Danijel Bara
BCC Services d.o.o.
danijel.bara@gmail.com

Stručni članak

ULOGA *CYBER*-OSIGURANJA U UPRAVLJANJU I PRIJENOSU RIZIKA *CYBER*-SIGURNOSTI

U današnjemu vremenu, koje u mnogočemu ovisi o informatičkoj tehnologiji i elektroničkim komunikacijama, poslovni subjekti sve više postaju izloženi raznim oblicima cyber-kriminala. Cyber-kriminalni napadi i događaji poput cyber-špijunaže, cyber-ratovanja, cyber-terorizma, cyber-prijevara ili cyberbullyinga[1], mogu imati razorne posljedice i velik utjecaj na poslovne subjekte, njihove djelatnike, kupce, osiguranike, ali i treće osobe. Takve radnje mogu dovesti do krađe intelektualnoga vlasništva, ugrožavanja korporativne strategije, pronevjere ili manipuliranja s povjerljivim i osobnim podatcima, smanjenja reputacije brenda i poslovnoga subjekta, a u pojedinim slučajevima mogu čak ugroziti postojanje poslovnoga subjekta. Kako cyber-kriminal ima velik utjecaj na organizacije, problem cyber-sigurnosti prerastao je IT odjel, koji je sve donedavno bio isključivo nadležan za poslove cyber-sigurnosti, te je postao jedan od strateških rizika nad kojima izvršni menadžment mora preuzeti vlasništvo. Ovaj članak istražuje utjecaj koji cyber-kriminal ima na poslovanje, kao i proaktivne mjere koje mogu transferirati rizike od cyber-prijetnji, a posebno se to odnosi na cyber-osiguranje kao dodatni alat za prijenos rizika. U posljednje vrijeme svjedoci smo porasta cyber-kriminala i u Republici Hrvatskoj, te se u članku analizira i hrvatsko tržište cyber-osiguranja i predlaže model čiji je cilj povećanje ponude cyber-osiguranja na tržištu osiguranja.

Držimo nužnim primijeniti proaktivnu strategiju za upravljanje cyber-rizicima u poslovnim subjektima, pogotovo onima koji imaju značajnu podatkovnu i informacijsku imovinu ili posluju putem interneta, kako bi zaštitili svoju infrastrukturu i osigurali opstojnost na tržištu. Ako je to postignuto, cyber-osiguranje može biti dio sveukupne poslovne strategije smanjivanja rizika.

***Ključne riječi**: osiguranje, cyber-osiguranje, cyber-sigurnost, cyber-kriminal, cyber-rizik, model cyber-osiguranja*

1. UVOD

Rastuća kompleksnost, međusobna povezanost i međuovisnost tehnologije *cyber*-zaštitu stavlja pred velika iskušenja. U praksi ne možemo sagraditi zidove dovoljno visoke ili dovoljno snažne da služe kao potpuna zaštita (OpenDNS, 2014). Prema riječima Roberta S. Muellera, direktora FBI-a: „*postoje samo dvije vrste tvrtki: one koje su hakirane*[2] *i one koje će biti hakirane. Pa čak i one konvergiraju u jednu kategoriju: tvrtke koje su hakirane i one koje će opet biti hakirane*" (Mueller, 2012).

2. ZNAČAJKE *CYBER*-RIZIKA

Postoji konstantan rizik od sigurnosnih propusta koji su čak u stanju ugroziti i funkcioniranje tvrtke. Ovakve opasnosti najčešće su uzrokovane ljudskim ponašanjem, više nego što su to tehnološki rizici. Kako bi se smanjili *cyber*-rizici definirane su četiri temeljne aktivnosti (CROForum, 2014):

Priprema Potrebno je razumjeti svoju kritičnu imovinu; razvijati sposobnosti za rješavanje različitih razina rizika; utvrditi sklonost riziku i upravljanje rizicima ugraditi u cijelu organizaciju.

[1] *Cyberbullying* je namjerno štetno ili uznemirujuće djelovanje putem informacijske tehnologije. *Cyberbullying* može biti ograničen na objavljivanje glasina ili tračeva o osobi na internetu, čime se izaziva mržnju kod drugih osoba, ili može ići do te mjere da se o žrtvi izdaje materijal koji ju ozbiljno vrijeđa i ponižava. https://en.wikipedia.org/wiki/Cyberbullying (15. 9. 2015.).

[2] Hakiranje je pojam koji u kontekstu ovoga rada označava neovlašten pokušaj zaobilaženja sigurnosnih mehanizama informacijskoga sustava ili mreže. https://en.wiktionary.org/wiki/hacking (15. 9. 2015.).

Zaštita	Osigurati dobro utemeljenu i ponovljivu *cyber*-pripravnost; poduzeti ocjenjivanje prijetnji i kontrola: osigurati odgovarajućom pozornošću provjeru procesa za treće osobe; omogućiti i osnažiti upravljanje incidentima i sposobnost odgovora; razvijati i provoditi plan odgovora na incident, kontinuirano se obrazovati i usavršavati.
Detekcija	Razviti otkrivanje i kontinuirano praćenje sposobnosti za rješavanje nepravilnosti i prijetnji prema imovini tvrtke.
Poboljšanje	Izgraditi sveobuhvatnu bazu podataka sigurnosnih incidenata koji podržavaju kontinuirano učenje i omogućiti oporavak od incidenta u najkraćemu roku.

3. IZLOŽENOST *CYBER*-RIZICIMA

Potencijalni gubitci koji proizlaze iz *cyber*-napada ili nenamjernih IT propusta razvrstani su u 11 kategorija, kao što je prikazano u sljedećoj tablici.

Tablica 1. Kategorije gubitaka koji proizlaze iz *cyber*-napada i nenamjernih IT propusta

	KATEGORIJA GUBITKA	OPIS
A	Krađa intelektualnoga vlasništva	Gubitak vrijednosti imovine intelektualnoga vlasništva, izraženo u smislu gubitka prihoda kao rezultat smanjenoga udjela na tržištu.
B	Prekid poslovanja	Izgubljena dobit ili drugi troškovi nastali zbog nedostupnosti IT sustava ili podataka kao posljedica *cyber*-napada ili ostalih zlonamjernih IT propusta.
C	Gubitak podataka i aplikacija	Trošak rekonstrukcije podataka ili softvera koji je izbrisan ili korumpiran.
D	*Cyber*-iznuda	Trošak stručnjaka za rukovanje incidentom *cyber*-iznude, u kombinaciji s iznosom plaćanja otkupnine.
E	*Cyber*-kriminal/*cyber*-prijevara	Izravni financijski gubitak koji je pretrpjela organizacija, a koji proizlazi iz korištenja računala za počinjenje prijevare ili krađe novca, vrijednosnih papira ili druge imovine.
F	Događaj povrede privatnosti	Trošak istraživanja i odgovora na događaj povrede privatnosti, uključujući i IT forenziku i obavještavanje zahvaćenih nositelja podataka. Odgovornosti potraživanja trećih strana koje proizlaze iz istoga incidenta. Kazne od regulatora i udruga.
G	Mrežne pogreške	Obveze trećih strana koje proizlaze iz nekih sigurnosnih događaja koji se javljaju u organizaciji IT mreže ili prolaze kroz nju da bi napali treću osobu.
H	Utjecaj na reputaciju	Gubitci prihoda koji proizlaze iz povećanja odljeva kupaca ili smanjenja volumena transakcija, koji se mogu izravno pripisati objavi događaja povrede sigurnosti.
I	Fizičko oštećenje imovine	Gubitak prve strane zbog uništenja fizičke imovine koji proizlazi iz *cyber*-napada.
J	Smrt i tjelesna oštećenja	Odgovornost trećih osoba za smrt i tjelesne ozljede proizašle iz *cyber*-napada.
K	Istraživanje incidenta i troškovi odgovora	Izravni troškovi nastali istraživanjem i zatvaranjem incidenta i smanjivanje gubitaka nakon incidenta. Odnosi se na sve ostale kategorije/događaje.

Izvor: Marsh, 2015.

