UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

ZAVAROVANJE KIBERNETSKIH TVEGANJ KOT NOV PRODUKT NA SLOVENSKEM ZAVAROVALNEM TRGU

Ljubljana, julij 2016 BOJANA KIFNAR STRMČNIK

IZJAVA O AVTORSTVU

Spodaj podpisana Bojana Kifnar Strmčnik, študentka Ekonomske fakultete Univerze v Ljubljani, avtorica predloženega dela z naslovom Zavarovanje kibernetskih tveganj kot nov produkt na slovenskem zavarovalnem trgu, pripravljenega v sodelovanju s svetovalcem izr. prof. dr. Alešem Ahčanom

IZJAVLJAM

1. da sem predloženo delo pripravila samostojno;

2. da je tiskana oblika predloženega dela istovetna njegovi elektronski obliki;

3. da je besedilo predloženega dela jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem poskrbela, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam oziroma navajam v besedilu, citirana oziroma povzeta v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani;

4. da se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku Republike Slovenije;

5. da se zavedam posledic, ki bi jih na osnovi predloženega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom;

6. da sem pridobila vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označila;

7. da sem pri pripravi predloženega dela ravnala v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobila soglasje etične komisije;

8. da soglašam, da se elektronska oblika predloženega dela uporabi za preverjanje podobnosti vsebine z drugimi deli s programsko opremo za preverjanje podobnosti vsebine, ki je povezana s študijskim informacijskim sistemom članice;

9. da na Univerzo v Ljubljani neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve predloženega dela v elektronski obliki, pravico reproduciranja ter pravico dajanja predloženega dela na voljo javnosti na svetovnem spletu preko Repozitorija Univerze v Ljubljani;

10. da hkrati z objavo predloženega dela dovoljujem objavo svojih osebnih podatkov, ki so navedeni v njem in v tej izjavi.

V Ljubljani, dne _____ Podpis študentke:_____

KAZALO

UVOD **1**
1 KIBERNETSKE NEVARNOSTI **4**
1.1 Opredelitev kibernetskih nevarnosti 4
1.2 Kategorije kibernetskih nevarnosti glede na vir izvora 6
1.3 Najodmevnejši primeri varnostnih incidentov 12
1.4 Sistemi varnostne zaščite informacijskih sistemov 17
2 TVEGANJA, POVEZANA S KIBERNETSKIMI NEVARNOSTMI **24**
2.1 Kibernetske nevarnosti kot varnostno tveganje in povezava z operativnim tveganjem 24
2.2 Zavedanje o obstoju kibernetskih nevarnostih in varnostnega tveganja, ki jih prinašajo 26
2.3 Ekonomske razsežnosti in stroškovni vidik varnostnih incidentov 40
3 OBVLADOVANJE TVEGANJ, POVEZANIH S KIBERNETSKIMI NEVARNOSTMI **49**
3.1 Razvoj ustrezne strategije obvladovanja varnostnih tveganj 49
3.2 Možni načini za prenos tveganja na druge subjekte 51
4 ZAVAROVANJE KIBERNETSKIH TVEGANJ V SVETU **55**
4.1 Razvoj zavarovalnega/pozavarovalnega trga in produkta zavarovanja kibernetskih nevarnosti v svetu 55
4.2 Značilnosti in zavarovaljivost kibernetskih tveganj 59
4.2.1 Kriteriji zavarovaljivosti in značilnosti kibernetskih tveganj 59
4.2.2 Načini za izboljšanje stopnje zavarovaljivosti kibernetskih tveganj 63
4.3 Zavarovalni produkti za kritje kibernetskih tveganj 65
4.3.1 Produkti za zavarovanje kibernetskih tveganj kot samostojno kritje 65
4.3.2 Obstoječi produkti drugih zavarovalnih vrst in potencialno kritje / izključitev kibernetskih tveganj 67
4.4 Izzivi zavarovalnic/pozavarovalnic za prihodnost 69
5 SWOT ANALIZA Z VIDIKA VPELJAVE ZAVAROVANJA KIBERNETSKIH TVEGANJ NA SLOVENSKI TRG **70**
SKLEP **75**
LITERATURA IN VIRI **77**

KAZALO TABEL

Tabela 1: Izbrane nevarnosti kibernetskih rizikov po viru izvora za leti 2014 in 2015 s prikazom trenda glede na število napadov 11
Tabela 2: Gibanje povprečne ocene globalnih nevarnosti v letih 2014–2016 27
Tabela 3: Kibernetske nevarnosti po doseženem mestu glede na pomembnost za družbe z deleži udeležencev v letih 2014–2016 39

Tabela 4: Kibernetske nevarnosti po doseženem mestu glede na pomembnost za družbe in deleži udeležencev v letih 2014–2016 39
Tabela 5: Deleži stroška po vrsti aktivnosti v deležu od BDP 43
Tabela 6: Obseg kosmate zavarovalne premije po skupinah zavarovanj v letu 2014 v milijardah USD 56
Tabela 7: Kritja po tradicionalnih produktih zavarovanja in možna manjkajoča kritja vezana na kibernetske nevarnosti 68
Tabela 8: SWOT matrika 71

KAZALO SLIK

Slika 1: Število varnostnih incidentov po vrsti incidenta v letih 2008–2015 11
Slika 2: Zneski skupne škode in odškodnina zavarovalnic pri izbranih primerih varnostnih incidentov (v milijonih USD) 15
Slika 3: Število obravnavanih varnostnih incidentov v SI-CERT v letih 2008–2015 16
Slika 4: Prikaz primera notranjega informacijskega sistema družbe z rezervno lokacijo 19
Slika 5: Prikaz primera mreže notranjega informacijskega sistema družbe 21
Slika 6: Število izdanih certifikatov ISO/IEC 27001 v letih 2006–2014 23
Slika 7: Delež izdanih certifikatov ISO/IEC 27001 v deležih po regijah sveta v letih 2006–2014 24
Slika 8: Število izdanih certifikatov ISO/IEC 27001 v Sloveniji v letih 2006–2014 24
Slika 9: Ocene kibernetskih nevarnosti po izvoru glede na verjetnost nastanka dogodka v letih 2014–2016 28
Slika 10: Ocene kibernetskih nevarnosti po izvoru glede na učinek dogodka v letih 2014–2016 28
Slika 11: Ocene kibernetskih nevarnosti po izvoru v letih 2014–2016 32
Slika 12: Ocena uporabe mednarodnih standardov na področju informacijske varnosti. .. 32
Slika 13: Koristnost vključitve zunanje institucije za oceno izpostavljenosti 33
Slika 14: Na čem temelji ocena potrebnega zavarovalnega kritja 34
Slika 15: Vzroki za sklenitev zavarovanja kibernetskih tveganj 34
Slika 16: Delež družb brez oziroma s sklenjenim zavarovanjem kibernetskih tveganj 35
Slika 17: Delež družb brez oziroma z vnaprej določenimi finančnimi sredstvi za zavarovanje 35
Slika 18: Prikaz najpomembnejših elementov zavarovanja 36
Slika 19: Višine limitov kritja za katere se odločajo zavarovanci 36
Slika 20: Višine izbranih retencij zavarovancev 37
Slika 21: Odgovori udeležencev glede njihove skrbi glede korektnosti obdelave in izplačila škode 38
Slika 22: Ocene kibernetskih nevarnosti po izvoru v letih 2014–2016 38
Slika 23: Deleži stroška kibernetskega kriminala od BDP po državah skupine G20 42

