Zlatan Filipović

Bosna Reosiguranje d.d. Sarajevo

zlatan.filipovic@bosnare.ba

# CYBER RIZICI I OSIGURANJE

## NASTANAK I RAZVOJ DIGITALNOG SVIJETA

Elektronski uređaji, kao i prikupljanje i obrada podataka putem njih prisutni su dosta dugo, ali u današnjem smislu cyber rizici (ili kibernetski rizici) se nisu pojavili tako davno. Ili barem nisu predstavljali tako veliku opasnost.

Možda prva velika cyber prijetnja je bila tzv. Millenium bug, kada se pretpostavljalo da će zbog prelaska godine sa 1999. na 2000. doći do masovnog zatajenja računarske opreme, posebno procesne odnosno upravljačke opreme bilo koje vrste koja ima ugrađenu elektroniku i programe, te posljedičnih šteta usljed toga. Pretpostavka je bila da će računari koji su godinu prepoznavali po zadnja dva broja biti zbunjena ulaskom u novu godinu koja će biti označena kao „00“ (kalendarski gledano, 21. stoljeće je započelo 01.01.2001.). Srećom, straha je bilo puno više nego što ga je zaista trebalo biti, štete su bile ograničene i jedino su se veliki iznosi novca utrošili na poboljšanje opreme i programa i „rješavanje“ tog problema.

No, za implikacije cyber rizika potrebna je bila infrastruktura koja je nastala tek stvaranjem globalnih mreža za prijenos podataka, a za omasovljenje korištenja tih mreža neophodna je bila pojava dovoljno malih elektronskih uređaja, kako stacionarnih poput PC-ja koji su postojali i ranije, do laptopa, tableta i konačno pametnih telefona koji omogućavaju pristup podacima, obradu, kao i uticaj na druge uređaje i programe praktički s bilo koje lokacije na svijetu s koje postoji pristup mreži. Prvi pametni telefon je bio IBM-ov Angler inženjera Franka Canove, koji je prezentiran novembra 1992. Naravno, nije imao mnogo poveznica sa modernim uređajima. Niz proizvođača je od 2000. nadalje predstavilo brojne varijante takvih uređaja, u početku s tipkovnicama, preko onih s ekranima osjetljivim na dodir, a od januara 2007. s pojavom iPhonea pametni telefoni osjetljivi na dodir su postali masovno dostupni.[1]

[1] https://en.wikipedia.org/wiki/Smartphone#:~:text=The%20first%20commercially%20available%20device%20that%20could%20be,year%20at%20the%20COMDEX%20computer%20industry%20trade%20show.

Po nekim studijama, prosječan korisnik pametnog mobilnog telefona u SAD pogleda u njega 150 puta dnevno[2], a dotakne ga 2.617 puta dnevno.[3] Broj mobilnih aparata u svijetu je prešao 5 milijardi do 2019. godine[4].

Prednosti svekolike povezanosti su jako velike, te omogućavaju znatno lakšu komunikaciju, informiranje, nabavku, poslovanje s bankama, pa čak u nekim naprednijim zemljama i komunikaciju s državnim organima te dobijanje elektronske dokumentacije.

Naravno, digitalizacija svijeta ne staje samo na mobilnim telefonima, ona je općenita, i napreduje velikom brzinom, čak i kada je jasno da su brojna pitanja ostala otvorena. Omogućava upravljanje proizvodnim procesima i sa udaljenih lokacija ili uz korištenje umjetne inteligencije, daje perspektivu za upotrebu vozila koja sama sobom upravljaju, pomaže kod distribucije robe, omogućava razvoj bankarskih usluga kroz elektronsko bankarstvo, a omogućila je i pojavu tzv. kriptovaluta (1.110 njih[5], a broj im raste). I pojedine vlade razmatraju mogućnosti uključenja u njihovo izdavanje, te čak 80 centralnih banaka istražuje digitalne valute[6].

Praktički nema oblasti života u kojoj digitalizacija nema primjenu. I to na način kojim se u potpunosti mijenja način života i zatvaraju stari a otvaraju novi poslovi, nestaju stari a nastaju novi proizvodi ili nove usluge. Tako su nestaju razni fizički predmeti, neki mediji za pohranjivanje slike, zvuka i podataka, a sve teže možete nabaviti uređaje za njihovu reprodukciju. Televizori se još uvijek prodaju, ali kako možete programe gledati i na svom mobilnom telefonu, tabletu ili računaru, bilo prenosnom ili desk-topu, a nivo pozornosti koji pojedinac obraća na video sadržaj je sve manji i koncentracija sve kraća, pitanje je do kada će se televizor smatrati potrebnim kućanskim aparatom. A ovo je samo jedan mali, izdvojeni segment promjena u životu.

