuna polica u tom razdoblju, što je povećanje od oko 60%. S druge strane, iznos zaračunatih premija porastao je za oko 50% tijekom navedenog razdoblja, s 2,1 milijardi dolara, na 3,1 milijardi dolara.

Grafikon 18: Procijenjena vrijednost premija cyber osiguranja zaračunatih na globalnoj razini od 2014. do 2020.



Izvor: Yeo, Ende (2019.)

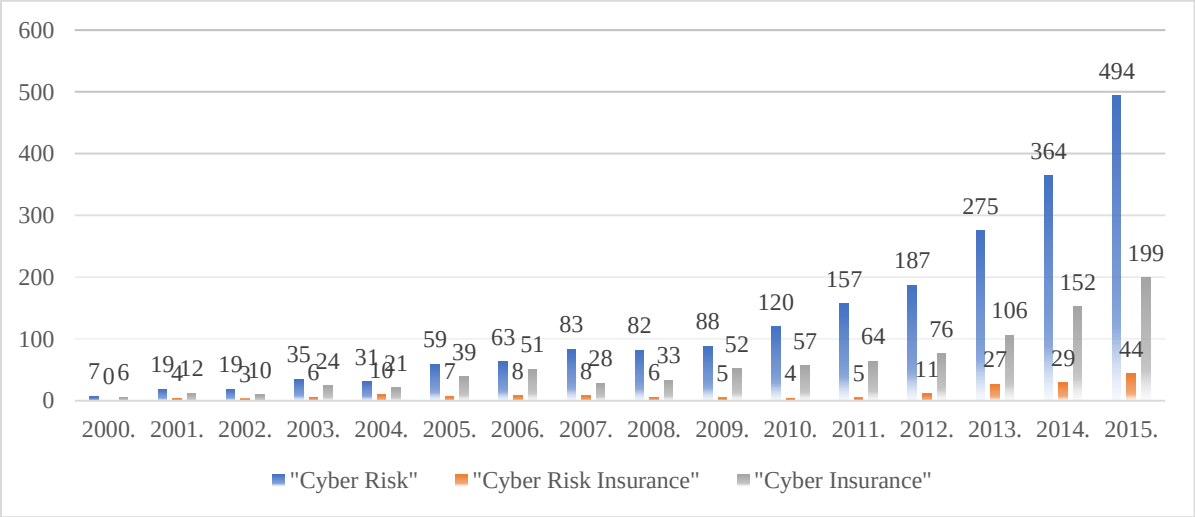
Zaračunate premije od 2014. rastu godišnje za otprilike 20%. Od početnih 2,5 milijardi dolara u 2014. godini, u 2020. su zaračunate premije narasle na 7,5 milijardi dolara. (Yeo, Ende, 2019.)

Bez obzira na sve navedene prednosti cyber osiguranja, ono nije jedino rješenje za upravljanje cyber rizikom. Osiguranje ne može zamijeniti aktivno upravljanje cyber rizicima u poduzećima. No, kako društva za osiguranje stječu sve više iskustva zbog većeg broja polica osiguranja za cyber rizike, a tržište sazrijeva, tako će i određivanje cijena polica i alokacija rizika u financijskim sustavima postati učinkovitija, tržišta potpunija, a osiguranje će efikasnije prenositi i udruživati rizike i tako povećati svoju ulogu u upravljanju cyber rizicima. (Kopp, Kaffenberger, Wilson, 2017.)

U 2017. godini premije osiguranja iznosile su 2,5 milijarde dolara, a do 2025. očekuje se da će one narasti do 20 milijardi dolara ili više. Ključno za takav rast su bolji podaci i analitika. Rast će i podrška reosiguranju, kao odgovor na bolje podatke i alate, podržavajući ukupan rast tržišta. Poduzeća koja žele sklopiti ugovor o osiguranju moći će pristupiti višim limitima jer će društva za osiguranje prenijeti dio rizika na reosiguratelje. Vanjski stručnjaci trebaju biti uključeni u

suradnju s osiguranicima i osigurateljima, sudjelovati u prevenciji gubitaka i pomoći pri kršenjima. Osiguratelji u suradnji s poduzećima za cyber sigurnost mogu stvarati stres testove i simulirane situacije za svoje klijente, kako bi se ocijenio odgovor na incidente. Takve simulacije pomažu menadžmentu da bolje razumiju potencijalne cyber incidente i donose bolje odluke, a također mogu biti korisni za osoblje jer će simulirani, na primjer, phishing napad pojedince učiniti budnijima u budućnosti. U budućnosti, očekuje se da će društva za osiguranje moći prilagoditi pokrića koja pružaju na temelju promjenjivog profila rizika svojih klijenata. Time društva za osiguranje dodatno povećavaju svoju ulogu i pozitivan učinak na upravljanje cyber rizicima. (Camillo, 2017.)