Povećanje međusobne povezanosti, globalizacija i komercijalizacija *cyber*-kriminala dovode do veće učestalosti i ozbiljnosti *cyber*-incidenata, uključujući povrede podataka. Privatnost i zaštita podataka jedan je od ključnih *cyber*-rizika (EC3, 2014).

Prema Allianzovu izvještaju *cyber*-rizika (Allianz, 2015), u skoroj budućnosti mogu se očekivati i veće novčane kazne za slučajeve povrede podataka. Zakonodavstvo je već postalo mnogo strože u SAD-u, Hong Kongu, Singapuru i Australiji, dok Europska unija traži da se dogovore paneuropska pravila o zaštiti podataka. U ovisnosti o pojedinoj zemlji mogu se očekivati čvršće smjernice u tome smjeru.

Prekid poslovanja, krađe intelektualnoga vlasništva i *cyber*-iznude, bilo za financijsku, bilo za nefinancijsku dobit, povećavaju potencijalni rizik. Troškovi prekida poslovanja mogu biti jednaki ili čak premašiti izravne gubitke od povrede podataka. Utjecaj prekida poslovanja pokrenut tehničkim kvarom često je podcijenjen u odnosu na *cyber*-napad (Allianz, 2015).

Važno je napomenuti kako velike kompanije i državne tvrtke nisu jedine ranjive na razorne *cyber*-napade. Podatak je taj koji čini posao atraktivnim, a ne veličina – pogotovo ako je riječ o zanimljivim podatcima, kao što su kontakt-informacije o kupcima, podatci o kreditnim karticama, zdravstveni podatci ili vrijedno intelektualno vlasništvo (Armerding, 2015).

Manje su tvrtke atraktivne jer nemaju iste resurse kao velika poduzeća, stoga imaju tendenciju ka slabijoj strategiji *cyber*-sigurnosti. Zbog niskih troškova prodaje više posluju *online*[3] i putem različitih *cloud*-usluga[4]. Te se tvrtke koriste slabijom sigurnosnom zaštitom i slabijom tehnologijom enkriptiranja, tako da su više osjetljive na širok raspon *cyber*-napada. Izvještaj Verizon Communications 2013 vezano uz povrede podataka utvrdio je kako je blizu 62% povreda podataka 2013. godine bilo usmjereno na mala i srednja poduzeća. Slabosti malih i srednjih poduzeća, koje su kriminalcima privlačne (Verizon, 2013), jesu:

- nedostatak vremena, proračuna i stručnosti za provedbu sveobuhvatnih sigurnosnih obrana
- nedostatak IT sigurnosnoga stručnjaka
- nedostatak svijesti o rizicima
- nedostatak obuke zaposlenika
- neuspjeh ažuriranja sigurnosne obrane
- *outsourcing* sigurnosti nekvalificiranim izvođačima ili administratorima sustava
- neuspjeh osiguranja krajnjih točki.

Osim toga, u današnjemu povezanom svijetu male tvrtke uključene su u složenije mreže, mobilne veze i *cloudom* sa svojim klijentima i partnerima. Ako mala tvrtka u svojemu portfelju ima veliku tvrtku kao partnera ili kupca, vrlo je privlačna meta jer dopušta ulazak u unosnije tržište kroz stražnja vrata.

4. OZBILJNIJI *CYBER*-INCIDENTI U SVIJETU

Ranjivost sustava industrijskih kontrola na *cyber*-napad predstavlja veliku prijetnju. Zabilježeno je nekoliko slučajeva manipulacije centrifugama u nuklearnim elektranama, kao i ostalim elektranama, koji su u pojedinim slučajevima nanijeli izrazite štete, kao u slučaju Stuxneta[5] i iranskoga nuklearnog programa (Zetter, 2014), ili u slučaju Dragonfly (Symantec, 2015) virusa i američkih centrala (Maloof, 2014).

Početkom ove godine pojavila se vijest kako je američka vlada verzijom Stuxneta neuspješno pokušala napasti nuklearne elektrane u Sjevernoj Koreji (Menn, 2015). Možemo pretpostaviti da će se ovakvi i slični napadi nastaviti i u budućnosti. Iako se ovi rizici ubrajaju u *cyber*-terorizam, odnosno *cyber*-ratovanje, oni zorno prikazuju koliko je globalno društvo osjetljivo na ovakve rizike, kao i koje opasnosti postoje od potencijalnih budućih napada u tome smjeru.

Iako nije službeno potvrđeno daje riječ o *cyber*-napadu, prekid rada NYSE-a (New York Stock Exchange) u srpnju, na gotovo četiri sata (CNN Wire Service, 2015), dovodi se u vezu sa *cyber*-ratovanjem i tvrdnjom da se u pozadini događaja kriju kineski hakeri[6] (Allen-Ebrahimian, 2015).

Uz navedene incidente, 2015. godinu obilježili su mnogobrojni incidenti koji govore u prilog činjenici kako *cyber*-rizici čine goleme štete gospodarstvu, a prema Allianzovu izvještaju (Allianz, 2015) te štete na globalnoj razini iznose 445 milijardi dolara, dok 50% toga iznosa odlazi na 10 najvećih svjetskih ekonomija.

Problem sa sigurnosnim napadima toliko je ozbiljan da je Pentagon nedavno objavio (Meek, 2015) kako radi na planu za financiranje alata i znanstvenika koji bi organizacijama pomogao u obrani protiv sveprisutne prijetnje klasičnoga *cyber*-napada, poznatog kao Distributed Denial-of-service (DDoS)[7]. Problem s DDoS napadom je što je on relativno jednostavan za počinitelja, pa napadač ne mora imati preveliko informatičko znanje da bi ga potaknuo. Osim toga, na internetu postoje brojni besplatni programi, kao na primjer LOIC[8], i objašnjenja (Ashwini, 2014) kako počiniti DDoS napad.

S druge strane, u ovoj su godini zabilježeni i mnogo jači i sofisticiraniji DDoS napadi, za koje je ipak potrebno mnogo više znanja i resursa za pokretanje. Ti napadi premašivali su količinu podataka od 100 gigabita u sekundi i 50 milijuna paketa u sekundi, što su enormne količine podataka kojima se opterećuju serveri, pa je čak i Google, koji ima jaku i distribuiranu serversku infrastrukturu, prošle godine nakratko prekinuo rad prouzročen DDoS napadom (D'Mello, 2014). Mete ovih napada najčešće su medijske kuće, *web*-trgovine i sl., a prema podatcima (Matthews, 2015), prosječni troškovi po satu ovakvoga napada iznose više od 40 000 dolara.

---

[3] *Online*-poslovanje – obavljanje poslovnih procesa na internetu. http://searchcio.techtarget.com/definition/e-business, (15. 9. 2015.).

[4] *Cloud* – opći termin koji se upotrebljava za pružanje iznajmljenih usluga putem interneta. http://searchcloudcomputing.techtarget.com/definition/cloud-computing, (15. 9. 2015.).

[5] Prema https://en.wikipedia.org/wiki/Stuxnet, Stuxnet je američko-izraelsko *cyber*-oružje i kompjuterski crv (14. 9. 2015.).

[6] Haker – netko tko traži i iskorištava slabosti u računalnome sustavu ili mreži računala. https://en.wikipedia.org/wiki/Hacker (15. 9. 2015.).

[7] DDoS napad je takav *cyber*-napad s više računala na neki računalni servis s ciljem da se korisnicima onemogući njegovo korištenje. https://en.wikipedia.org/wiki/Denial-of-service_attack (15. 9. 2015.).

[8] LOIC (Low Orbit Inon Cannon) je besplatan program koji se upotrebljava za analizu rada mreže i primjenu DoS napada. https://en.m.wikipedia.org/wiki/Low_Orbit_Ion_Cannon (15. 9. 2015.).