## OPASNOSTI DIGITALNOG SVIJETA

Uz ogromne mogućnosti koje digitalni svijet otvara, još su i veće opasnosti koje su došle s njim, a u svakom slučaju su još uvijek nedovoljno poznate.

Prekid lanca snabdijevanja u modernom, globaliziranom svijetu može dovesti do nestašica, velikih poslovnih gubitaka, pa i propasti pojedinih poduzeća. Iako se do sada prekidi snabdijevanja usljed ostvarenja cyber rizika nisu pokazali globalnim problemom, to lako mogu postati. A koliko velike posljedice mogu biti može se naslutiti iz posljedica prekida trgovanja kao i zatvaranja ne samo pojedinih firmi, već cijelih ekonomija usljed pandemije Covid-19. Troškovi prekida poslovanja

[2] https://www.textrequest.com/blog/americans-check-their-cell-phones-150-times-a-day/
[3] https://www.networkworld.com/article/3092446/smartphones/we-touch-our-phones-2617-times-a-day-says-study.html
[4] https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/
[5] https://venturebeat.com/2017/09/20/how-many-cryptocurrencies-does-the-world-need/
[6] Svet osiguranja, septembar 2020.

dosežu milijarde USD i predmet su velikih rasprava i sudskih sporova, ali u slučaju cyber napada većih razmjera očito je da bi scenarij kao i veličina šteta bili dosta slični.

Potencijalna šteta može nastati bilo kada i bilo gdje. Podjednako su ugroženi kako vlade pa čak i vojske, bez obzira na značajna sredstva, ljudstvo i tehniku kojima se štite, tako i proizvodni pogoni, transport, zdravstvo, edukacija, financijski sektor, razni drugi poslovi.

Segment koji je možda i najčešće pogođen cyber rizicima su baze podataka. Prema podacima organizacije Identity Theft Resource Center u 2017. je bilo oko 1.300 proboja u podatke, u kojima je 174 miliona podataka bilo izloženo. Godinu ranije zabilježeno je 1.093 poboja. Poslovni sektor je pretrpio najviše udara, 50,5%, zdravstveni sektor 28,3%, edukacioni sektor 8,8%, vlada/vojni sektor 5,3% od broja svih incidenata. Bankarski i financijski sektor 7,1%. Procjenjuje se da se podaci po osobi prodaju u prosjeku za 8 USD, a da mogu porasti u nekim specifičnim slučajevima na 15, pa i 30 USD[7]. Pri tome, broj dobijenih podataka, čak 91,4%, potiče iz upada u sisteme poslovnog sektora. Stoga je jasan financijski interes onih koji pokušavaju preoteti podatke. S druge strane, procijenjeni trošak po ukradenom ili izgubljenom zapisu za njihovu obnovu u prosjeku je u 2013. godini iznosio 188 USD[8].

Cyber rizici su još 2014. ušli među 10 najvećih globalnih poslovnih rizika, a u zadnje vrijeme se porede sa iznosima šteta koje nastanu usljed prirodnih katastrofa. Prema Allianz Risk Barometer Survey, anketi u kojoj je sudjelovalo 824 ispitanika iz 44 države, u 2016. su bili na 3. mjestu, a u Ujedinjenom Kraljevstvu na prvom[9]. Svjetska ekonomija gubi zbog cyber kriminala 445 milijardi USD godišnje[10].

## RAZVOJ CYBER OSIGURANJA

Prva pojava cyber osiguranja je bila u SAD 1996. U Kaliforniji su 2003. donijeti zakoni o obavještavanju o kršenju privatnosti (Privacy breach notice laws) kojima je povećana tražnja cyber osiguranja. Nakon toga, ukupno 47 od 50 država SAD je uvelo zakone o obaveznom obavještavanju o kršenju, te je zakonodavstvo tako postalo glavni pokretač razvoja ovog osiguranja. 2014. preko 60 društava je preuzimalo cyber rizike u osiguranje, s premijom od preko 1 milijarde USD.