Grafikon 19: Sve veća relevantnost cyber rizika i cyber osiguranja u posljednja 2 desetljeća



Izvor: Eling, Schnell, Sommerrock (2016.)

Na grafikonu 19, prema Eling, Schnell, Sommerrock (2016.), pokazana je sve veća relevantnost cyber rizika i osiguranja od cyber rizika – prikazani su podaci s Google Scholara o radovima koji sadrže riječi „cyber risk“ ili „cyber insurance“ od 28. veljače 2016. Radovi koji su pretraženi na Google Scholaru ne moraju nužno raspravljati o toj temi kao glavnoj temi, ali ju mogu spomenuti kao sporednu.

Cyber rizici će se nastaviti razvijati i povećavati te ostati u svijetu rizika. Zbog toga se poslovni subjekti i pojedinci moraju pripremiti, preventivnim mjerama i svakim mogućim ublažavanjem gdje je to izvedivo, kako se ne bi susretali s velikim gubicima. Dobro razumijevanje između osiguratelja, osiguranika, posrednika, obrazovanje i edukacija pojedinaca i poslovnih subjekata bit će ključni za tržište cyber osiguranja, njegov rast i razvoj te dostizanje punog potencijala za opsluživanje svih sudionika. (Ferma, Insurance Europe, Bipar, Aon, Marsh, 2018.)

5. ZAKLJUČAK

U ovom diplomskom radu istražena je uloga društava za osiguranje u upravljanju cyber rizicima. Društva za osiguranje postoje od samih začetaka financijskih tržišta i važan su segment poslovnim subjektima u upravljanju tradicionalnim rizicima. Police osiguranja često su standardizirane i vrlo lako se prodaju. U slučaju cyber rizika, to je nešto drugačije. Cyber rizici su relativno noviji rizici s obzirom na tradicionalne rizike s kojima se poslovni subjekti susreću. Razvojem i napretkom tehnologije, nastaju i povećava se obujam cyber rizika koji prijete poslovnim subjektima, ali i pojedincima. Mobiteli, Internet, mrežna komunikacija, dijeljenje medija, društvene mreže, sve su to idealni faktori za sve veći razvoj cyber prijetnji i rizika.

Poslovni subjekti moraju, kako i ostalim rizicima, tako i cyber rizicima, upravljati. Pod upravljanje rizikom spadaju izbjegavanje rizika, smanjivanje rizika, smanjivanje izloženosti i prijenos rizika. U slučaju cyber osiguranja, nemoguće je izbjegavati rizik, jer bi to značilo neupotrebljavanje informacijske tehnologije, što bi dovelo do propasti poslovnog subjekta prije nego cyber incident. Poduzeća moraju koristiti tehnologiju da bi bila konkurentna na tržištu, mogla se razvijati i općenito poboljšati svoje poslovanje.

Transfer rizika na društva za osiguranje jedna je od najvažnijih strategija u upravljanju takvim rizicima. Veća ponuda polica osiguranja za cyber rizike povećava svijest o važnosti cyber prijetnji i povećava zaštitu poslovnih subjekata. Ipak, postoje brojne prepreke cyber osiguranju. Najveći problem je nedostatak aktuarskih podataka – povijesnih podataka o riziku, izloženosti, incidentima i slično, na temelju kojih se mogu raditi analize i procjene te na temelju čega se onda sastavi polica osiguranja. Zbog nedostatka podataka, osiguratelji moraju imati pomoć stručnjaka pri procjeni i prognoziranju eventualnih budućih incidenata i na temelju toga sastavljati cijene polica. Zbog toga, cijene polica su često visoke i nedostupne za velik broj subjekata ili pojedinaca.

Da bi se povećao obujam osiguranja cyber rizika, neka od rješenja su stvaranje pool-ova osiguratelja, gdje bi mogli podijeliti rizike i troškove incidenata, reosiguranje cyber osiguranja, edukacija i obrazovanje o važnosti, poticaji vlade, kod velikih rizika koji uzrokuju katastrofalne posljedice i vlada bi trebala biti reosiguratelj, kao zadnje utočište.