Kao jedan od najvećih incidenata u 2015. godini zabilježen je OPM (Office Of Personnel Management) *cyber*-sigurnosni incident (OPM, 2015), koji je po mnogočemu najveći sigurnosni incident u povijesti, a sastojao se od dvaju neovisnih incidenata. Veći od dvaju incidenata utjecao je na otuđenje podataka oko 21,5 milijuna državnih službenika, a otkriven je potkraj svibnja, dok je drugi incident ovu državnu agenciju pogodio u travnju, otkrivajući kadrovske podatke oko 4,2 milijuna ljudi. Iako akteri napada nisu službeno objavljeni, izvješća ih povezuju s kineskim hakerima. Detalji o opsegu napada i njihov utjecaj na milijune saveznih radnika još nisu objavljeni, no neke od posljedica već su počele ostavkom OPM ravnatelja. O ozbiljnosti samoga incidenta dovoljno govori i podatak kako su odnosi između dviju zemalja narušeni ovim incidentom te je američki predsjednik Obama izrazio zabrinutost kineskom predsjedniku Jinpingu zbog *cyber*-sigurnosnoga ponašanja Kine (Reuters, 2015a). *Cyber*-sigurnost također je bila i jedna od tema njihova sastanka u rujnu ove godine (BBC, 2015a), a izvjesna uvertira tomu sastanku bila je uhićenje skupine kineskih hakera, optuženih da su otuđili informacije od američkih firmi i plasirali ih kineskim tvrtkama (BBC, 2015b), čime je kineska vlada nastojala odbaciti optužbe o njihovoj uključenosti u incident. Tijekom godine zabilježeno je nekoliko sigurnosnih incidenata vezanih uz američko zdravstveno osiguranje, pa je tako u svibnju otkriveno kako je 1,1 milijun podataka o korisnicima osiguravajućega društva CareFirst BlueCross BlueShield kompromitirano (Goldman, 2015), u napadu na osiguravajuće društvo Premera BlueCross BlueShield otuđeni su podatci o njihovih 11,2 milijuna korisnika (Reuters, 2015b), dok je zdravstveno osiguranje Anthem pretrpjelo golemu štetu u *cyber*-napadu, u kojemu su napadači došli u posjed podataka oko 80 milijuna njihovih korisnika i zaposlenika (McNeal, 2015).

U veljači je otkrivena milijardu dolara „teška" *cyber*-pljačka, na štetu više od 100 banaka diljem svijeta (Westervelt, 2015). Krađa koju je otkrila tvrtka Kaspersky Lab obavljena je tako da su se kradljivci infiltrirali u mreže banaka pomoću taktika kao što su krađe identiteta i dobivanja pristupa ključnim resursima, uključujući korisnička prava zaposlenika. *Cyber*-kriminalna mreža, poznata kao Carbanak, iskoristila je ta korisnička prava te napravila lažne transfere kojima su proslijedili sredstva na bankomate te na taj način preusmjerili više od 1 milijarde dolara. Napadi su prvi put otkriveni u prosincu 2013. godine, a intenzivirali su se između veljače i travnja prošle godine.

U lipnju je otkriveno kako su napadnuti pojedini interni sustavi jedne od najvećih svjetskih tvrtki na području sigurnosne zaštite Kaspersky Lab (Kuranda, 2015), a gotovo u isto vrijeme objavljen je i podatak da je napadnuta talijanska tvrtka Hacking Team (Greenberg, 2015), za koju se poslije utvrdilo da se bavi špijuniranjem svojih korisnika.

Vrlo specifičan napad nedavno je otkrila tvrtka Kaspersky Lab, a vezan je uz preuzimanje nadzora nad satelitima u Zemljinoj orbiti i korištenje skrivenih prijamnih stanica u Africi i na Bliskome istoku, kako bi se prikrili napadi na zapadne vojne i državne mreže. Ovaj se napad povezuje sa skupinom *Ouroboros*, koja je odgovorna za prošlogodišnje masovne napade na informatičku infrastrukturu Ukrajine, a povezana je i sa *cyber*-napadima na američku i britansku vladu, a riječ o jednoj od najjačih hakerskih skupina na svijetu. Problem ovakvoga napada preko satelita je što se danas zapravo nemoguće zaštititi od ovakvoga napada zbog činjenice da u orbiti postoji 1265 satelita od kojih su neki stari i 50-ak godina, odnosno u doba kada nije predviđana nikakva zaštita te sateliti s prijamnim stanicama na Zemlji komuniciraju bez enkripcije (Drozhzhin, 2015).

5. *CYBER*-INCIDENTI U REPUBLICI HRVATSKOJ

S obzirom na navedeno, logično je da tvrtke koje posluju u Republici Hrvatskoj također nisu imune na *cyber*-kriminal. U Republici Hrvatskoj, u godinama prije ulaska u EU, postojali su sporadični slučajevi *cyber*-napada, međutim, ulaskom u EU, prema javno objavljenim podatcima o prikazanim incidenata, taj se broj dramatično povećao, a napadi su postali veći i sustavniji. U 2014. godini, nakon šest mjeseci uzastopnih *cyber*-napada na korisnike internet-bankarstva u Republici Hrvatskoj, voditelj Ureda za odnose s javnošću HNB-a (Hrvatska narodna banka) izjavio je da je prema dostupnim podatcima uistinu u konačnici otuđeno i plaćeno manje od šest posto od potencijalno neovlaštenih transakcija, u ukupnome iznosu od gotovo 1,8 milijuna kuna (Ivezić, 2014).

Sredinom ožujka 2015. godine Hrvatska je ponovno bila na meti snažnih *cyber*-napada. Napadi su došli preko višestrukih vektora, od kojih se jedan odnosio na poruke e-pošte, a drugi na *online*-bankarstvo. Ono što je problematično u tim napadima jest da su se događali preko *exploita*[9] koji se nalazio u okviru reklamnih poruka na najvećim hrvatskim pružateljima internet-promocije (Portal Svijet Sigurnosti, 2015).

Stručnjaci za *cyber*-sigurnost očekuju daljnji porast prijetnji *cyber*-sigurnosti, s novim inovativnim napadima. *Cyber*-

[9] *Exploit* je komad softvera, komad podataka ili slijed naredbi koje iskorištava *bug* ili ranjivost kako bi uzrokovao pojavu neželjenoga ili neočekivanoga ponašanja računalnoga softvera, hardvera ili nečega elektroničkog (obično kompjuterizirano). https://en.wikipedia.org/wiki/Exploit_(computer_security) (15. 9. 2015.).

kriminal je isplativ i rizici da će kriminalci biti uhvaćeni ili kažnjeni još uvijek su zanemarivi (Schrader, 2015).

Dok su zasad sofisticirani napadi rezervirani za *cyber*-ratovanje, napadi poput posljednjega koji se dogodio u Republici Hrvatskoj ne samo da su jednostavni nego na internetu postoje i besplatne upute kako napraviti takav alat za ucjenu (Khandelwal, 2015). Postojanje takvih uputa dodatno otežava rad sigurnosnim stručnjacima i stoga je realno očekivati kako će ovakvi napadi postati još učestaliji. Nešto složenije napade moguće je danas kupiti ili naručiti putem *darknet weba*[10], od kojih se neki čak mogu kupiti uz IT podršku, a koji nisu pretjerano skupi i obično su odmah dostupni. Očito je da se ovakve usluge ne kupuju putem tradicionalnih metoda plaćanja, što je jedan od razloga porasta alternativnih oblika plaćanja i *crypto*-valuta, kao što je *bitcoin*[11].

6. *CYBER*-OSIGURANJE

6.1. TRŽIŠTE *CYBER*-OSIGURANJA

Financijske implikacije *cyber*-incidenta mogu imati znatan utjecaj na bilancu tvrtke u obliku stvarno prouzročene štete, troškova obavijesti korisnicima, potencijalnih kazni za gubitke te –dodatno na sve to – štete za ugled tvrtke. Usto, tvrtke se potencijalno izlažu riziku odgovornosti ako se adekvatno ne osiguraju od *cyber*-riziku, bilo kupnjom osiguranja ili nekom drugom strategijom za smanjenje rizika. Ako se dogodi *cyber*-incident, postavit će se pitanje zbog čega nije implementirano odgovarajuće osiguranje i/ili strategija upravljanja *cyber*-rizicima (Pearson, 2014).