Od 1995. donošenjem Direktive EU o zaštiti podataka, počinje razvoj u Europi, a zaštita podataka ustanovljena kao pravo građana EU. Sredinom 2000. povećana zavisnost od infromacione tehnologije i veliki hakerski skandali su doveli do povećane tražnje cyber osiguranja. EU je 2013. najavila Direktivu EU o cyber sigurnosti, kojom se određuju minimalne mjere zaštite u poslovanju.

[7] http://247wallst.com/technology-3/2017/12/23/2017-data-breach-total-nears-1300-easily-a-new-record/
[8] https://www.ponemon.org/local/upload/file/Cyber%20Insurance%20white%20paper%20FINAL%207.pdf
[9] http://www.agcs.allianz.com/assets/PDFs/Reports/AllianzRiskBarometer2016.pdf
[10] http://www.agcs.allianz.com/assets/PDFs/Reports/AllianzRiskBarometer2016.pdf

2013./2014. društva za osiguranje daju ponude na širem tržištu, a u Londonu postoji 25-30 tržišta za ovo osiguranje. 2015. se očekivala primjena reforme zakonodavstva o zaštiti podataka, ali je to pomaknuto za kasnije[11].

Procjene su da tržište cyber osiguranja generira 700 miliona EUR premije, a da će u 2018. godini dosegnuti 800 miliona EUR[12]. Svježije podatke nismo uspjeli pronaći, bez obzira na sve veći značaj cyber osiguranja.

Donošenjem strožijih zakona o zaštiti ličnih podataka, trošak rješavanja cyber upada je povećan, kroz troškove obavještavanja vlasti unutar 72 sata, klijenata, troškove odnosa sa javnošću i pravnih troškova. 2016. je donijeta Direktiva o sigurnosti mreža i informacija kojom je uvedena obaveza prijavljivanja vlastima ozbiljnih cyber incidenata, kao i obaveza društava da primijene odgovarajuće mjere cyber zaštite. U Europi je 2018. na snagu stupila European Global Data Protection Regulation, odredba donijeta još 2016. Ukoliko bi neko društvo propustilo da ispuni odredbe ove regulative, može biti kažnjeno sa 2% do 4% njihovog globalnog prihoda, zavisno od vrste aktivnosti i uz primjenu monetarnih ograničenja (maksimum od 20 miliona EUR). Donošenje ove regulative je doprinijelo daljnjem ubrzanom rast cyber osiguranja[13] u EU.

## PRILIKE ZA OSIGURANJE

U situaciji kada premije osiguranja padaju u uobičajenim vrstama osiguranja, mnogi razmišljaju da bi okretanje osiguranju cyber rizika bila dobra orijentacija i da bi pružila mogućnost za povećanje premijskog prihoda. U periodu od 2012. do 2015. premija je porasla sa 1 milijarde USD na 2 milijarde USD, a očekuje se utrostručenje premije do 2020.[14], a po nekim procjenama skok na 20 milijardi USD do 2025. godine[15]. Tržište je od 2019. krenulo putem „otvrđavanja“ koje podrazumijeva i rast premija, odnosno premijskih stopa. Zbog pandemije Covida-19 taj proces poskupljenja osiguranja i reosiguranja se nastavlja i kroz 2020. i sasvim sigurno će se nastaviti i kroz 2021., uključujući i premije cyber osiguranja.

Bez dužeg iskustva u osiguranju cyber rizika i preciznijih statistika nemoguće je reći kakav efekt tako uvećana premija može imati na rezultate poslovanja pojedinih društava ili općenito, na statistike pojedinih tržišta. Poredeći sa ukupnim ekonomskim štetama (445 milijardi USD), ako

[11] www.guycarp.com/.../AheadoftheCurve-UnderstandingEmergingRisks.pdf
[12] www.guycarp.com/.../AheadoftheCurve-UnderstandingEmergingRisks.pdf
[13] http://www.aon.com/inpoint/bin/pdfs/white-papers/Cyber.pdf
[14] https://www.darkreading.com/operations/average-breach-falls-below-cyber-insurance-policy-deductible-study-shows/d/d-id/1324652
[15] http://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf

ništa drugo treba ukazati na oprez kod preuzimanja ovakvih rizika, jer je izloženost očito vrlo visoka.