Tržište cyber osiguranja razvija se iz dana u dan. U posljednja dva desetljeća doživjelo je ogroman porast. SAD prednjači u razvijenosti osiguranja naspram EU i ostatka svijeta, ali

očekuje se jak razvitak tržišta u Europi također. Za poslovne subjekte tržište je donekle razvijeno, ali za pojedince puno slabije. I za to se očekuje veći razvoj u narednom vremenu zbog sve većeg broja incidenata i hakiranja, i svijesti pojedinaca o cyber prijetnjama. Cyber rizici najviše prijete velikim sustavima kao što su zdravstvo, financijski sustav, proizvodnja i slično.

Cjelokupni proces upravljanja cyber rizicima trebao bi se bazirati na samozaštiti, na educiranju zaposlenika, pažnji, instaliranju najnovijih antivirusnih aplikacija, softvera i ostalih zaštitnih mjera. Uz to, cyber osiguranje igra glavnu ulogu za sprečavanje velikih gubitaka i za nastavak poslovanja u slučaju cyber incidenata. Osiguratelji također mogu pomoći poslovnim subjektima u zaštiti od cyber rizika, preporučivanjem najboljih mogućnosti obrane od cyber prijetnji i zaštite.

U radu je vidljivo da se važnost društava za osiguranje u upravljanju cyber rizicima iz godine u godinu povećava, da se sve više koriste police takvog osiguranja i da se povećava ponuda i potražnja. Pojedinci i poslovni subjekti postaju sve svjesniji da su cyber rizici u vrhu svjetskih rizika i da mora postojati efikasna linija obrane. Cyber osiguranje bi kroz vrijeme trebalo postati sastavni dio poslovanja. Uz osiguranje i mjere samozaštite, poslovni subjekti u mogućnosti su efikasno se nositi sa cyber prijetnjama i iskoristiti sve prednosti tehnologije i suvremenog doba.

LITERATURA

1. Adelmann, F., Elliot, J., Ergen, I., Gaidosch, T., Jenkinson, N., Khiaonarong, T., …, Wilson, C. (2020.), Cyber Risk and Financial Stability: It's a Small World After All, *Staff Discussion Notes*, 2020(007), https://doi.org/10.5089/9781513512297.006
2. AGCS, (b.d.), *Cyber Insurance*, Pristupljeno: 28. 8. 2022. https://www.agcs.allianz.com/solutions/financial-lines-insurance/cyber-insurance.html#tabpar_8903_1Tab
3. AIA Insurance Agency, (b.d.), *Cyber Liability Insurance,* Pristupljeno: 28. 8. 2022. https://www.aiainsagency.com/commercial-insurance-coverages/liability-insurance/cyber-liability-insurance/
4. Andrijanić, I., Gregurek, M., Merkaš, Z. (2016.), *Upravljanje poslovnim rizicima,* Zagreb: Libertas – Plejada
5. AXA XL, (b.d.), *Cyber Insurance*, Pristupljeno: 25. 8. 2022. https://axaxl.com/insurance/products/cyber-insurance-international
6. Bara, D. (2015.), Uloga cyber-osiguranja u upravljanju i prijenosu rizika cyber-sigurnosti, u: Ćurković, M., Dobrić S., Horvat Martinović J., Krišto J., Šker T. (ur.), *Dani hrvatskog osiguranja 2015*. (127-138), Zagreb: Hrvatska gospodarska komora
7. Baranoff, E., (2004), *Risk Management and Insurance*, Danvers MA: John Wiley & Sons
8. Bijelić, M., (2002.), *Osiguranje i reosiguranje*, Zagreb: Tectus d.o.o.
9. Biener, C., Eling, M., Hendrik Wirfs, J. (2014.), *Insurability of Cyber Risk* [e-publikacija], preuzeto s: https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/ga2014-if14-biener_elingwirfs.pdf
10. Camillo, M. (2017.), Cyber risk and the changing role of insurance, *Journal of Cyber Policy*, 2(1), 53-63., https://doi.org/10.1080/23738871.2017.1296878
11. Cesarec, I. (2020.), Beyond Physical Threats: Cyber-attacks on Critical Infrastructure as a Challenge of Changing Security Environment – Overview of Cyber-security legislation and implementation in SEE Countries, *Annals of Disaster Risk Sciences : ADRS*, 3(1), 1-13., https://doi.org/10.51381/adrs.v3i1.45
12. Chabrow, E., (2012.), *10 Concerns When Buying Cyber Insurance,* Pristupljeno: 30. 5. 2022. https://www.bankinfosecurity.com/10-concerns-when-buying-cyber-insurance-a-4859/op-1