Slika 24: Deleži stroška kibernetskega kriminala od BDP po drugih državah 42
Slika 25: Povprečni strošek na enoto razkritega podatka v USD v obdobju 2013–2015...46
Slika 26: Povprečni skupni strošek družbe iz naslova razkritja podatkov v mio USD v obdobju 2013–2015 47
Slika 27: Delež napadov z namenom razkritja podatkov glede na vir izvora v letu 2015..47
Slika 28: Pozitivni finančni učinek v USD na višino stroška razkritja enote podatka po faktorjih 48
Slika 29: Rast globalne kosmate zavarovalne premije zavarovanj kibernetskih tveganj v letih 2002–2025 v milijardah USD.....59

UVOD

Svet postaja vse bolj globalno povezan in soodvisen. Hiter razvoj tehnologije in sistemov informacijske tehnologije po eni strani gospodarskim družbam (v nadaljevanju družba) prinaša priložnosti za večjo produktivnost, učinkovitost in dobičkonosnost, po drugi strani pa tudi izpostavljenost potencialnim kibernetskim nevarnostim in tveganjem, ki iz njih izidejo in povzročijo podjetju visoke stroške. Podjetja so razširila poslovanje izven meja svojih držav, poslujejo v mednarodnem okolju, imajo razvejane distribucijske mreže in prodajne poti in prav razvoj tehnologije je prinesel preobrat pri rokovanju s podatki, z distribucijo in hrambo podatkov (Association for financial professionals, 2016).

V našem življenjskem okolju se pojavlja vse več naprav, ki temeljijo na internetu, kar pomeni, da smo pri uporabi povezani z internetom in s tem izpostavljeni nevarnosti varnostnega incidenta, pa se tega pogosto niti ne zavedamo. Tak primer je pametni telefon, preko katerega lahko dobimo virus celo na svoj domači računalnik (preko internetne povezave s telefonom). Napredne tehnologije, ki so močno medsebojno odvisne in pri katerih je zato še posebej pomembna zaščita informacijskih sistemov pred vdori in zlorabami podatkov, da bi lahko uživali njihove prednosti in se izognili stroškom, ki bi jih nezaželeni vdori lahko povzročili, so npr. mobilni internet, tehnologija poslovanja v oblaku, Internet stvari (angl. *Internet of Things*), napredna robotika, avtonomna vozila, 3D tiskanje in druge tehnologije, ki so na pohodu (Association for financial professionals, 2016). Tehnološki napredek v informacijski in komunikacijski tehnologiji tako bistveno vpliva na obnašanje podjetij, ki se morajo zaradi doseganja večje konkurenčnosti na trgu posluževati vse večje uporabe interneta in s tem prilagoditi novim kibernetskim nevarnostim.

Družbe vseh velikosti so iz dneva v dan bolj izpostavljene napadom in vdorom v informacijske sisteme in napadalci sproti izboljšujejo metode vdorov in razbijanja zaščitnih sistemov in glede na večanje števila vdorov v informacijske sisteme se zdi, da vse težje sledijo inovativnim pristopom vdiralcev. Vdiralci na primer sledijo motivu pridobitve finančnega zaslužka, prekinitvi delovanja informacijskega sistema ali celo motivu vohunjenja. Finančni učinek, ki ga lahko povzročijo, je lahko velik in v skrajnih primerih celo poguben za družbe (na primer učinek izgube ugleda), zato morajo ustrezno prilagoditi svoje strategije obvladovanja varnostnih tveganj.

Mnoge študije so pokazale, da je število vdorov v porastu (na primer Verizon, Data Breach Report, 2014, 2015, 2016; Ponemon institute, Cost of Data Breach Study, 2015), zato danes za družbe ni več vprašanje, ali bo do vdorov sploh prišlo, temveč kdaj in v kakšnem obsegu, zato se morajo osredotočiti na prepoznavanje in opredelitev kibernetskih nevarnosti in tveganj, ki jih prinašajo in pomembno vplivajo na njihovo poslovanje, med katerimi pomembno mesto zaseda tudi varnostno tveganje in sprejeti strategijo, s katero

tveganja identificirajo, ovrednotijo, nadzirajo, ter določijo ukrepe za odpravljanje oz. zmanjšanje tveganja.

Raziskava Association for financial professionals iz leta 2015 je pokazala, da se družbe zavedajo, da je v današnjem poslovnem okolju negotovost dobička dejstvo in da je prepoznava nevarnosti in ocena z njimi povezanih tveganj še naprej velik izziv vseh gospodarskih panog. Zato je obvladovanje varnostnih tveganj pridobilo na pomenu kot ključnemu procesu v podjetju, ki je podlaga za boljše strateške in operativne odločitve (Association for financial professionals, 2016).

V Evropi je bila na ravni Evropske unije (v nadaljevanju EU) sprejeta direktiva o varstvu osebnih podatkov, ki bo predvidoma stopila v veljavo po dve letnem prehodnem obdobju, tj. v letu 2018. Med drugim direktiva določa pravila za poročanje o varnostnih incidentih in sankcije v primeru neizpolnjevanja predpisanih pravil, kar bo po mnenju zavarovalnega sektorja pomembno vplivalo tudi na dvig zavedanja o nevarnostih, ki jih grožnje in varnostni incidenti predstavljajo za družbe in bo prispevalo k dvigu pomena upravljanja z varnostnimi tveganji.

V študiji globalnih rizikov Svetovni Ekonomski Forum (v nadaljevanju WEF) ugotavlja, da so kibernetske nevarnosti (angl. *cyber risk*) glede na odgovore anketiranih podjetij umeščene visoko na lestvici nevarnosti, s katerimi se bodo morala v prihodnosti soočiti (WEF, 2016), skupina G-20 pa je kibernetske nevarnosti opredelila kot grožnjo globalnega gospodarstva (Ackermann, 2013). Temu pritrjujejo tudi mnogi odmevni primeri varnostnih incidentov. Ne le, da je nevarnost varnostnih incidentov postala realnost, veča se število incidentov in njihova razsežnost, kar terja primerno obravnavo, tako z vidika mehanizmov obvladovanja varnostnih tveganj kot tudi v smislu zmanjšanja tveganja s prenosom na druge subjekte, med katerimi so prav gotovo aktualne zavarovalnice.

Zavarovalništvo se zaradi pomanjkanja zanesljivih podatkov, ki bi omogočili poglobljene analize kibernetskih nevarnosti in iz njih izhajajočih tveganj, sooča z mnogimi izzivi, ki se nanašajo na razumevanje in obravnavo kibernetskih nevarnosti pri razvoju produkta zavarovanja kibernetskih tveganj (Eling & Wirfs, 2016). Še posebej je izpostavljeno vprašanje zavarovaljivosti, kar posledično vpliva na razvoj zavarovalnega trga za tovrstna tveganja, ki je še vedno relativno majhen in se je zato celo pojavilo vprašanje, ali niso prevelika za zavarovalnice in bi bilo potrebno iskati rešitev v smislu zavarovalnih poolov, ki bi lahko izboljšali stopnjo zavarovaljivosti kibernetskih tveganj in morda tudi vključitev države v primeru ekstremnih škodnih scenarijev (Eling & Wirfs, 2016). Avtorja Eling in Wirfs (2016) sta nadalje s študijo ugotovila, da je po drugi strani možno dvigniti stopnjo zavarovaljivosti kibernetskih tveganj manjših razsežnosti, na eni strani preko pozavarovanja, ter po drugi preko medsebojnega sodelovanja zavarovalnic, v smislu izgradnje skupne podatkovne baze kot nujno potrebno osnovo za aktuarske analize kibernetskih tveganj in določitev primerne premije. Pri večjih rizikih je možnost delitve

tveganj tudi preko povezovanja v »pool«. Omenjena avtorja študije tudi za primer ekstremnih scenarijev vidita možnost dviga stopnje zavarovaljivosti in sicer v smislu vključitve države preko javno-zasebnega partnerstva z zavarovalnicami, kjer bi šlo lahko za direkten vstop države s svojimi kapacitetami (na primer v primeru ekstremnih škodnih scenarijev) ali posredno preko davčnih spodbud za zavarovalnice, da bi povečale svoje kapacitete za tovrstna tveganja.