Stopa osiguranih društava puno je veća kod imovinskih osiguranja, npr. od požara (59%), iako je vjerojatnoća ostvarenja događaja požara manja od vjerojatnoće ostvarenja cyber napada. Samo nekih 15% društava osigurava svoju informatičku aktivu[16].

## PROSJEČNI TROŠKOVI CYBER NAPADA U SAD I U SVIJETU

Društva u SAD po nekim studijama su izložena većem riziku financijskih gubitaka preko 1 milion USD usljed cyber kriminala. 7% društava u SAD je izgubilo 1 milion USD ili više, dok je na svjetskom nivou taj postotak 3%. Potom, 19% organizacija u SAD su izgubile između 50.000 USD i 1 miliona USD, naprema 8% organizacija na svjetskom nivou. Najveći vanjski trošak po društva koja pretrpe cyber napad je krađa informacija, a troškovi vezani uz poremećeno poslovanje ili izgubljenu produktivnost su drugi najveći vanjski trošak. Tu su kazne, sudski postupci, utrživost ukradene intelektualne imovine itd. Rješavanje problema nastalih cyber napadima, ukoliko nije brzo riješeno, dovodi do povećanja troškova. Prosječno vrijeme za rješavanje cyber napada bilo 32 dana. Prosječni trošak društava iz SAD koja su bila uključena u godišnju studiju iz 2013. Ponemon Instituta je prelazio 1 milion USD. Godinu ranije studija je pokazivala period od 24 dana potrebna da se riješe problemi cyber napada, a prosječni trošak je bio 591.780 USD[17].

Studija Ponemon Instituta iz 2017.[18], Cost of Data Breach Study (sponzorirana od strane IBM-a, te stoga dostupna na toj stranici), daje prikaz do kakvih je promjena došlo. Na uzorku od 419 kompanija iz 13 zemalja, prosječni trošak je dosegao 3,62 miliona USD, što je ipak nekih 10% manje u odnosu na prethodnu godinu. Prosječan trošak po izgubljenom podatku je bio 141 USD, a šanse za ponovni napad su bile 27,7% u periodu od naredne dvije godine.

## NEKI OD VELIKIH CYBER NAPADA

Brošura Aon-a Global Cyber Market Overview[19] i neki drugi izvori daju pregled većih cyber napada:

[16] http://www.aon.com/attachments/risk-services/cyber/2017-Global-Cyber-Risk-Transfer-Report-Final.pdf
[17] https://www.iii.org/sites/default/files/docs/pdf/paper_cyberrisk_2014.pdf
[18] https://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03130wwen/security-ibm-security-services-se-research-report-sel03130wwen-20180122.pdf
[19] http://www.aon.com/inpoint/bin/pdfs/white-papers/Cyber.pdf

Hunter Water - Negdje 2000. nezadovoljni radnik upao je u sistem vodovoda i oslobodio 264.000 litara otpadnih voda na različitim lokacijama, u periodu od 3 mjeseca. Napad je doveo do značajnog onečišćenja okoline.

Los Angeles City Hall – 2006. Uprava grada je bila odgovorna zbog prekida poslovanja jer su hakeri ušli u sistem i na nekoliko dana zakrčili 4 glavne raskrsnice.

TJX (maloprodaja) – 2006., 2007., 90 miliona USD troškova, ukradeni podaci o kreditnim i debitnim karticama klijenata.

Heartland (financijske usluge – procesori za plaćanje) – 2008., 2009., 110 miliona USD troška. Ukradeni podaci su uključivali i magnetne zapise učitane na magnetne trake kreditnih i debitnih kartica, koje su hakeri mogli onda duplirati na lažne kartice.

Lodz City Tram system – 2010. poljski tinejdžer je premostio daljinski upravljač TV-a te je njim upao u bežični sistem upravljanja skretnicama. Jedan tramvaj je zbog toga iskočio iz tračnica i udario u drugi, prouzrokovavši lakše povrede nekolicine putnika, što je prvi cyber napad koji je doveo do povreda.

2010. napadnut je razvojni nuklerani program Irana, kada je virus Stuxnet ubrzao 1/5 nuklearnih centrifuga i doveo do njihovog raspada. Nema procjene visine štete.

Saudi Aramico – 2012., hakeri su prouzrokovali uništavanje 30.000 desktop kompjutera i 2.000 servera, a informatički sistem kompanije je bio isključen 2 sedmice.