13. CroForum, Bank info security, (2014.), *Cyber resilience – The cyber risk challenge and the role of insurance*, [e-publikacija], preuzeto s: https://www.thecroforum.org/wp-content/uploads/2015/01/Cyber-Risk-Paper-version-24-1.pdf
14. CSIS, (b.d.), Significant Cyber Incidents, Pristupljeno: 30. 5. 2022. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
15. Cyberlev, (b.d.), *Koja pokrića uključuje cyber polica za velike korporacije?*, Prisupljeno: 28. 8. 2022. https://cyberlevins.com/hr/cyber-one-insurance-policy
16. Čerić, V., Varga, M. (2004.), *Informacijska tehnologija u poslovanju*, Zagreb: Element
17. Ćurak, M., Jakovčević, D. (2007.), *Osiguranje i rizici*, Zagreb: RRIF plus
18. Eling, M., Schnell, W., Sommerrock, F. (2016.), *Ten Key Questions on Cyber Risk and Cyber Risk Insurance*, [e-publikacija], preuzeto s: https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/cyber-risk-10_key_questions.pdf
19. ENISA, Robinson, N., RAND Europe, (2012)., *Incentives and barriers of the cyber insurance market in Europe*, [e-publikacija], preuzeto s: https://www.enisa.europa.eu/publications/incentives-and-barriers-of-the-cyber-insurance-market-in-europe
20. Ferma, Insurance Europe, Bipar, Aon, Marsh, (2018.), *Preparing for cyber insurance* [e-publikacija], preuzeto s: https://www.insuranceeurope.eu/publications/466/preparing-for-cyber-insurance/
21. Fortinet, (b.d.), Recent Cyber Attacks, Pristupljeno: 30. 5. 2022. https://www.fortinet.com/resources/cyberglossary/recent-cyber-attacks
22. Gajski Kovačić, N., Svijet osiguranja, (2020.), *Nedostatak podataka o kibernetičkim rizicima – glavna prepreka razvoju tržišta cyber osiguranja,* Pristupljeno: 30. 5. 2022. https://www.svijetosiguranja.eu/nedostatak-podataka-o-kibernetickim-rizicima-glavna-prepreka-razvoju-trzista-cyber-osiguranja-2/
23. Galinec, D., Možnik, D., Guberina B. (2017.), Cybersecurity and cyber defence: national level strategic approach, *Automatika*, 58(3), 273-286., https://doi.org/10.1080/00051144.2017.1407022
24. GAO, (2021.), *Cyber Insurance – Insurers and Policyholders Face Challenges in an Evolving Market*, [e-publikacija], preuzeto s: https://www.gao.gov/products/gao-21-477

25. Geer, D., Jardine, E., Leverett, E. (2020.), On market concentration and cybersecurity risk, *Journal of Cyber Policy*, 5(1), 9-29., https://doi.org/10.1080/23738871.2020.1728355
26. Generali, (b.d.), *Cyber Insurance solutions for you*, Pristupljeno: 25. 8. 2022. https://www.generaliglobalcorporate.com/solutions-for-you/cyber-insurance/cyber-insurance-solution-for-you.html
27. Harrington, S. E., Niehaus, G. R., (2003.), *Risk Management & Insurance*, New York: McGraw-Hill
28. Hiscox, (b.d.), *What is cyber insurance?*, Pristupljeno: 30. 5. 2022. https://www.hiscox.co.uk/business-insurance/cyber-and-data-insurance/faq/what-is-cyber-insurance
29. Hlača, S. (2018.), Kibernetička sigurnost u hrvatskim medijima, *Polemos : časopis za interdisciplinarna istraživanja rata i mira*, 21(42), 167-185., preuzeto s: https://hrcak.srce.hr/index.php?show=clanak&id_clanak_jezik=319596
30. Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, (2021.) Pristupljeno: 30. 5. 2022. http://www.enciklopedija.hr/Natuknica.aspx?ID=45672
31. Insurance Europe (2019.), *Insurers' role in EU cyber resilience* [e-publikacija], preuzeto s: https://www.insuranceeurope.eu/publications/2315/insurers-role-in-eu-cyber-resilience/
32. Klasić, K., Andrijanić, I. (2007.), *Osnove osiguranja načela i praksa*, Zagreb: Teb – poslovno savjetovanje d.o.o.
33. Klobučar, D. (2007.), *Risk management i osiguranje*, Zagreb: Tectus d.o.o.
34. Kopp, E., Kaffenberger, L., Wilson, C. (2017.), Cyber Risk, Market Failures, and Financial Stability, *IMF Working Papers*, 2017(185), https://doi.org/10.5089/9781484313787.001
35. Kovač, D. (2021.), Ulaganje u kibernetičku sigurnost, *Zbornik radova Veleučilišta u Šibeniku*, 15(1-2), 61-73., https://doi.org/10.51650/ezrvs.15.1-2.4
36. Marsh, (2015.), *UK 2015 Cyber Risk Survey Report*, [e-publikacija], preuzeto s: https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/UK%202015%20Cyber%20Risk%20Survey%20Report-06-2015.pdf
37. Marsh, McLennan, (2017.), *2017 Cyber Threats: A Perfect Storm to Hit Europe*, [e-publikacija], preuzeto s: https://fronteirasxxi.pt/wp-content/uploads/2018/06/MMC-FireEye-Cyber-Risk-Report.pdf