U svjetlu nedavnih mnogobrojnih *cyber*-incidenata, mnogo je toga objavljeno na temu *cyber*-osiguranja od odgovornosti. Profesionalne police odgovornosti za tvrtke koje pružaju računalne hardverske i softverske usluge povećale su svoj opseg te uključuju prikupljanje, pohranjivanje i obradu elektroničkih podataka svojih kupaca. Iako tržište za osiguranje od *cyber*-odgovornosti postoji desetak godina, tek je nedavno doživjelo povećanu potražnju i ekspanziju. Prema istraživanju PR Newswire (2015), globalno tržište osiguranja od *cyber*-rizika naraslo je s 850 milijuna USD u 2012. godini na 2,5 milijardi USD u 2014. godini.

Očekuje se da će potražnja za *cyber*-osiguranjem u Europi znatno rasti, nakon što se novi Zakon o zaštiti općih podataka (GDPR – General Data Protection) finalizira do kraja 2015. godine, a očekuje se da će stupiti na snagu do 2017. godine u svim državama članicama EU-a. S tim zakonom morat će se izvještavati o *cyber*-napadima. To će zasigurno dati više snage regulatoru, uz povećanje kazne u slučaju neobavještavanja – do 1 milijun EUR (1,3 milijuna USD) ili 2% globalnoga godišnjeg prometa tvrtke. Tržište *cyber*-osiguranja u Europi relativno je nerazvijeno, s procijenjenom vrijednosti od 150 milijuna USD u zaračunatoj bruto premiji u 2014. Za usporedbu, u SAD-u je prihodovano oko 90% globalne premije na tržištu *cyber*-osiguranja u vrijednosti od 2 milijarde USD bruto premije u 2014. godini (PR Newswire, 2015). Iako je tržište *cyber*-osiguranja SAD-a najrazvijenije na svijetu, ipak prema podatcima istraživanja Hanover Research (2014), 54% ispitanih tvrtki još uvijek u svojoj ponudi nema osiguranje od *cyber*-rizika, a među njima je 58% onih koji u idućoj godini u svoju ponudu planiraju uvesti ovu vrstu osiguranja, što je evidentan pokazatelj trenda i mogućnosti razvoja *cyber*-osiguranja.

Procjenjuje se da će ovo tržište na globalnoj razini do 2020. godine dosegnuti vrijednost od oko 7,5 milijardi USD, a ako osiguravajuća društva ubrzo ne reagiraju na ponudu proizvoda, suočit će se s novim konkurentima na tome tržištu, kao što je Google, navodi se u nedavno objavljenome izvještaju PwC-a (PwC, 2015).

6.2. ZNAČAJKE PROIZVODA

Raznolikost nedavnih *cyber*-incidenata skrenula je pozornost na to koliku važnost treba imati odgovarajuća osigurateljna pokrivenost u slučaju kada *cyber*-napad ugrožava poslovanje. Nema poslovanja koje je imuno na *cyber*-napade, koji mogu opustošiti ne samo IT okruženje nego u potpunosti ugroziti poslovanje tvrtke. Unatoč svemu tome, *cyber*-osiguranje proizvod je koji je još uvijek u povojima. Iako postoji širok opseg dostupnih opcija *cyber*-osiguranja, one mogu biti vrlo ograničene jer standardizirana procjena *cyber*-rizika još uvijek ne postoji. Upravo je to mjesto gdje prava *cyber*-informacija može pomoći pri donošenju odluka oko jedinstvene organizacije *cyber*-rizika, potencijalnoga utjecaja,

[10] Darknet je privatna mreža u kojoj se povezivanja događaju samo između pouzdanih korisnika koji se koriste nestandardnim protokolima i portovima. To uključuje i tzv. *deep web*, koji se sastoji od neindeksiranih *web*-stranica koje se mogu naći jedino ako se točno zna što se traži. https://en.wikipedia.org/wiki/Darknet (15. 9. 2015.).

[11] Bitcoin je inovativna mreža plaćanja i nova vrsta valute. Bitcoin upotrebljava *peer-to-peer* tehnologiju za rad bez središnje vlasti ili banaka; upravljanje transakcijama i izdavanje bitcoina provodi se zajednički od strane mreže. Bitcoin je otvoren sustav; njegov dizajn je javan, nitko ne posjeduje ili kontrolira bitcoin i svatko može sudjelovati. Kroz mnoge od svojih jedinstvenih svojstava, bitcoin omogućuje prijenos sredstava bez mogućnosti praćenja primatelja i pošiljatelja bitcoina. http://crobitcoin.com/bitcoin/sto-je-bitcoin/ (15. 9. 2015.).

kao i gdje je potrebno usredotočiti sigurnosne napore i proračun, kada je riječ o odabiru odgovarajućega osiguranja od *cyber*-odgovornosti (SurfWatch Labs, 2014).

Polica osiguranja sama za sebe definitivno ne može smanjiti rizik, ali može djelovati kao mehanizam prijenosa rizika koji štiti bilancu tvrtke od ozbiljnoga financijskog šoka. Većina osiguratelja koji nude *cyber*-osiguranje također pruža dodatne usluge kao što su dostupnost IT stručnjaka ili forenzičara koji mogu pomoći prije i poslije gubitka podataka te savjetovati o odgovarajućim politikama i postupcima kako bi se osigurala najbolja informacijska sigurnost (Pearson, 2014).

Iako se osiguranje može činiti kao uzak i netehnički način pristupa tako složenoj i dalekosežnoj prijetnji, ipak daje vrijednu perspektivu *cyber*-riziku (PwC, 2014), kao što je vidljivo u sljedećoj tablici.

Tablica 2. Osiguranje kao vrijedna perspektiva u okviru *cyber*-rizika

Razlog perspektive	Opis
Premijski trošak	Osiguranje računa cijenu *cyber*-opasnosti kroz premiju koju tvrtka plaća, a izgledi za smanjivanje premije tada potiču tvrtke da poduzmu korake za ublažavanje rizika.
Prevencija gubitka	Osiguranje ide ruku pod ruku sa sprečavanjem gubitka. Osiguratelji će pomoći smanjiti gubitke tvrtkama pružajući uvid u vlastitu bazu i preko postojećih klijenata.
Znanje i iskustvo	Osiguratelji donose svoje znanje i iskustvo o različitim vrstama rizika, a koji se onda mogu primijeniti i na *cyber*-rizike.

Izvor: SurfWatch Labs, 2014.

6.3. VRSTE I POKRIĆA *CYBER*-POLICA OSIGURANJA

U istraživanju Hanover Research (2014), 8% osiguratelјnih tvrtki nudi samostalnu policu *cyber*-osiguranja, u 63% slučaja tvrtke nude osiguranje od *cyber*-odgovornosti u kombinaciji ili kao dodatak nekim drugim oblicima osiguranja, kao što su police vlasnika poslovanja[12] (BOP – Business Owner Policy) ili police profesionalne odgovornosti, dok 29% osiguranja nude obje kombinacije polica.

Samostalne police *cyber*-osiguranja nude se pod različitim imenima, a pokrivaju *cyber*-rizike, informacijsku sigurnost, privatnost i medijsku odgovornost. Za razliku od drugih vrsta osiguranja, ne postoji standardni obrazac prema kojemu industrija osiguranja u cjelini pribavlja *cyber*-pokriće. Iako to predstavlja neke izazove za kupnju pokrića, osobito za neupućene, to često daje više prostora za pregovore o uvjetima *cyber*-polica od mnogih drugih vrsta pokrića (Raptis, 2015).

Većina *cyber*-polica na tržištu trenutačno nudi neke kombinacije pokrića tradicionalne odgovornosti kao zaštitu protiv zahtjeva trećih osoba i pokrića prve strane kao zaštitu od gubitaka koje su pretrpjeli osiguranici. Također su važni uvjeti *cyber*-polica koji mogu imati znatan utjecaj na raspoloživa pokrića. Iako niti jedna organizacija ne može razumno očekivati osiguranje svih dostupnih komponenti pokrića, svijest o razlikama među policama koje se nude najvažnija je za optimiziranje novca utrošenoga na premiju osiguranja (Raptis, 2015).