Zappos (internet prodaja) – 2012., 500 miliona USD troška zbog preuzimanja podataka o klijentima.

Adobe (tehnologija) – 2013., bez procjene troška. Ukradeni podaci o kreditnim i debitnim karticama 3,1 miliona klijenata, lozinke 33 miliona korisnika, kao i izvorni kod za razne pakete, uključujući i Adobe Photoshop.

Kompanija JP Morgan Chase (financijske usluge/bankarstvo) napadnuta je 2014. Iako nema iznosa štete, plan je napravljen da se godišnje na digitalnu sigurnost troši 250 miliona USD.

Ebay (internet trgovina) – napadnuti 2014., smanjili su planirani godišnji prihod za 200 miliona USD zbog napada.

Target (maloprodaja) – 2014., trošak incidenta 162 miliona USD, ukradeno 40 miliona podataka o kreditnim i debitnim karticama i lični podaci 70 miliona kupaca.

LOT – 2015. poljska aviokompanija je zbog hakiranja hardware-a koji izdaje planove leta morala otkazati desetak letova.

Kompanija Anthem (djelatnost: zdravstvo) je 2015. Imala štetu od 100 miliona USD zbog pristupa hakera ličnim informacijama.

Equifax (kreditni registar) je u cyber napadu 2017. imao preko 160 miliona kompromitiranih ličnih podataka. Napad je započeo u martu, ali se nisu oglašavali, a glavni napadi su bili u maju i junu mjesecu. Prvi izvještaj o obavještenjima je datiran 18.09.2017. Prvog dana po objavi napada, vrijednost dionica je pala 13%, a ukupno 25%, dok su u dvije tzv. klasne tužbe potrošači iz Kanade potraživali odštetu u visini od 450 milijardi USD, a iz SAD 70 milijardi USD[20]. Konačna šteta se zasigurno neće moći znati godinama. Osiguranje koje je Equifax ugovorio pokriva između 100 i 150 miliona USD[21].

2017. WannaCry ransomware je inficirao stotine hiljada računara, a napadači su tražili od žrtava iz više od 150 zemalja 300 miliona USD, plativo u bitcoinima.

Coincheck je 2018. objavio gubitak 534 miliona USD vrijednih bitcoina u hakerskom napadu[22]. Procjene su da je do sada u takvim napadima izgubljeno na milijarde USD. Neka društva su spremna osigurati takve napade do 25 miliona USD, neka pokrivaju samo krađe koje počine zaposlenici kompanija, ali ne i od trećih osoba, a neki pak samo kriptovalute na tzv. „hladnim novčanicima“, ali ne i online račune („vrući novčanici“).

U oktobru 2019. izveden je veliki cyber napad na web stranice kao i sisteme državnih organa, javnih insittucija, nevladinih organizacija, kao i privatnih firmi u Gruziji.[23]

U prvih pola godine 2020. je zabilježeno više cyber napada u odnosu na prvih pola godine 2019. (41.000 : 35.000).[24]

Viđenje javnosti je da dvije trećine ispitanika smatra da su korporacije odgovorne za cyber napade, kada se oni dese, a 62% ispitanika iz SAD smatra da vlada SAD treba biti odgovorna za zaštitu američkih poslova od cyber napada[25].

U SAD se i na saveznom nivou razmatra donošenje regulative u oblasti osiguranja kojom će se obuhvatiti sigurnost podataka specifičnih za industriju osiguranja.

[20] Global Reinsurance, 14.12.2017
[21] Osiguranje.hr, 09.10.2017
[22] Poslovni dnevnik, 02.02.2018.
[23] https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/
[24] https://www.darkreading.com/attacks-breaches/more-cyberattacks-in-the-first-half-of-2020-than-in-all-of-2019/d/d-id/1338926
[25] https://www.iii.org/sites/default/files/docs/pdf/paper_cyberrisk_2014.pdf

## ŠTA SE MOŽE OSIGURATI

Industrija osiguranja je sve manje podložna standardiziranju, čak i kada bi to bilo potpuno opravdano. Osiguranje cyber rizika, čini mi se, je takva oblast gdje bi značajan stepen standardizacije bio prednost, no i mišljenje da se za svakog klijenta treba napraviti ponuda koja mu odgovara je legitimno. No, za veliki broj društava koja ne spadaju u red velikih uglavnom će uvjeti osiguranja i isključenja biti zbunjujuća i ponude od strane nekoliko osiguravača teško uporedive. Postoje mišljenja da bi bilo pogrešno uvoditi standardizaciju u okolnostima nedovoljnog poznavanja rizika.