38. Marsh, (2015.), *Managing Cyber Risk*, [e-publikacija], preuzeto s: Cyber Risk Brochure.pdf
39. Marsh, (2015.), *The Role of Insurance in Managing and Mitigating the Risk*, [e-publikacija], preuzeto s: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf
40. Marsh, (2018.), *Managing cyber risk how prepared are you?*, [e-publikacija], preuzeto s: managing-cyber-risk.pdf
41. Miller, B. (2022.), *Here Are the Top 10 Countries Where DDoS Attacks Originate,* Pristupljeno: 29. 5. 2022. https://www.govtech.com/security/here-are-the-top-10-countries-where-ddos-attacks-originate
42. Moj bankar, (b.d.), *Ugovor o osiguranju*, Pristupljeno: 30. 5. 2022. https://www.moj-bankar.hr/Kazalo/U/Ugovor-o-osiguranju
43. Mraković, I., Vojinović R. (2019.), Maritime Cyber Security Analysis – How to Reduce Threats?, *Transactions on Maritime Science*, 8(1), 132-139., https://doi.org/10.7225/toms.v08.n01.013
44. Munich Re, (b.d.), *Navigating safely with Munich Re Cyber Insurance*, Pristupljeno: 28. 8. 2022. https://www.munichre.com/en/solutions/for-industry-clients/cyber-solutions-for-industry-clients.html
45. Müller, J. (2001.), Upravljanje informacijskom tehnologijom u suvremenim tvrtkama te hrvatska poslovna praksa korištenja informacijskih tehnologija, *Ekonomski pregled*, 52(5-6), 587-612., preuzeto s: https://hrcak.srce.hr/clanak/45067
46. Nationwide, (b.d.), *What is cyber insurance?*, Pristupljeno: 30. 5. 2022. https://www.nationwide.com/lc/resources/small-business/articles/what-is-cyber-insurance
47. OECD, (2017), *Enhancing the Role of Insurance in Cyber Risk Management*, Paris: OECD Publishing, https://doi.org/10.1787/9789264282148-en
48. PartnerRe & Advisen, (2018.), *2018 Survey of Cyber Insurance Market Trends*, [e-publikacija], preuzeto s: https://www.partnerre.com/wp-content/uploads/2018/10/2018-Survey-of-Cyber-Insurance-Market-Trends.pdf
49. Protrka, N., Marić K., Plećaš M. (2017.), Challenges and aspects of cyber security of the Republic of Croatia, *Acta Economica Et Turistica*, 3(1), 87-95., preuzeto s: https://hrcak.srce.hr/180778