Kod osiguranja trećih osoba (odgovornost), potrebno je posebnu pozornost obratiti na sljedeće:

Pokriće privatne (osobne) odgovornosti. Ovaj tip pokrića uključuje odgovornost prema osiguranim kupcima/klijentima i zaposlenicima zbog povrede osobnih podataka. Potrebno je obratiti pozornost na neuspjeh zaštite povjerljivih informacija, bez obzira na uzrok. Primjerice, u polici može stajati *osiguranje bilo koje pogreške*, bez posebnoga naglašavanja namjera. Pojedine *cyber*-police također pružaju pokrivenost neuspjeha osiguranika u otkrivanju gubitka podataka o privatnosti u skladu sa zakonima o privatnosti. Budući da to može biti glavni dio odgovornosti u slučaju povrede podataka, važno je obratiti pozornost na ovo pokriće.

Regulatorne akcije. Postoje bitna odstupanja među *cyber*-policama u tome pružaju li, i u kojoj mjeri, pokrića za regulatorne i druge vladine akcije. Čak i kada pružaju regulatorno pokriće, neke police zahtijevaju da se osiguratelјni slučaj pokrene od formalnoga tijela kako bi se pokrenula obveza obrane. Ovaj limit obično onemogućuje obranu u istražnoj fazi vladinih akcija, što je često i najskuplja faza za osobe pod istragom. Potrebno je obratiti pozornost na ona pokrića koja uključuju obranu u najranijoj fazi istrage, koje obično uključuju civilne istražne zahtjeve ili slične zahtjeve za informacijama. Civilne su kazne pokrivene mnogim *cyber*-policama i treba obratiti pozornost je li to pokriće isključeno.

[12] BOP – Business Owner Policy posebna je vrsta osiguranja namijenjena malim i srednjim tvrtkama. Police obuhvaćaju osiguranje imovine i opće osiguranje od odgovornosti u jedinstvenu policu, što smanjuje cijenu police koja bi bila skuplja od dviju odvojenih polica osiguranja. https://en.wikipedia.org/wiki/Business_owner%27s_policy (15. 9. 2015.).

Troškovi obavijesti. Ovo pokriće uključuje troškove obavijesti trećih osoba potencijalno pogođenih povredom podataka. Trošak slanja obavijesti uključen je u većini *cyber*-polica. Međutim, mnoge police, često nakon odobrenja, ograničavaju broj pojedinaca koji moraju biti obaviješteni, kao i način(e) obavještavanja. Neke police također mogu dati osiguratelju kontrolu nad procesom obavijesti (što je često osjetljivo za osiguranika). Ta ograničenja mogu definirati podjelu troškova obavijesti ako dođe do povrede, a osiguratelj može zatražiti od organizacije odricanje dijela kontrole nad procesom obavijesti.

Upravljanje krizom. Pokrivenost kriznoga menadžmenta uključuje troškove upravljanja odnosa s javnošću. Većina *cyber*-polica sadržava neki oblik pokrića upravljanja krizom. Katkad osiguranik treba odabrati dobavljača s unaprijed definiranoga popisa. U većini slučajeva, ako osiguranik odabere drugoga dobavljača, osiguratelj nije dužan platiti te usluge. Međutim, ovo ograničenje može biti po dogovoru.

Pozivni (*call*) centri. Ovo pokriće može biti uključeno u pokriće troškova obavijesti i/ili pokriće upravljanja krizom, može biti samostalno pokriće ili se uopće ne osigurava. Zbog činjenice da troškovi pozivnoga centra imaju tendenciju biti jedan od većih troškova povezanih s povredama podataka, važno je izrijekom utvrditi je li ovo pokriveno, kao i sva primjenjiva ograničenja (uključujući broj pogođenih osoba koje ispunjavaju uvjete za primanje usluga pozivnoga centra, sate i mjesta pozivnoga centra te posebne usluge koje će pružiti osoblje pozivnoga centra).

Nadzor identiteta. Iako je ovo pokriće uključeno u većini *cyber*-polica, kao i pokriće pozivnih centara, moguće je ograničiti broj pogođenih pojedinaca koji mogu primati usluge te propisati dostupne dobavljače.

Prijenos virusa/zlonamjernoga koda. Kao što sam naziv sugerira, ovo pokriće štiti od odgovornosti potraživanja navodne naknade štete od prijenosa virusa i drugoga malicioznog koda ili podataka. Nemaju sve police *cyber*-osiguranja ovo pokriće. Prije nego što se odredi prioritetom, organizacije trebaju uzeti u obzir u kojoj mjeri njihovi operativni sustavi realno imaju potencijal biti izvorom ove vrste odgovornosti.

Osiguranje prvih strana: definiranje ključnih pojmova.

Krađa i prijevara pokriva određene troškove vezane uz krađe ili uništenja podataka osiguranika, kao i krađu osiguranih sredstava.

Forenzičke istrage pokrivaju troškove utvrđivanja uzroka gubitka podataka.

Pad mreže/prekid poslovanja pokriva troškove gubitka poslovanja, kao i dodatne troškove koji proizlaze iz prekida računalnoga sustava osiguranika. Neke *cyber*-police zahtijevaju da je prekid uzrokovan namjernim *cyber*-napadom, a neke ne. Uobičajena ograničenja ovoga pokrića uključuju i zahtjev da prekid traje određenu definiranu duljinu vremena prije početka pokrića i ograničenje ukupne duljine prekida koji će biti pokriven. Ovo pokriće također može uključiti potencijalne troškove poslovanja.

Iznuda pokriva troškove otkupa ako treća strana zahtijeva isplatu zbog suzdržavanja od javnoga objavljivanja ili uzrokovanja štete objavljivanjem povjerljivih elektroničkih podataka osiguranika.

Gubitak i obnova podataka pokriva troškove vraćanja podataka ako su izgubljeni te u nekim slučajevima dijagnosticiranje i popravak uzroka gubitka. To je uključeno u nekim *cyber*-policama. Pokriće gubitka i obnove podataka obično podliježe značajnom zadržavanju, a može biti ograničeno u smislu pitanja uzroka gubitka podataka.

Ostale ključne odredbe

Okidač događaja – gubitak ili šteta. *Cyber*-police obično se pokreću bilo događajem koji rezultira gubitkom podataka, bilo štetom koja proizlazi iz događaja koji je napravljen protiv osiguranika (ili napravljen protiv osiguranika i prijavljen osiguratelju) u razdoblju važenja police. Police kojima je okidač štetni događaj obično su restriktivnije u odnosu na događaje koji mogu potaknuti pokriće. Osim toga, vremenski opseg rezultirajućega zahtjeva u odnosu na gubitak može ograničiti ili spriječiti dostupnost pokrića. Iz toga razloga, tip police kojoj je okidač gubitak preferirani je izbor, iako to može biti skuplji izbor.

Okidač događaja – obrana. U nekim *cyber*-policama obveza obrane pokreće nadležno tijelo koje zahtijeva tužbu ili pisani zahtjev protiv osiguranika. Ova definicija može spriječiti obranu od zahtjeva koji sazrijevaju u parnici ili pisanome zahtjevu (u kojemu može biti potrošena većina troškova obrane na određenu stvar). U nekim *cyber*-policama ograničenje na tijelo ne odnosi se na vladine mjere (kao što su istraživanja).

Obrana – izbor branitelja. U nekim *cyber*-policama troškovi obrane pokriveni su samo u mjeri u kojoj je osiguranicima omogućen odabir iz osiguratelјeva popisa ponuđenih odvjetničkih društava. Ako osiguranik odabere drugu tvrtku, troškovi obrane vrlo vjerojatno neće biti pokriveni. S obzirom na znatne troškove i vjerojatnost da će biti povezan sa značajnim povredama podataka (koji bi mogli prelaziti limite police), osiguranik bi trebao imati veći doprinos u izboru savjetnika. Prema tome, poželjno je tražiti uravnoteženiji izbor savjetnika (npr. osiguranik i osiguratelj međusobno će se

dogovoriti o branitelju, a ako se ne mogu dogovoriti, osiguranik će izabrati branitelja za kojeg je osiguratelj dužan isplatiti iznos do, primjerice, definirane cijene sata).