V prvem poglavju bom najprej opredelila kibernetske nevarnosti, tako terminološko kot vsebinsko, kjer bom tudi razdelala različne izvore teh nevarnosti in podala nekaj najodmevnejših primerov varnostnih incidentov. Opisala bom sisteme varnostne zaščite.

V drugem poglavju je poudarek na tveganjih, ki jih kibernetske nevarnosti prinašajo ter obvladovanje teh tveganj, ki vse bolj pridobiva na pomenu zaradi vse večjega zavedanja o kibernetskih nevarnostih, tudi zaradi naraščajočega števila incidentov in večji stopnji informiranosti o varnostnih incidentih in njihovega ekonomskega učinka na gospodarske subjekte.

Tretje poglavje vsebuje prikaz elementov, potrebnih za oblikovanje ustrezne varnostne strategije, k čemur bo po pričakovanjih pomembno vplivala v našem prostoru tudi zakonodaja EU na področju varnosti osebnih podatkov, ki bo od članic zahtevala tudi vzpostavitev nacionalne varnostne strategije. Pregledala bom tudi različne načine prenosa tveganja na druge subjekte, med katerimi se bom še posebej osredotočila na zavarovalnice in pozavarovalnice.

Četrto poglavje je pregled dosedanjega razvoja zavarovalnega/pozavarovalnega trga in produkta zavarovanja kibernetskih tveganj. Pomembno vprašanje, ki ga bom obravnavala v tem poglavju je poleg karakteristik kibernetskih nevarnosti vprašanje zavarovaljivosti, ki je z naraščanjem števila in razsežnosti varnostnih incidentov vse bolj aktualno in so s tem povezani tudi mnogi izzivi za prihodnost.

V petem poglavju bom pripravila SWOT analizo glede vpeljave zavarovanja kibernetskih tveganj na slovenski zavarovalni trg, kjer bom obravnavala zavarovanje kibernetskih tveganj z vidika elementov iz predhodnih poglavij in na koncu podala sklepne ugotovitve z usmeritvami glede vpeljave tega produkta na slovenski zavarovalni trg.

V nalogi se bom omejila na proučevanje vplivov kibernetskih nevarnosti in izhajajočih tveganj na družbe z vidika njihovega notranjega informacijskega sistema.

Namen magistrskega dela je pregledati obstoječo literaturo in vire na temo kibernetskih nevarnosti, tveganj, ki jih prinaša, možnih načinov obvladovanja teh tveganj in vlogo zavarovalnic pri tem. Temeljna raziskovalna vprašanja, ki jih bom v svojem delu obravnavala so: kaj je kibernetska nevarnost, katera tveganja prinaša, kakšni so možni

načini obvladovanja teh tveganj, kakšno vlogo imajo pri tem zavarovalnice in sicer, ali in do katere mere je kibernetsko tveganje zavarovaljivo, kakšni so obstoječi zavarovalni produkti v svetu ter izzivi, s katerimi se zavarovalnice soočajo, zato da bi razumela, kateri so ključni elementi pri razvoju produkta zavarovanja kibernetskih tveganj. Na podlagi tega bom pripravila sistematični pregled obstoječih dognanj ter z uporabo SWOT analize obdelala različne vidike tega zavarovalnega produkta in izpostavila ključne elemente glede vpeljave na slovenski zavarovalni trg, z namenom prispevati k razvoju slovenskega zavarovalnega trga na tem področju.

Cilj magistrskega dela je podati vpogled v obstoječa spoznanja glede kibernetskih nevarnosti in vloge zavarovalnic pri obvladovanju tveganj, ki jih kibernetske nevarnosti prinašajo ter s pomočjo SWOT analize ustvariti strokovni prispevek z usmeritvami glede vpeljave zavarovanja kibernetskih tveganj na slovenski zavarovalni trg.

Metodologija. Pri izdelavi magistrskega dela sem uporabila splošno raziskovalno metodo spoznavnega procesa ter metodo deskripcije. Splošno raziskovalna metoda procesa je temeljila na pregledu večinoma tuje literature, objavljene v znanstvenih člankih, revijah, knjigah ter objavah renomiranih, svetovno uveljavljenih zavarovalnic in pozavarovalnic ter drugih specializiranih panožnih institucij, ki se ukvarjajo s problematiko kibernetskih nevarnosti in zavarovanjem kibernetskih tveganj. Pri opredelitvi pojmov in raziskovanju obravnavane problematike sem uporabila metodo sistematičnega pregleda literature, kjer sem pregledala do sedaj zbrana spoznanja.

1 KIBERNETSKE NEVARNOSTI

1.1 Opredelitev kibernetskih nevarnosti

V tuji literaturi se pojavlja izraz kibernetski (angl. *cyber*) kot predpona v različnih besednih zvezah. Taki so naslednji primeri: kibernetska nevarnost (angl. *cyber-risk*), kibernetska varnost (angl. *cyber-security*), varnostna grožnja (angl. *cyber-threat*), varnostni incident (angl. *cyber-attack*), kibernetski kriminal (angl. *cyber-crime*), kibernetski terorizem (angl. *cyber-terrorism*).

Kot navaja spletni angleški slovar Oxford (Oxford Dictionaries, b.l.) je izraz kibernetski kot predpona opredeljena kot nekaj, kar je povezano z računalniki, informacijsko tehnologijo (v nadaljevanju IT), virtualno realnostjo. Z etimološkega vidika pa po navedbah v spletnem angleškem slovarju Oxford izvira iz grške besede krmar (grško *kubernetes*), krmariti (grško *kubernan*), ki jo je leta 1948 ameriški matematik Norbert Wiener uporabil za poimenovanje celotnega teoretičnega področja upravljanja in komunikacije pri mehanskih sistemih in pri živalih, kar je posledično z razmahom interneta v devetdesetih letih prejšnjega tisočletja prispevalo k nastanku novih besed, povezanih s kibernetiko (kot na primer omenjeni primeri zgoraj).

V literaturi ni poenotene definicije kibernetskih nevarnosti. Naslednji so primeri opredelitve kibernetskih nevarnosti z zavarovalniškega vidika. Mukhopadhyay, Chatterjee, Saha, Mahanti in Sadhukan (v Eling & Wirfs, 2016, str. 6) povezujejo kibernetske nevarnosti z zlonamernimi elektronskimi dogodki, ki povzročijo motnjo v poslovnem procesu in finančno škodo. Böhme in Kataria (v Eling & Wirfs, 2016, str. 6) opredeljujeta kibernetske nevarnosti z okvaro informacijskih sistemov. Cebula in Young (v Eling & Wirfs, 2016, str. 6) definirata kibernetske nevarnosti in izhajajoča tveganja kot operativno tveganje, kateremu so izpostavljena informacijska in tehnološka sredstva, ki imajo vpliv na dostopnost, integriteto in zaupnost informacij ali informacijskega sistema. Ögüt, Raghunathan in Menon (v Eling & Wirfs, 2016, str. 6) pravijo, da gre pri kibernetskih nevarnostih za nevarnosti, ki lahko ogrozijo informacijsko varnost. National Association of Insurance Commissioners (v Eling & Wirfs, 2016, str. 6) opiše kibernetske nevarnosti kot prekinitev poslovanja (angl. *Business interuption*) krajo identitete, razkritje zaupnih informacij. CRO Forum (2014, str. 5) opredeljuje kibernetske nevarnosti kot nevarnosti, ki izhajajo iz uporabe elektronskih podatkov, z njihovim rokovanjem in posredovanjem z uporabo interneta in telekomunikacijskih mrež in zajema tudi tveganje za: materialno škodo, kot posledico varnostnega incidenta, prevaro zaradi nepravilne uporabe podatkov in kakršnokoli odgovornost, ki izhaja iz hrambe, dostopnosti, integritete in zaupnosti elektronskih informacij, ne glede ali se nanašajo na posameznike, družbe ali državne institucije.