Privredna društva i vlade i njihove institucije u slučaju cyber napada su izložena sljedećim rizicima:

- Zakonska odgovornost
- Proboj kompjuterske sigurnosti
- Narušavanje privatnosti
- Cyber krađa
- Cyber špijunaža i industrijska špijunaža
- Cyber ucjene
- Cyber terorizam
- Gubitak prihoda
- Namirenje troškova
- Narušeni ugled
- Kontinuitet poslovanja/prekidi u lancu snabdijevanja
- Cyber prijetnje infrastrukturi[26]

Allianz upozorava da utjecaj prekida poslovanja prouzrokovan tehničkom greškom često bude podcijenjen u odnosu na cyber napade, a također i gubitak reputacije nakon cyber incidenta[27].

Iako općenito postoji vjerovanje da stariji informatički uređaji mogu biti ranjiviji od novijih, nažalost moderni svijet pokazuje i ružnu stranu velikih korporacija koje namjerno ažuriraju software za starije uređaje na način da ih usporavaju. I ovaj problem može utjecati na zatajenje ili lošiji rad starijih uređaja, makar oni bili potpuno funkcionalni. Uz to, dosta uređaja ima instalirani software koji se više ne podržava. Očito da moderni svijet prisiljava na kupovinu novih uređaja i novih software-a, te će svako za sebe morati donijeti odluku kako pristupiti rješavanju ovakvih problema.

[26] www.guycarp.com/.../AheadoftheCurve-UnderstandingEmergingRisks.pdf
[27] http://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf

Prema vrlo korisnoj brošuri A Guide to Cyber Risk[28] moguće je osiguranjem obuihvatiti sljedeće (a naravno, u zavisnosti od apetita za rizikom svakog pojedinog društva za osiguranje):

Pokriće za proboj privatnosti i podataka – Troškovi odbrane i štete za koje su odgovorni Osiguranik ili vanjski pružatelj usluga, a koji proistječu iz gubitka podataka.

Pokriće prekida poslovanja i troškova obnove – Gubitak poslovnog prihoda (i troškova obnove) prouzrokovanih ciljanim napadom na kompjuterski sistem društva.

Pokriće za odštetne zahtjeve na osnovu sigurnosti mreže – Troškovi odbrane i štete za koje je Osiguranik dogovoran, a koji proistječu iz ciljanog cyber napada.

Pokriće odgovornosti po odštetnim zahtjevima zbog medija – Troškovi odbrane i štete za koje je Osiguranik odgovoran, a koji proistječu iz publiciranja ili emitiranja sadržaja digitalnih medija.

Pokriće troškova nametnutih od strane regulatora – Troškovi odbrane zbog zahtjeva postavljenog od strane regulatora, a koji proizilazi iz gubitka podataka.

Pokriće kazni i penala od strane regulatora – Novčane kazne i penali koje nametnu regulatori (u mjeri u kojoj su osigurljivi) a koji proizilaze iz gubitka podataka.

Troškovi obavještavanja – U skladu sa zahtjevima po zakonu i od strane regulatora nakon gubitka podataka.

Troškovi odgovora – Naknade i troškovi za forenzičko istraživanje nakon gubitka podataka, identifikacija i prezervacija izgubljenih podataka, savjeti o zakonskim i regulatornim obavezama, određivanje obima obaveza naknade u ugovorima sa pružateljima usluga koji su treća strana, usluge kreditnog praćenja i druge akcije popravljanja situacije koje su neophodne nakon gubitka podataka.

Pokriće hakerske krađe – Naknada za ukradena sredstva usljed zlonamjerne aktivnosti treće strane.

Pokriće cyber ucjena – Naknada za rješenje stvarne prijetnje u pogledu kompromitiranja Osiguranikovih podataka ili sistema.

E-plaćanja – Troškovi odbrane, štete i ugovorni penali u pogledu kršenja standarda sigurnosti podataka industrije platnih kartica.

Pokriće za krizno komuniciranje – Troškovi odnosa s javnošću panela stručnjaka radi ublažavanja bilo kakvog negativnog publiciteta iz pokrivenog slučaja.