Retroaktivna pokrivenost. *Cyber*-police često sadržavaju *povratni datum*. Gubitci koji proizlaze iz događaja prije retroaktivnoga datuma neće biti pokriveni. Osiguratelji često namještaju povratni datum na datum početka pokrića, iako osiguranik možda može pregovarati s povratnim datumom dalje u prošlost.

Radnje i propusti trećih osoba. Djela i propusti trećih osoba često ne mogu biti izričito pokriveni ili čak mogu biti isključeni iz *cyber*-polica. Primjerice, ako se tvrtka koristi uslugama dobavljača treće strane za održavanje svojih povjerljivih podataka o zaposlenicima ili pretplatnicima u *cloudu*, a prodavatelj doživljava povredu podataka, tvrtka može biti tužena od strane svojih pretplatnika ili zaposlenika, a da nema pokriće za taj događaj. *Cyber*-polica pruža pokriće za povrede podataka koje vode trećim osobama dokle god postoji pisani sporazum između osiguranika i prodavatelja o pružanju takve usluge. Ako se organizacija oslanja na treće strane kod zadržavanja bilo kojih od svojih povjerljivih podataka pretplatnika ili zaposlenika, treba nastojati imati izričito pokriće za povredu podataka koje vodi trećim osobama.

Pokrivenost za nekodirane uređaje. Mnoge *cyber*-police uključuju pokriće za podatke izgubljene iz nekodiranih uređaja.

Pokriće za poduzeća i druge subjekta. *Cyber*-police često definiraju kako su pokrivene osobe, za potrebe odgovornosti, samo fizičke osobe – konkretna ljudska bića, za razliku od pravnih osoba koje mogu biti javne ili privatne organizacije ili osobe. Međutim, osobe pogođene povredom podataka mogu uključivati korporacije i druge poslovne subjekte. Tvrtke trebaju tražiti takva pokrića koja na odgovarajući način definiraju opseg subjekata potencijalno pogođenih povredom podataka.

Teritorij pokrivenosti police. Čak i ako tvrtka ne posluje izvan države, njezini zaposlenici tijekom putovanja u inozemstvo mogu izgubiti (ili im mogu biti ukradeni) prijenosno računalo, mobilni uređaj i druge elektroničke uređaje koji sadržavaju povjerljive informacije. Mnoge *cyber*-police ograničavaju pokrivenost na određenome teritoriju država. Organizacije trebaju osigurati da njihove *cyber*-police osiguravaju pokrivenost čak i ako se gubitak ili krađa povjerljivih informacija događa izvan teritorija domicilne države.

Povrede koje se ne odnose na elektroničke podatke. Neke police *cyber*-odgovornosti ograničavaju pokriće gubitka ili krađe elektroničkih podataka. Međutim, mnoge povrede pojavljuju se kao posljedica gubitka ili krađe papira (ili drugih neelektričnih) zapisa. Najbolji je način djelovanja odabrati policu koja pokriva elektroničke i neelektroničke podatke.

Lokacija sigurnosnih propusta. Pokriće je u nekim *cyber*-policama ograničeno na fizičku krađu podataka u prostorijama organizacije. To bi moglo biti problematično u brojnim situacijama, uključujući i krađu prijenosnoga računala, mobilnih uređaja ili vanjskoga diska iz zračne luke ili doma zaposlenika. Pojedine police ograničavaju pokriće za povredu podataka nastale krađom lozinke u situacijama u kojima se krađa događa neelektričnim sredstvima.

Isključenje za generalizirana djela ili propuste. Neke *cyber*-police uključuju pokriće za gubitke po (i) nedostatcima u sigurnosti kojih je osiguranik bio svjestan prije početka pokrića; (ii) osiguranik je propustio poduzeti razumne korake za projektiranje, održavanje i nadogradnje svoje sigurnosti; i (iii) određeni neuspjesi sigurnosnih računalnih programa.

Isključenje za djela terorizma ili rata. Nejasno je u kojoj se mjeri osiguratelji oslanjaju na ovakav zajednički tip isključenosti kada je proboj podataka rezultat organiziranoga napada stranoga naroda ili neprijateljske organizacije.

Tablica 3. Pregled pokrića koja nude neki od većih osiguratelja

POKRIĆE	**OSIGURATELJ**					
IMOVINA I KRAĐA	**ACE**	**AIG**	**CHUBB**	**CNA**	**ST. PAUL TRAVELERS**	**ZURICH**
Maksimalni limit (u milijunima USD)	**15**	**25**[a]	**25**	**10**[b]	**N/A**[c]	**7,5**
Uništavanje podataka ili softvera	✔	✔	✔	✔	✔[c]	✔
Oporavak od virusa i drugoga malicioznog koda		✔	✔	✔	✔[c]	✔
Prekid poslovanja	✔	✔	✔	✔	✔[c]	✔
Uskraćivanje usluge	✔	✔	✔	✔		✔
Krađa podataka		✔	✔	✔		✔
Cyber-iznuda	✔	✔	✔	✔		✔
Gubitci zbog terorističkoga djelovanja	✔	✔	✔	✔	✔[c]	✔
ODGOVORNOST						
Maksimalni limit (u milijunima USD)	**25**	**25**[a]	**50**	**10**[b]	**25**	**7,5**
Odgovornost mrežne sigurnosti	✔	✔	✔	✔	✔	✔
Povrede sadržaja/elektroničkih medija	✔	✔	✔	✔	✔	✔
Izjava/povreda obveze povjerljivosti	✔	✔	✔	✔	✔	✔

Izvor: Bear, Parkinson, 2007.

a) tvrtka će pomoći u postavljanju većih limita do 75 milijuna USD
b) tvrtka nudi granice do 20 milijuna USD na vrlo odabranoj bazi
c) nudi neka *cyber*-pokrića prvih strana kao dio tradicionalne politike vlasništva, ne kao specijalizirane police

6.4. INICIJATIVE

Kako bi potaknula upotrebu proizvoda *cyber*-osiguranja i smanjila *cyber*-rizike, Vlada Velike Britanije ponudila je rješenje za problem standardizacije procjene rizika uz pomoć sheme Cyber Essentials. Shemu je razvila vlada i industrija s ciljem ispunjenja dviju funkcija. U prvome redu ona daje jasne smjernice o osnovnim kontrolama koje organizacije trebaju provesti kako bi se smanjila opasnost od *cyber*-prijetnji, što je učinjeno kroz 10 preporuka, odnosno koraka do *cyber*-sigurnosti. Druga je funkcija da kroz okvir za osiguranje nudi mehanizam kojim će organizacije svojim klijentima, investitorima, osiguratelјima i drugim zainteresiranima pokazati kako su poduzeli bitne mjere opreza. Vlada Velike Britanije smatra da provedba ovih mjera može bitno smanjiti ranjivost organizacije. Naravno, to nije finalno rješenje koje će ukloniti sve rizike *cyber*-sigurnosti. Primjerice, nije namijenjeno za rješavanje naprednih, sofisticiranih *cyber*-napada, za koje će organizacije koje se suočavaju s tim prijetnjama ipak morati provesti dodatne mjere kao dio njihove sigurnosne strategije. Ono što Cyber Essentials čini jest definiranje fokusiranoga skupa kontrola koji će osigurati troškovno učinkovitu, osnovnu *cyber*-sigurnost za organizacije svih veličina (UK Government, 2014).