Swiss Re definicija kibernetskih nevarnosti (v Eling & Wirfs, 2016, str. 6) se nanaša tako na fizične osebe, gospodarske družbe kot tudi na vlade držav ter zajema vse nevarnosti, ki izhajajo iz uporabe in posredovanja elektronskih podatkov in vključuje tveganje za nastanek:

- materialne škode kot posledica kibernetskih napadov;
- izgube ali poškodovanja podatkov in s tem povezane finančne posledice;
- prevare na podlagi zlorabe podatkov;
- odgovornosti do tretjih oseb zaradi nerazpoložljivosti, integritete in zaupnosti elektronsko shranjenih informacij.

Na ta način Swiss Re v svoji definiciji vključuje nevarnosti, iz katerih izhaja tveganje za nastanek škode pri žrtvi varnostnega incidenta (angl. *first-party risks*) kot tudi za nastanek škode do tretjih oseb (angl. *third-party risks*), povezane z internetom, spletnim poslovanjem in informacijskimi sredstvi.

Cebula in Young (2010, str. 1) menita, da je najprimernejša definicija v smislu povezave z operativnim tveganjem, torej z vidika tveganj, ki jih kibernetske nevarnosti prinašajo za informacijska in tehnološka sredstva in ki posledično vplivajo na zaupnost, dostopnost ali integriteto informacij ali informacijskega sistema.

1.2 Kategorije kibernetskih nevarnosti glede na vir izvora

Uvodoma sem izpostavila vse večjo medsebojno povezanost, ki jo prinaša tehnološki razvoj in je vse bolj vpeta v naše življenje. Da bi čim bolje izkoristili priložnosti, ki jih razvoj prinaša, se moramo lotiti preučevanja z več zornih kotov, pri čemer je pomembno, da smo pozorni ne le na številne koristi, temveč tudi na nevarnosti in izzive, ki so z njim povezani. Po navedbah Willisove raziskave (Olsen, 2013, str. 7) je 73 % evropskih podjetij takih, katerih poslovanje sloni na internetu in je zato ključnega pomena, da poznajo nevarnosti, ki so jim preko interneta izpostavljene.

Tehnološki razvoj je omogočil razvoj informacijskih sistemov, ki so bolj odprti in lažje dostopni, kar je omogočilo večje medsebojno povezovanje, avtomatizacijo procesov in s tem doseganje večjih poslovnih učinkov, obenem pa večja odprtost in možnosti oddaljenega dostopanja pomenijo tudi potencialno nevarnost za zlorabo in nastanek ekonomske škode. Mnogi gospodarski sektorji temeljijo na sistemih, ki so med seboj povezani preko telekomunikacijskih storitev, računalniških sistemov, še posebej visoka pa je njihova odvisnost na področjih, ki temeljijo na uporabi interneta, kar pomeni, da varnostni incident lahko vpliva na več sistemov hkrati. Danes so informacijski sistemi osnova za delovanje skoraj vsake infrastrukture, kot so na primer proizvodnja in distribucija električne energije, transportni sistem, sistemi proizvodnje hrane, drugi oskrbovalni sistemi, sistem šolstva, zdravstva in drugih javnih ustanov in storitev. Zaradi globalne povezanosti in soodvisnosti teh sistemov lahko v ekstremnem primeru pride celo do kolapsa v širšem smislu, tj. odpoved oz. nedelovanje kritične infrastrukture (Swiss Re, 2014, str. 3).

Globalno povezanost lahko ponazorim z naslednjim primerom tovarne, kjer so prikazane različne poti, preko katerih je tovarna izpostavljena kibernetskim nevarnostim vsled naraščajoče povezanosti. Začnem lahko z oddaljenim dostopom v različne sisteme. Tu gre lahko za oddaljene dostope zaposlenih, ali v primeru sistemov bank omogočen dostop komitentov v sistem banke, ali primer javnih, davčnih uradov, ki omogočijo oddaljen dostop za lažje in hitrejše urejanje različnih zadev družb in posameznikov. Pomemben element v poslovanju tovarne je tudi plačilni sistem, ki povečini teče preko elektronskih povezav in se v tem procesu prenašajo velike količine zaupnih podatkov (tako podatkov uporabnika sistema kot tudi njegovih partnerjev, kupcev). Tudi nekatere servisne storitve, ki jih tovarna potrebuje, se lahko opravijo z uporabo spletnih orodij in je v tem primeru sistem tovarne odprt za potrebne posege za odpravo napake. Tudi sistem logističnih storitev, ki jih tovarna uporablja za namen prevzema surovin od svojih dobaviteljev in dobave izdelkov do svojih kupcev, je zelo napredoval in izkorišča prednosti tehnoloških rešitev za hitro in učinkovito obvladovanje logističnih procesov. Za tovarno je za vzdrževanje dobrih odnosov s strankami in obvladovanjem sistema oskrbovanja s surovinami in oskrbovanjem prodajne mreže izjemnega pomena hiter in učinkovit komunikacijski sistem, ki ga omogočajo ponudniki telekomunikacijskih storitev. Vsak od

omenjenih elementov lahko predstavlja potencialno ogroženost s strani kibernetskih nevarnosti in lahko v primeru varnostnega incidenta zaradi medsebojne povezanosti pomembno vpliva na poslovanje tovarne (Allianz Global Corporate & Specialty, 2015a, str. 16).

Eling in Wirfs (2016, str. 8) ločujeta kibernetske nevarnosti glede na vir izvora na ne-kriminalne in na kriminalne, tj. kibernetski kriminal.

Ne-kriminalni izvor zajema:

- naravne dogodke,
- tehnične napake,
- človeške napake.

Krimalni izvor zajema:

- fizične napade oziroma vdore,
- napade hekerjev,
- izsiljevanje.

Med **naravne dogodke** se upoštevajo dogodki, do katerih pride zaradi naravne nesreče. Tak primer so na primer izpad električne energije, prenehanje delovanja strežnikov in računalniških storitev zaradi potresa, poplave, požara in podobno.

Tehnične napake zajemajo nedelovanje, uničenje strojne, tehnične opreme. Primer tehnične napake je na primer nedelovanje, uničenje trdega diska, zaradi česar pride do izgube podatkov. Podobno lahko na izgubo ali okvaro podatkov vpliva pojav napake v programski opremi.

Človeške napake v kontekstu obravnave ne-kriminalnih izvorov so nenamerna dejanja brez zlonamernega delovanja kot na primer nenamerna razkritja informacij, razne napake pri pripravi poročil ali nenamerne opustitve potrebnih dejanj.