50. Rafaj, J., HANFA, (2009.), *Tržište osiguranja*, [e-publikacija], preuzeto s: https://www.hanfa.hr/getfile.ashx/?fileId=39205
51. Ray, S. (2021.), *What Is a Risk Register & How to Create One*, Pristupljeno: 28.8.2022. https://www.projectmanager.com/blog/guide-using-risk-register
52. Refsdal, A., Solhaug, B., Stolen, K., (2015.), *Cyber-Risk Management*, https://ftp.technotic.ca/pub/media/Audiobooks/pack1/Cyber-Risk%20Management.pdf
53. Rejda, G. E., (2005.), *Principles of Risk Management and Insurance*, 9. izdanje, London: Pearson Education
54. Risk Management Solutions, Inc., Cambridge Centre for Risk Studies, (2016.), *Managing Cyber Insurance Accumulation Risk*, [e-publikacija], preuzeto s: https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-rms-managing-cyber-insurance-accumulation-risk.pdf
55. SoftActivity, (b.d.), *Mind-blowing Cybersecurity Statistics in 2022*, Pristupljeno: 29. 5. 2022. https://www.softactivity.com/ideas/cybersecurity-statistics/?gclid=EAIaIQobChMIgszJj_zD9wIVpo1oCR1W7QLYEAMYAiAAEgKPBvD_BwE
56. Solar, C. (2020.), Cybersecurity and cyber defence in the emerging democracies, *Journal of Cyber Policy*, 5(3), 392-412., https://doi.org/10.1080/23738871.2020.1820546
57. SPECOPS, (2020.), *The countries experiencing the most 'significant' cyber-attacks*, Pristupljeno: 30. 5. 2022. https://specopssoft.com/blog/countries-experiencing-significant-cyber-attacks/
58. Srića, V., Spremić, M., (2000.), *Informacijskom tehnologijom do poslovnog uspjeha*, Zagreb: Sinergija
59. Stajšić Golijanin, N., (2020.), *Osiguranje kao način upravljanja sajber rizicima*, Zbornik radova fakulteta tehničkih nauka, 35(10), https://doi.org/10.24867/09GI13Stajsic
60. THREE, (b.d.), *Looking for Cyber Insurance?*, Pristupljeno: 28. 8. 2022. https://threeinsurance.com/cyber-coverage/
61. Tintor, D., (2020.) *OT i IT kibernetička sigurnost*, završni rad, Fakultet elektrotehnike, računarstva i informacijskih tehnologija, Osijek
62. Trieschmann, J. S., Gustavson S. G., (1995.), *Risk Management & Insurance*, 9. izdanje, Cincinnati: South-Western College Publishing

63. Vaughan, E., Vaughan, T., (1995.), *Osnove osiguranja: upravljanje rizicima*, Zagreb: MATE d.o.o.
64. Vuković, H. (2012.), Kibernetska sigurnost i sustav borbe protiv kibernetskih prijetnji u Republici Hrvatskoj, *National Security and Future*, 13(3), 12-31., preuzeto s: https://hrcak.srce.hr/index.php?show=clanak&id_clanak_jezik=148443
65. Yeo, J., Ende, R., (2019.), *Advancing Cyber Risk Management from Security to Resilience*, [e-publikacija], preuzeto s: advancing-cyber-risk-management-from-security-to-resilience.pdf
66. Zakon o osiguranju, Narodne novine br. 30/15, 112/18, 63/20, 133/20 (2020.), https://www.zakon.hr/z/369/Zakon-o-osiguranju
67. Zurich, (b.d.), *Zurich Cyber Solution*, Pristupljeno: 25. 8. 2022. https://www.zurich.com/en/products-and-services/protect-your-business/what-we-protect/cyber-risk

POPIS SLIKA

POPIS TABLICA

POPIS GRAFIKONA

ŽIVOTOPIS KANDIDATA

Ime i prezime: Daria Čurković

Datum i mjesto rođenja: 21.8.1997., Zagreb

Obrazovanje:

- 2012. – 2016.: X. gimnazija Ivan Supek
- 2016. – danas: Sveučilište u Zagrebu, Ekonomski fakultet, Trg J. F. Kennedyja 6, smjer: Financije

Radno iskustvo:

- *1/2022 – danas, Zagrebačka banka d.d.,* Savska 60-62, Zagreb (administrativni asistent, ispomoć VPO-ima)
- *12/2020 – 01/2021, Financijska agencija,* Vrtni put 3, Zagreb (administracija)
- *02/2019 – 03/2020, Financijska agencija,* Ulica grada Vukovara 70, Zagreb (skeniranje i unos podataka, arhiviranje, dostava dokumenata klijentima, zaprimanje pošte)
- *07/2018, Croatia osiguranje d.d.,* Savska 41, Zagreb (skeniranje i arhiviranje dokumenata, unos podataka)
- *09/2017 – 12/2017, eSport arena d.o.o.,* Avenija Dubrovnik 16, Zagreb (rad na recepciji)
- *Ostalo – Ledo d.d., Studio Conex d.o.o., Ex-Alto d.o.o.* (promocije i eventi)

Vještine:

- Microsoft Office (Excel, Word, PowerPoint)
- timski rad, komunikativnost
- organiziranost, analitičnost
- engleski jezik – aktivno u govoru i pismu
- vozačka dozvola B kategorije