Britanska vlada *cyber*-napade, uz terorističke prijetnje, smatra jednim od najvećih rizika za nacionalnu sigurnost. Stoga je uvela niz promjena koje bi trebale dovesti do sprečavanja *cyber*-napada, uključujući (ABI, 2015):

- Cyber Essentials – osnovni paket *cyber*-sigurnosne zaštite ponuđen organizacijama kako bi se zaštitile od najčešćih *cyber*-napada, kao što je prethodno objašnjeno;
- osnivanje Nacionalne jedinice za *cyber*-kriminal u okviru Nacionalne agencije za kriminal
- partnerstvo za razmjenu *cyber*-informacija – kako bi se omogućila razmjena informacija o *cyber*-prijetnjama između vlade i industrije
- jedinstveni sustav izvješćivanja *cyber*-incidenata
- novi Cyber Incident Response program koji bi trebao pomoći organizacijama u oporavku od *cyber*-napada
- mrežu centara izvrsnosti za Cyber Security Research u britanskim sveučilištima, kako bi se osiguralo pouzdano znanstveno istraživanje.

6.5. TRŽIŠTE *CYBER*-OSIGURANJA U REPUBLICI HRVATSKOJ

Osiguravajuća društva na hrvatskome tržištu osiguranja u svojemu portfelju usluga ne nude posebna *cyber*-osiguranja, iako je prema dostupnim podatcima o objavljenim incidentima očito da postoji potreba za ovim oblikom osiguranja. Stoga je nužno potrebno da se poduzeća maksimalno proaktivno posvete rješavanju problema *cyber*-sigurnosti, a ako to nisu sami u mogućnosti učiniti, trebaju zatražiti pomoć od specijaliziranih tvrtki za sigurnost. Hrvatski stručnjaci za sigurnost i forenziku među najboljima su u Europi (Ivezić, 2014), a njihovo je znanje potrebno iskoristiti kako bi se povećala zaštita od *cyber*-prijetnji. Osim toga, zapošljavanje sigurnosnih stručnjaka i njihovih tvrtki pri razvoju i izradi sigurnosnoga profila tvrtke kojoj je potrebno osiguranje, sigurno će ubrzati zasad nedovoljno razvijeno tržište *cyber*-osiguranja u Hrvatskoj. Primjeri takvih partnerstva između tvrtki za sigurnost i osiguravajućih društava već postoje i na taj se način omogućuje prijenos rizika. *Cyber*-osiguranje nije zamjena za uspostavljanje i održavanje sigurnoga okruženja. Međutim, *cyber*-osiguranje možda je ono što je potrebno kako bi se izbjegao ili smanjio utjecaj napada (Iasiello, 2015).

7. ZAKLJUČAK I PREPORUKE

U cilju smanjenja korporativnoga rizika današnje moderno poslovanje zahtijeva od tvrtki proaktivan pristup problemu *cyber*-sigurnosti. To posljedično znači proporcionalno veće ulaganje u samu sigurnosnu infrastrukturu, a time povećava njihove šanse za otkrivanje potencijalne prijetnje. Istodobno, poželjno je da tvrtka analizira trenutačno važeću policu osiguranja od odgovornosti, njezin obuhvat, te da napravi procjenu izloženosti *cyber*-opasnosti. Konačno, menadžeri trebaju odlučiti hoće li uložiti u neki oblik *cyber*-sigurnosti. Povećanjem razine korporativne sigurnosti, zajedno s dodatnom zaštitom u obliku police *cyber*-osiguranja, podići će se razina konkurentnosti tvrtke, a time će ona postati atraktivna za investitore.

Hrvatsko tržište osiguranja nerazvijeno je u policama *cyber*-osiguranja, te u tome segmentu leži velik potencijal za razvoj. Kako bi zadovoljili potrebe svojih klijenata i smanjili gubitke zbog *cyber*-napada, osiguravajuća društva u

Hrvatskoj morat će slijediti primjer razvijenih tržišta osiguranja i ponuditi usluge *cyber*-osiguranja. To je nužno kako bi se smanjila opasnost od *cyber*-prijetnji te smanjili gubitci od *cyber*-napada. Uključivanjem profesionalnih tvrtki i stručnjaka iz područja sigurnosti, otvara se novo područje poslovanja, koje je financijski atraktivno, a u budućnosti će zasigurno rasti potreba za stručnjacima toga profila. Uz državne poticaje i angažman postojećih stručnjaka, kako je to prikazano na primjeru Velike Britanije, moguće je stvoriti kvalitetan izvozni proizvod, kako u segmentu sigurnosti, tako i u segmentu osiguranja.

LITERATURA

ABI – Association of British Insurers (2015). „Cyber Insurance". https://www.abi.org.uk/Insurance-and-savings/Products/Business-insurance/Cyber-risk-insurance (14. 9. 2015.).

Allen-Ebrahimian, B. (2015). „China's Web Users Find NYSE Shutdown Hilarious – With Chinese stocks nosediving, the halt to trading on America's major stock platform hits close to home", kreirano 8. 7. 2015. http://foreignpolicy.com/category/tea-leaf-nation/ (14. 9. 2015.).

Allianz Global Corporate & Security (2015). „A Guide to Cyber Risk, Managing the Impact of Increasing Interconnectivity", Editor: Greg Dobie (greg.dobie@allianz.com). http://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf (13. 9. 2015.).

Armerding, T. (2015). „Why criminals pick on small business". http://www.csoonline.com/article/2866911/cyber-attacks-espionage/why-criminals-pick-on-small-business.html (13. 9. 2015.).

Ashwini, A. (2014). „How does one perform a DDoS attack? ". https://www.quora.com/How-does-one-perform-a-DDoS-attack (15. 9. 2015.).

Baer, W.S., Parkinson, A. (2007). „Cyberinsurance in IT Security Management", IEEE Security & Privacy, vol. 5, no. 3, pp. 50-56, May/June 2007, doi:10.1109/MSP.2007.57

BBC (2015a). „China's President Xi Jinping begins US state visit in Seattle". http://www.bbc.com/news/world-asia-china-34322054 (20. 9. 2015.).

BBC (2015b). „Chinese hackers arrested after US request". http://www.bbc.com/news/technology-34504317 (15. 10. 2015.).

CNN Wire Service (2015). „Latest: Trading resumes on New York Stock Exchange after three-hour suspension". http://fox6now.com/2015/07/08/new-york-stock-exchange-suspends-trading/ (14. 9. 2015.).

CROForum (2014). „Cyber Resilience – The cyber risk challenge and the role of insurance", KPMG Advisory N.V. http://www.munichre.com/site/corporate/get/documents_E-558890045/mr/assetpool.shared/Documents/0_Corporate%20Website/1_The%20Group/Emerging-Risks/CRO-Forum-cyber-risk-paper-2014-12.pdf (13. 9. 2015.).

D'Mello, G. (2014). „Google reels under DDoS attack". http://www.dnaindia.com/scitech/report-google-reels-under-ddos-attack-2040211 (14. 9. 2015.).

Drozhzhin, A. (2015). „Russian-speaking cyber spies exploit satellites". https://blog.kaspersky.com/turla-apt-exploiting-satellites/9771/ (13. 9. 2015.).

European Cybercrime Centre (EC3) – Europol (2014). „The Internet Organised Crime Threat Assesment (iOCTA) ". file:///Users/Air/Downloads/europol_iocta_web.pdf (15. 9. 2015.).

Goldman, J. (2015). „CareFirst BlueCross BlueShield Data Breach Impacts 1.1 Million People". http://www.esecurityplanet.com/network-security/carefirst-bluecross-blueshield-data-breach-impacts-1.1-million-people.html (13. 9. 2015.).

Greenberg, A. (2015). „Hacking Team Breach Shows a Global Spying Firm Run Amok". http://www.wired.com/2015/07/hacking-team-breach-shows-global-spying-firm-run-amok/ (13. 9. 2015.).

Hanover Research (2014). „Cyber Insurance Survey -Prepared for ISO". http://www.verisk.com/downloads/emerging-issues/cyber-survey.pdf (15. 9. 2015.).

Iasiello, E. (2015). „Cyber Security Tool, Not a Solution". http://darkmatters.norsecorp.com/2015/09/28/cyber-insurance-is-another-cyber-security-tool-not-a-solution/ (28. 9. 2015.).