Fizični napadi oziroma vdori zajemajo namerna dejanja zaposlenih, sedanjih ali bivših in celo zunanjih pogodbenikov, ki so v preteklosti sodelovali z družbo, z namenom zlonamernega delovanja. Tak primer je na primer kraja zaupnih podatkov iz informacijskega sistema družbe. Agencija Evropske unije za varnost omrežij in informacij (v nadaljevanju ENISA) med tovrstne napade umešča napade z namenom razkritja zaupnih podatkov (angl. *data breach*) in napade v smislu kraje identitete (angl. *identity theft*). V tem delu se naprej osredotočim na notranje napade. V poročilu je nadalje navedeno, da je pri tovrstnih napadih opaziti trend, ki je v porastu, deloma tudi zato, ker se ti incidenti vedno bolj analizirajo (odkar se je zgodil incident Snowden).

Napadi hekerjev so napadi, usmerjeni na različne podatke družb, njihovih strank in partnerjev z namenom vohunjenja ali sabotaže, kar skušajo doseči z različnimi načini. Na tem mestu se bom za namen te naloge omejila na najbolj razširjene vrste napadov, ki sem jih zasledila v literaturi in se ves čas razvijajo, nadgrajujejo in je zato težko zaobjeti vse aktualne pristope, ki jih hekerji pri svojih napadih ubirajo. Med najpogosteje omenjenimi vrstami napadov so sledeči (ENISA, 2016, str. 19–50):

- napadi z namenom razkritja zaupnih podatkov (angl. *data breach*),
- napadi v smislu kraje identitete (angl. *identity theft*),
- napadi z zavračanjem storitve (angl. *denial of service*),
- napadi s škodljivo, zlonamerno kodo (*angl. malware*),
- napadi preko elektronske pošte in lažnih internetnih strani (angl. *phishing*),
- napadi preko neželene elektronske pošte (angl. *spam*),
- napadi z namenom vohunjenja (angl. *cyber espionage*),
- napadi na spletne aplikacije (angl. web applications).

Napadi z namenom razkritja zaupnih informacij so po navedbah v poročilu ENISE (2016, str. 30) usmerjeni v točno določene gospodarske sektorje, predvsem v institucije zdravstvene oskrbe in vladne organizacije, ki razpolagajo z občutljivimi podatki. Nadalje poročilo omenja naraščajoči trend incidentov prav v zdravstvenem sektorju, medtem ko se pri ostalih sektorjih tovrstni napadi po številu stabilizirajo. V letu 2015 so bili napadi z namenom razkritja zaupnih podatkov najštevilčnejši med vsemi napadi. Zanimiva je tudi informacija iz omenjenega poročila, ki pravi, da pri več kot 50 % incidentih ni jasno, koliko informacij po številu je bilo razkritih, kar kaže na slabše stanje trenutne analitike pri tovrstnih incidentih.

Pri kraji identitete gre za krajo identifikacijskih kod, številk in vseh drugih identifikacijskih oznak, ki označujejo informacije točno določenega uporabnika. Koristi takega napada so lahko mnoge. Od na primer dostopa do podatkov, do katerih lahko dostopa le lastnik in postane informacija s tem ogrožena in izpostavljena zlorabi, za uporabnika pa to prinese bodisi negativni finančni učinek ali krajo občutljivih informacij ali pa vsaj nujno zamenjavo gesel. Tudi ti napadi so pogosto usmerjeni v zdravstveni sektor in so v porastu. Po navedbah v poročilu (ENISA, 2016, str. 41) predstavljajo ti napadi do tretjine vseh kraj identitete, nato sledijo maloprodajne mreže s 15 %, vladne organizacije s 13 %, finančne organizacije 10 % ter izobraževalne organizacije 10 %.

Napadi z zavračanjem storitve delujejo na način, da z masovnim pošiljanjem elektronskih sporočil paralizirajo računalniški sistem uporabnika. V obdobju zadnjega leta je po poročilu ENISE (2016, str. 28) opaziti tovrstne incidente v povezavi z zahtevo po odkupnini, tj. da napadi prenehajo in se odpravi blokada računalniškega sistema uporabnika ob plačilu odkupnine. Poročilo nadalje navaja, da so tovrstni napadi usmerjeni

predvsem v sektor iger na srečo, sektor programske opreme in tehnologije ter ponudnike internetnih storitev, podatki o incidentih pa kažejo, da je bilo največ napadov na javne organizacije ter organizacije iz maloprodajnega in finančnega sektorja, ter da je splošni trend teh napadov v porastu.

Napadi s škodljivo, zlonamerno kodo običajno dosežejo ciljni računalnik preko elektronske pošte. Zlonamerna koda se instalira na računalnik preko odprtja priponke iz elektronske pošte, druga pot pa je tudi preko spletnih strani, ki jih napadalci priredijo na način, da se zdijo navzven avtentične, dejansko pa vsebujejo zlonamerno kodo, ki si jo uporabnik ob pregledovanju spletne strani nevede prenese na svoj računalnik (SI-CERT, 2012, str. 18). Po navedbah poročila ENISE (2016, str. 19) je v letu 2015 prišlo do porasta ti. mobilnih zlonamernih kod za cca 17 %, vendar še vedno ostaja pomemben razlog za skrb za prihodnost zaradi široke razširjenosti mobilnih naprav. Poročilo navaja, da je tudi pri tovrstnih napadih opaziti trend naraščanja.

Napadi preko elektronske pošte in lažnih internetnih strani so usmerjene v krajo gesel uporabnikov ali namestitev zlonamerne kode. Gre za ti. »phishing« napad, ki s primernimi sporočili ali internetnimi stranmi namamijo uporabnike, da odprejo elektronsko pošto in omogočijo napadalcu vstop ali pa na primer ob vstopu na lažno spletno stran banke vpišejo svoje ime in geslo ter napadalcem omogočijo dostop do svojega bančnega računa (ENISA, 2016, str. 33). Poročilo ENISE navaja optimistično ugotovitev na podlagi statističnih podatkov o številu tovrstnih incidentov, in sicer, da je opaziti trend upadanja že drugo leto zapored.

Napadi preko neželene elektronske pošte (angl. *spam*) so ena najstarejših oblik napadov in se še vedno ocenjujejo kot učinkovit način za namestitev zlonamernih kod. Po poročilu ENISE (2016, str. 35) je sicer število napadov v upadanju že zadnjih nekaj let, kar je posledica predvsem učinkovitega filtriranja elektronske pošte in opozoril ponudnikov internetnih storitev in državnih strokovnih agencij.

Napadi z namenom vohunjenja so po podatkih ENISE (2016, str. 47) v porastu in so vse bolj sofisticirani. ENISA (2016, str. 48) je po navedbah v poročilu mnenja, da gre pri teh napadih za usmerjene napade na točno določene cilje, ni pa nujno, da so napadi povezani z vohunjenjem. Usmerjeni napadi se izvedejo na način »spear-phishing« napada, ki je značilno usmerjen v točno določeno uporabniško skupino. Zanj je značilno manjše število poslanih elektronskih sporočil kot pri klasičnem »phishingu« in je lahko po navedbah poročila dosežen učinek napada bistveno večji kot pri klasičnem pristopu. Večina napadov (85 %) tipa »spear-phishing« so zlonamerna priponka internetne pošte, zlonamerna internetna povezava in namestitev zlonamerne kode ob ogledu običajne spletne strani (brez vnosa vstopnih kod ali zagona aplikacije ali programa). Tarče tovrstnih napadov so industrijska proizvodnja, javna administracija in kar 87 % napadov v ozadju podpirajo države, 1 % napadov organizirani kriminal, 1 % konkurenčna družba, bivši zaposleni 1 %.