Pokriće konsultantskih usluga – Troškovi IT stručnjaka da bi se odredio iznos i obim štete pokrivene po ovoj polici.

[28] http://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf

Prekid poslovanja.

U pokrićima cyber osiguranja koja se zasebno prodaju, fizičko oštećenje uobičajeno nije pokriveno. Često je fizička šteta koja proizilazi iz cyber napada isključena i po imovinskom osiguranju, te na ovo treba obratiti pažnju.

Kod ovakvih pokrića je velika opasnost od kumuliranja rizika, a modele je teško napraviti.

No, postoje ipak scenariji koje je napravio Lloyd's skupa sa firmom Cyence pod nazivom „Counting the cost: Cyber exposure decoded“[29] koji ukazuju da prekid u pružanju usluga putem tzv. clouda može koštati od 4,6 milijardi USD za veliki događaj do 53,1 milijardu USD za ekstremno veliki događaj, a za masovni događaj ranjivosti softwarea raspon je od 9,7 milijardi USD za veliki događaj do 28,7 milijardi USD za ekstremno veliki događaj. Pri tome, scenariji ukazuju na nedostatak pokrića osiguranjem, gdje bi osigurane štete bile od 620 miliona USD do 8,1 milijardu USD za incident koji uključuje cloud, a od 762 miliona USD do 2,1 milijardu USD za masovni događaj ranjivosti softwarea[30].

No već sljedeći izvještaj Lloyd'sa, ovaj put u suradnji sa Air Worldwide („Cloud Down – The impacts on the US economy) procjenjuje da bi poslovi u SAD pretrpjeli 15 milijardi USD ekonomske štete (3 milijarde USD osigurane štete) ako bi jedan od vodećih pružatelja usluga clouda prestao raditi na tri do šest dana[31].

Također, na tržištu se javljaju i osiguranja direktora i zvaničnika (D&O), kojim se pokriva širok spektar odgovornosti direktora i zvaničnika jednog društva, uključujući i cyber rizike[32].

## RAZUMIJEVANJE RIZIKA I TEŠKOĆE KOD PRODAJE CYBER OSIGURANJA

Osiguranje cyber rizika iziskuje dobro razumijevanje rizika koji se preuzimaju. Stoga je preuzimanje kod cyber rizika možda i važnije od preuzimanja kod nekih drugih vrsta osiguranja. Stoga ne čudi da je u jednoj anketi nedostatak shvatanja izloženosti naveden kao najveća prepreka prodaji cyber pokrića[33]. Jedan od brokera je prodajni proces nazvao vođenjem bitke uzbrdo, sa informatičarima koji ne prihvataju mogućnost da njihovi sistemi mogu biti kompromitirani, dosta

[29] Global Reinsurance, 17.07.2017
[30] Asia Insurance Review, 18.07.2017
[31] Global Reinsurance, 25.01.2018
[32] https://www.iii.org/sites/default/files/docs/pdf/paper_cyberrisk_2014.pdf

[33] http://www.partnerre.com/assets/uploads/docs/cyber-survey-results.pdf

klijenata srednjeg nivoa odbijaju mogućnost da su izloženi, ili prema riziku imaju stav „nikad mi se to nije desilo“[34].

Značajan broj klijenata nije u mogućnosti dostaviti dodatnu dokumentaciju potrebnu za postupak preuzimanja, a dostupne aplikacije su previše kompliciranе za manje rizike[35].

Čini se da su brokeri značajan kanal za prodaju ovog osiguranja, te njihova specijalizacija u ovom smjeru može olakšati posao društvima za osiguranje.

Ipak, preporuka za društva za osiguranje koja su spremna dati veći kapacitet za cyber rizike je da uzmu u razmatranje kod pripreme proizvoda vanjske pružatelje usluga, definicije kompjuterskih sistema, kumule, mogućnosti odgovora osiguranika na proboj, kao i okidače za prekid poslovanja[36].

Stoga ne treba čuditi da je relativno mali broj društava za osiguranje spreman preuzimati cyber rizike.

[34] http://www.partnerre.com/assets/uploads/docs/cyber-survey-results.pdf
[35] http://www.partnerre.com/assets/uploads/docs/cyber-survey-results.pdf
[36] www.guycarp.com/.../AheadoftheCurve-UnderstandingEmergingRisks.pdf