Ivezić, B., (2014). „HNB: Sumnja se da su cyber kriminalci Hrvatima ukrali 1,8 milijuna kuna", Poslovni dnevnik. http://www.poslovni.hr/tehnologija/manje-napada-cyber-kriminalaca-ali-opasnost-i-dalje-postoji-274466 (13. 9. 2015.).

Khandelwal, S. (2015). „Tox' Offers Free build-your-own Ransomware Malware Toolkit". http://thehackernews.com/2015/05/ransomware-creator.html (13. 9. 2015.).

Kuranda, S. (2015). „Security Vendor Kaspersky Lab Is Latest Cyberattack Target". http://www.crn.com/news/security/300077098/security-vendor-kaspersky-lab-is-latest-cyberattack-target.htm (13. 9. 2015.).

Maloof, F. E, (2014). „Dragonfly' virus strikes U.S. power plants- Cyberattacks seek to control or even sabotage America's energy grid". http://www.wnd.com/2014/07/dragonfly-virus-strikes-u-s-power-plants/ (13. 9. 2015.).

Marsh (2015). „UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk", HM Government, Marsh Ltd. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf (14. 9. 2015.).

Matthews, T. (2015). „Incapsula Survey : What DDoS Attacks Really Cost Businesses". http://lp.incapsula.com/rs/incapsulainc/images/eBook%20-%20DDoS%20Impact%20Survey.pdf (13. 9. 2015.).

MCNeal, G. S. (2015). „Health Insurer Anthem Struck By Massive Data Breach", kreirano 4. 2. 2015. http://www.forbes.com/sites/gregorymcneal/2015/02/04/massive-data-breach-at-health-insurer-anthem-reveals-social-security-numbers-and-more/ (13. 9. 2015.).

Meek, A, (2015). „DDoS attacks are getting much more powerful and the Pentagon is scrambling for solutions", kreirano 31. 8. 2015. http://bgr.com/2015/08/31/ddos-attacks-report-2015-trends/ (13. 9. 2015.).

Menn, J. (2015). „U.S. tried Stuxnet-style campaign against North Korea but failed – sources". http://www.reuters.com/article/2015/05/29/us-usa-northkorea-stuxnet-idUSKBN0OE2DM20150529 (13. 9. 2015.).

Mueller, R., S. (2012). FBI Director speech on RSA Cyber Security Conference, San Francisco, CA. https://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies (15. 9. 2015.).

OpenDNS (2014). „Prevention is No Match for Persistence: Rethinking Cyber Security in the Age of Relentless Attacks". http://info.opendns.com/rs/opendns/images/WP-Rethinking-Cyber-Security.pdf (15. 9. 2015.).

OPM (2015). Information about OPM Cybersecurity Incidents. https://www.opm.gov/cybersecurity (13. 9. 2015.).

Pearson, N. (2014). „A larger problem: financial and reputational risks", Computer Fraud & Security, 12–13.

Portal Svijet sigurnosti (2015). „U posljednja 72 sata Hrvatska je meta intenzivnih hakerskih napada". http://www.svijetsigurnosti.com/blogs/5433-u-posljednja-72-sata-hrvatska-je-meta-intenzivnih-hakerskih-napada (13. 9. 2015.).

PR Newswire (2015). „Cyber Insurance Market Growing Rapidly Inspite Of Risks Says A New 2015 Research Report". http://www.thestreet.com/story/13318325/1/cyber-insurance-market-growing-rapidly-inspite-of-risks-says-a-new-2015-research-report.html (15. 9. 2015.).

PwC (2014). „Information Security Breaches Survey 2014 | technical report", The Department for Business, Innovation and Skills , conducted by PwC, in association with Infosecurity Europe & Reed Exhibitions, HM Government. http://www.pwc.co.uk/assets/pdf/cyber-security-2014-technical-report.pdf (14. 9. 2015.).

PwC (2015). „Cyber insurance market set to reach $7.5 billion by 2020 – PwC report". kreirano 14.09.2015, http://pwc.blogs.com/press_room/2015/09/cyber-insurance-market-set-to-reach-75-billion-by-2020-pwc-report.html (14. 9. 2015.).

Raptis, S. (2015). „Cyber Risk Insurance Policies: What You Need to Know". https://www.manatt.com/health-law/Cyber-Risk-Insurance-Policies-What-You-Need.aspx (15. 9. 2015.).

Reuters (2015a). U.S., „Chinese officials meet on cyber security issues: White House". http://news.yahoo.com/u-chinese-officials-meet-cyber-security-issues-white-005330544.html?soc_src=mediacontentstory&soc_trk=ma (13. 9. 2015.).

Reuters (2015b). „Premera Blue Cross Says Data Breach Exposed Medical Data", kreirano 17.03.2015. http://www.nytimes.com/2015/03/18/business/premera-blue-cross-says-data-breach-exposed-medical-data.html?_r=0. (13. 9. 2015.).

Schrader, C. (2015). „2015 Small Business Cyber Security Threats". http://www.nationalcybersecurityinstitute.org/small-business/2015-small-business-cyber-security-threats/ (15. 9. 2015.).

SurfWatch Labs (2014). „Using Cyber Insurance and Cybercrime Data to Limit Your Business Risk", Surf Watch Cyber in Sight. http://www.cutoday.info/content/download/14326/109311/version/1/file/Cyber+Insurance+Data+to+Limit+Risk.pdf (14. 9. 2015.).

Symantec Security Response (2014). „Dragonfly: Western Energy Companies Under Sabotage Threat - Cyberespionage campaign stole information from targets and had the capability to launch sabotage operations". http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat (13. 9. 2015.).

UK Government (2014). „Cyber Essentials Scheme Summary", HM Government, Department for Business, Innovation and Skills and cabinet Office. https://www.gov.uk/government/publications/cyber-essentials-scheme-overview (14. 9. 2015.).

Verizon (2013). „2013 Data Breach Investigation Report (2013), A global study conducted by the Verizon RISK team with cooperation from: *number of companies*". http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf (13. 9. 2015.).

Westervelt, R. (2015). „Billion-Dollar Cyberheist Used Phishing, Malicious Attachments", kreirano 17.02.2015. http://www.crn.com/news/security/300075786/billion-dollar-cyberheist-used-phishing-malicious-attachments.htm (13. 9. 2015.).

Zetter, K. (2014). „An Unprecedented Look at Stuxnet, the World's First Digital Weapon", Crown Publishing, New York.

Danijel Bara

THE ROLE OF CYBER-INSURANCE IN MANAGING AND TRENSFERING CYBER SECURITY RISK

In today's age, which in many respects depends on information technology and electronic communications, businesses are becoming more exposed to various forms of cyber crime. Cyber criminal attacks and events such as cyber espionage, cyber warfare, cyber terrorism, cyber fraud and cyber bullying can have devastating consequences and a major impact on businesses, their employees, customers, the insured or a third person. Such actions can lead to intellectual property theft, compromising corporate strategy, embezzlement or manipulation of confidential and personal information, reducing the reputation of the brand and the business entity, and in some cases may even threaten the existence of the company. As cyber crime has a major impact on the organization, the problem of cyber security outgrow the IT department, which until recently only deal with cyber security, and has become one of the strategic risks over which the executive management must take ownership. This article explores the impact that cyber crime has on business, as well as proactive measures that can transfer the risks of cyber threats, in particular, it relates to cyber security as an additional tool for the transfer of risk. Lately, we have witnessed the rise of cyber crime in the Republic of Croatia and the article analyzes and Croatian cyber security market and proposes a model that aims to expand the supply of cyber security, because it is evident that there is a need. We hold it necessary to implement a proactive strategy for managing cyber risks to businesses, especially those with significant data and information assets or doing business over the Internet, to protect its infrastructure and ensure the viability of the market. If this is achieved, cyber security can be part of the overall business strategy of reducing risk.

Keywords: insurance, cyber insurance, cyber security, cyber crime, cyber risk, cyber insurance model