Napadi na spletne aplikacije običajno poškodujejo lahko celotno okolje aplikacije, mehanizme preverjanja avtentičnosti ob vstopu in s pomočjo tega vgradijo napadalci razne škodljive kode. Z največ tovrstnimi napadi se soočajo v Združenih državah Amerike (v nadaljevanju ZDA) (80 % vseh tovrstnih napadov na globalnem nivoju), sledita ji Brazilija (7 %) in Kitajska (4 %), preostali svet z deležem 9 %. Sodeč po oceni poročila ENISE (2016, str. 25), so tovrstni napadi v porasti.

Izsiljevanje (angl. *ransomware*) so oblike napadov preko interneta, pri čemer običajno preko vdora s pomočjo elektronske pošte napadalec namesti kodo, ki blokira dostop do računalniškega sistema in kasneje od uporabnika zahteva odkupnino v zameno za odblokiranje dostopa. V svojem poročilu ENISA (2016, str. 45) navaja, da je bilo v letu 2015 skoraj dvojno število napadov z izsiljevanjem kot leto prej, kar pripisujejo predvsem temu, da se sedanje različice tovrstnih napadov težko odkrijejo in so ponavadi izvedejo skupaj z agresivnim »phishing« napadom. Napadi z izsiljevanjem so usmerjeni na posameznike, ki po ocenah napadalcev razpolagajo z večjim premoženjem (50 %), večja podjetja (25 %) in manjša podjetja (14 %); od vseh napadov se jih 50 % nanaša na ZDA in Evropo skupaj. Zanimivo je tudi navedeno dejstvo, da je težko doseči popolno vzpostavitev v prvotno stanje po okužbi s tovrstnim napadom. Na novo so se po navedbah ENISE (2016, str. 46) pojavili ti napadi na način, da enkriptirajo datoteke in ti predstavljajo kar 50 % novo prijavljenih incidentov, ki so tudi sicer v porastu.

V Tabeli 1 je prikaz izbranih kibernetskih nevarnosti glede na vir izvora za leti 2014 in 2015 s trendi razvoja.

V Sloveniji je bil leta 1995 ustanovljen nacionalni odzivni center za obravnavo varnostnih incidentov na internetu (v nadaljevanju SI-CERT), ki deluje v okviru javnega zavoda akademske in raziskovalne mreže Slovenije (v nadaljevanju Arnes). Sprejema prijave zaznanih zlorab, vdorov, okužb in drugih dogodkov, ki se nanašajo na računalniško in omrežno varnost in svetuje ob incidentih s svojimi izkušnjami in znanjem (SI-CERT, 2015, str. 9).

V poročilu SI-CERT (2015, str. 22) je zanimiva informacija o vrstah varnostnih incidentov po izvoru kibernetskega rizika, ki so jih ločili v poročilu na tehnične napade in na goljufije ter prevare. Slika 1 prikazuje gibanje števila varnostnih incidentov po vrsti napada za leta 2008–2015.

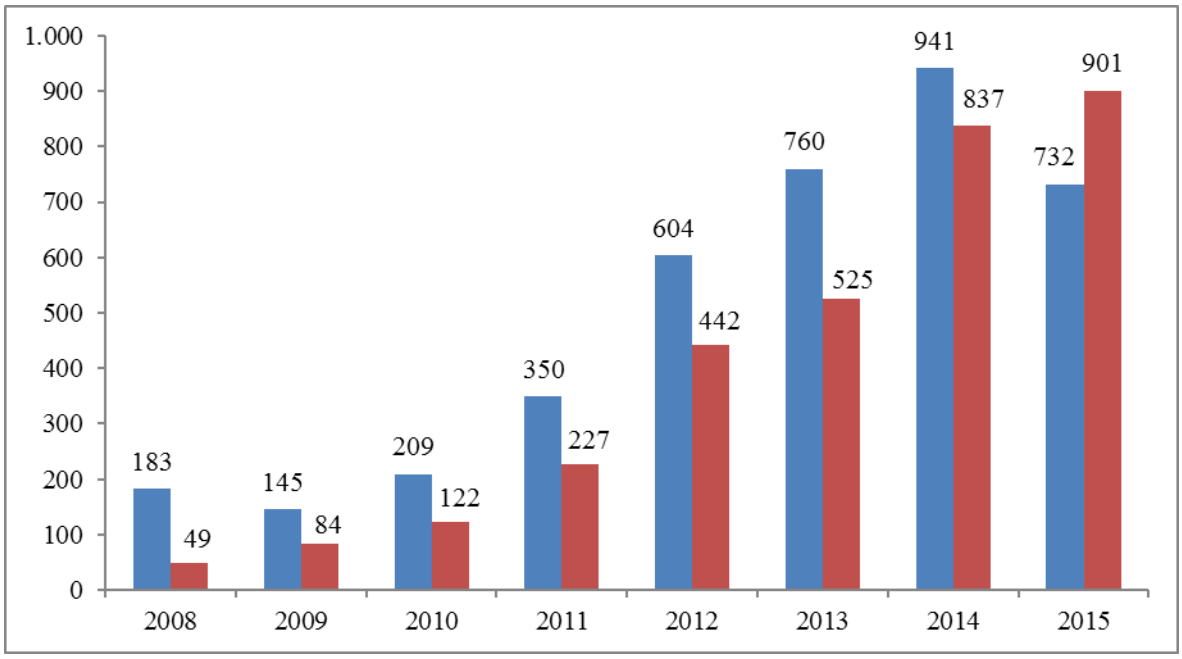
Tabela 1: Izbrane nevarnosti kibernetskih rizikov po viru izvora za leti 2014 in 2015 s prikazom trenda glede na število napadov

	2014	2015
Napadi z namenom namestitve zlonamerne kode (angl. *malware*)	↑	↑
Napadi z namenom zavračanja storitve (angl. *denial of service*)	↑	↑
Materialna škoda na tehnoloških sredstvih/kraja/izguba	↑	→
Dejanja zaposlenih - nenamerna, namerna	→	↑
Napadi preko lažnih internetnih strani (angl. *phishing*)	↑	→
Napadi preko neželene elektronske pošte (angl. *spam*)	↓	↓
Napadi z namenom razkritja zaupnih podatkov (angl. *data breach*)	↑	→
Napadi z namenom kraje identitete	↑	→
Napadi z namenom izsiljevanja	↓	↑
Napadi z namenom vohunjenja	↑	↑

Legenda: rdeča puščica – naraščajoči trend; zelena puščica – padajoči trend; modra puščica – nevtralni trend

Vir: European Network and Information Security Agency, ENISA Threat Landscape 2015, 2016, str. 7.

Slika 1: Število varnostnih incidentov po vrsti incidenta v letih 2008–2015



Legenda: modri stolpci: tehnični napadi; rdeči stolpci: goljufije in prevare

Vir: SI-CERT, Poročilo o omrežni varnosti, 2015, str. 22

Med tehničnimi napadi so v opazovanem obdobju po številu prevladovali varnostni incidenti zlonamerne kode in vdorov v sistem. Največjo rast v obdobju je opaziti pri incidentih zlonamerne kode, saj jih je bilo po številu v letu 2015 kar 418 v primerjavi z 18 primeri v letu 2008 (SI-CERT, 2015, str. 22). Med goljufijami in prevarami so v letih 2008–2015 prevladovale goljufije in »phishing« napadi. Med goljufijami je šlo pretežno za goljufije, povezane s spletnimi nakupi in prodajo, pri »phishingu« pa za napad s ciljem pridobiti gesla in uporabniška imena internetnih uporabnikov, in sicer s pomočjo internetne pošte in lažnih spletnih strani. Največji skok v porastu števila tovrstnih incidentov je bil med letoma 2011 in 2012, sicer pa je število goljufij in prevar zraslo iz 26 primerov v letu 2008 na 618 v letu 2015, število »phishing« napadov pa iz 23 primerov v 2008 na 283 v letu 2015.

1.3 Najodmevnejši primeri varnostnih incidentov

V nadaljevanju je prikazanih nekaj primerov najodmevnejših varnostnih incidentov, ki so bili izvedeni na različne, predhodno že omenjene načine in so bili usmerjeni tako na fizične osebe kot uporabnike sodobnih tehnologij in sredstev, kot tudi na družbe ter države in njihove organe in druge institucije z različnimi cilji.

Moonlight Maze (napad, usmerjen v krajo informacij vladnih organizacij). Varnostni incident, ki je bil usmerjen na Pentagon, sektor za energijo, NASO in različne univerze in raziskovalne laboratorije z namenom vdora v ameriški računalniški sistem za pridobitev vojaških zemljevidov, shem in drugih konfiguracij ameriških čet. Incident so po naključju odkrili vladni uradniki marca 1988, domnevno naj bi šlo za ruske napadalce, ki pa so to zanikali. Incident je eden zgodnejših tovrstnih oblik vdora takih razsežnosti v ameriški informacijski sistem (Balkhi, 2013).

Vdor v informacijski sistem NASE (napad, usmerjen v krajo informacij vstopnih kod). V letu 1999 je najstnik (15 let) izvedel napad s pomočjo vgradnje zlonamerne kode, s katero si je preko elektronske pošte odprl pot do interne komunikacije med različnimi vladnmimi organizacijami ter prišel do različnih uporabniških gesel in tajnih kod z dostopom do vojaškega dela sistema. Uspelo mu je ukrasti del programske opreme NASE, kar je povzročilo prekinitev delovanja za tri tedne. Po navedbah NASE je bila ukradena programska oprema vredna 1,7 milijona ameriških dolarjev (v nadaljevanju USD) in je skrbela za vzdrževanje primerne temperature in vlažnosti v bivalnem delu mednarodne vesoljske postaje. Storilca so kasneje prijeli, vendar je zaradi mladoletnosti dobil le blažjo kazen (ARN, 2015).

V letu 2000 je najstnik iz Kanade izvedel napad na način, ki posledično onemogoči delovanje storitev napadenega (angl. *denial of service*). Njegov cilj so bile družbe **Amazon, CNN, eBay in Yahoo!**. Škoda je bila ocenjena na 1,2 milijona USD. Kot že pri

zgoraj omenjenem primeru najstnika, je tudi njega zaradi mladoletnosti doletela milejša kazen (ARN, 2015).

Titan Rain (napad, usmerjen v krajo informacij vladnih organizacij). V letu 2004 je Shawn Carpenter odkril serijo vdorov, za katere je bil Federal Buro of Investigation (v nadaljevanju FBI) mnenja, da stoji za tem Kitajska. Šlo je za vdore v različne informacijske sistreme kot so NASA, Lockheed Martin, Redstone Arsenal in Sandia National Laboratories (Balkhi, 2013).

TJX (napad, usmerjen v krajo kreditnih kartic in finančnih informacij). TJX je največja veriga prodajaln za oblačila in opremo za dom v ZDA. Leta 2007 je družba razkrila, da se je zgodil varnostni incident in kot posledica so jim bile v razdobju osemnajstih mesecev odtujene informacije o njihovih kupcih, in sicer o kreditnih in debitnih karticah, čekih in transakcijah vezanih na vračilo blaga, celo številkah vozniških dovoljenj kupcev, v skupni ocenjeni vrednosti 90 milijonov USD. Kasneje so odkrili, da je bil incident možen zaradi nezaščitenega brezžičnega interneta v eni od trgovin, odgovorni za vdor je bil A. Gonzales, ki je s skupino pomočnikov izkoristil to slabost in TJX ukradel 45 milijonov številk kreditnih in debitnih kartic (Balkhi, 2013).

Projekt Chanology (napad z motivom izraza protesta). Največji protestni napad proti novi religiji, t.i. scientologiji, je izvedla skupina Anonymous v januarju 2008. Razlog za izvedbo napada je bil v začetku namen cerkve, da iz javnosti umakne intervju s Tomom Cruisom, kot enim vidnejših članov nove religije, ki je bil objavljen na spletu januarja 2008. Skupina Anonymous je za nekaj dni onemogočila delovanje spletne strani cerkve, s katerim je želela izraziti svoje nasprotovanje novi religiji in cenzoriranju na internetu (ARN, 2015).

Stuxnet (vsesplošni, vseobsegajoči incident) je ime zlonamerne programske oprema, ki je bila odkrita leta 2010. Usmerjena je bila v sabotažo industrijskih sistemov in je okužil vrsto industrijskih sistemov po vsem svetu. V napadeni sistem se prenese preko USB prenosnih ključkov, nato se tam zamaskira in prenese naprej po sistemu in omogoči napadalcem, da prevzamejo nadzor brez vednosti operaterjev. Prva tarča Struxneta naj bi bil iranski jedrski program, kjer naj bi Struxnet sabotiral centrifuge v procesu bogatenja urana (Swiss Re, 2014, str. 3).

Sony Corporation (napad, usmerjen v krajo informacij gospodarskih družb). V letu 2011 je prišlo do varnostnega incidenta, ki je bil usmerjen v Sonyjevo internetno storitev PlayStation in Qriocity, povzročil prekinitev delovanja in onemogočil dostop uporabnikom. V času prekinitve, ki je trajala 23 dni, je bilo izpostavljenih 77 milijonov uporabniških računov, vključno z informacijami o kreditnih in debitnih karticah uporabnikov (Balkhi, 2013).

Epsilon (napad, usmerjen v krajo informacij vstopnih kod specifičnih spletnih strani). Epsilon je eden največjih svetovnih ponudnikov marketinških storitev z uporabo spletne pošte več kot 2.500 družbam. Med njimi naj omenim največje, kot so: JP Morgan Chase, Best Buy, CitiGroup, Barklay's bank. Napadalci so leta 2011 vdrli v podatkovno bazo Epsilona z imeni in spletnimi naslovi strank družb, kar še dodatno potencira razsežnosti tega incidenta (Balkhi, 2013).

Target Corporation (napad, usmerjen v krajo kreditnih kartic in finančnih informacij). Target je za Wallmartom drugi največji diskontni prodajalec v ZDA. V letu 2013 se je v času soočil z varnostnim incidentom, katerega posledice so bile kraja 40 milijonov podatkov o računih kreditnih in debitnih kartic kupcev, ki so nakupovali v trgovinah Target (ocena pravi, da je bilo v incident vključeno 1.797 trgovin v ZDA) v času prazničnih nakupov (december 2013). Vdiralci so v računalniški sistem Targeta namestili zlonamerno kodo, s pomočjo katere so prišli do kartičnih podatkov kupcev (imena, številke kartic, varnostne kode) in jih dnevno, v času odprtja trgovin prenašali najprej na tri kraje v ZDA, od tam pa naprej v Moskvo. Varnostni sistem Targeta je sicer javil opozorilo, da je zaznal večji prenos podatkov, vendar ni nihče odreagiral. Alarm se je sprožil šele na podlagi opozoril izdajateljev kartic in njihovih izvajalcev kartičnih storitev, ki so zaznali val goljufivih transkacij (Finkle & Skariachan, 2013).

Operacija Aurora (napad, usmerjen v krajo informacij od gospodarskih družb). Tako je poimenovana serija varnostnih incidentov v letu 2009, ki jih je izvedla skupina Elderwood iz Pekinga, ki jih je javno razkril Google v začetku leta 2010. Tudi družbe Rackspace, Juniper Networks in Adobe Systems so javno priznale, da so bile tarča incidentov, v medijih pa so se omenjale tudi Yahoo, Symantec, Mogran Stanley. Vdiralci so vstopili preko spletnih strani družb, zlonamerna koda pa se je ob uporabniški izbiri spletne strani namestila v informacijski sistem družbe z namenom pridobitve dostopa do pomembnih podatkov in morda celo z namenom spremeniti izvorne kode za dostop (Balkhi, 2013).

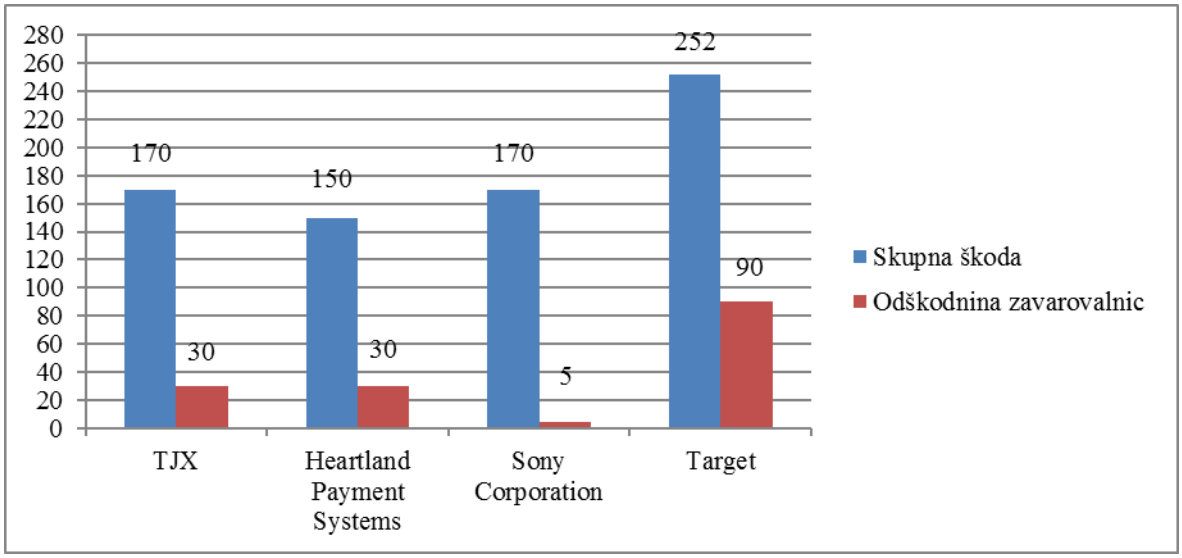
Heartland Payment Systems (napad, usmerjen v krajo kreditnih kartic in finančnih informacij). V letu 2009 je plačilni sistem Heartland objavil novico, da je bil v letu 2008 tarča varnostnega incidenta. Izvedel ga je A. Gonzales s pomočniki, pri čemer so pokradli 100 milijonov številk kreditnih in debitnih kartic. Škoda je bila ocenjena na več 140 milijonov USD. V letu 2010 so A. Gonzalesa obsodili na 20 let zaporne kazni za vdor v plačilni sistem Heartlanda (Balkhi, 2013).

Anthem (napad, usmerjen v krajo zdravstvenih informacij). V letu 2015 je bila zdravstvena zavarovalnica Anthem žrtev varnostnega incidenta, ki je bil usmerjen na informacijski sistem zavarovalnic in je zajel 80 milijonov občutljivih osebnih podatkov kot so rojstni datumi, naslovi prebivališča, številke socialnega zavarovanja, spletni naslovi, podatki o zaposlitvi in dohodki strank zavarovalnice. Po navedah preiskovalcev bi incident lahko izviral iz Kitajske, upoštevaje način odtujitve podatkov in t.i. prstne odtise, ki so

kazali na Kitajsko. Ob tem dogodku se pojavljajo številna vprašanja glede resničnih ciljev, ki so za temi incidenti in niso povezani z doseganjem profita. Med zavarovanci Anthema so zaposleni Boeinga, ki imajo obrambno enoto v Missouriju, ZDA in bi bili lahko zanimivi za tuje organizacije (foreign intelligence organisations). V virih se na primer omenja tudi cilj vohunjenja kot možni scenarij, še posebej, če govorimo o zavarovancih, ki so zaposleni pri dobaviteljih opreme za obrambne namene (Balkhi, 2013).

Varnostni incidenti imajo lahko velike finančne učinke za družbe, ki so jim bile izpostavljene. Za primere varnostnih incidentov pri TJX, Heartland Payment Systems, Sony Corporation in Target sem našla podatke o skupnem znesku škode in povračilu škode od zavarovalnic (Schlayer, 2015, str. 5) in so prikazani v Sliki 2.

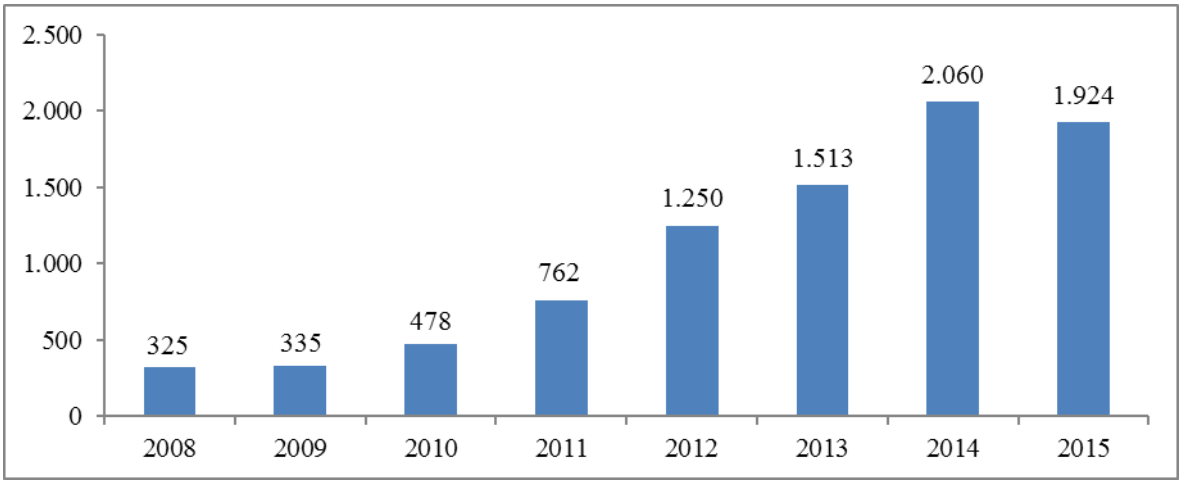
Slika 2: Zneski skupne škode in odškodnina zavarovalnic pri izbranih primerih varnostnih incidentov (v milijonih USD)



Vir: A. Schlayer, Cyber insurance – a new product to ensure premium growth?, 2015, str. 5.

Iz poročila SI-CERT o omrežni varnosti (2015, str. 20) je razbrati, da se tudi v Sloveniji že soočamo z varnostnimi incidenti, ki so v porastu, kar je razbrati tudi iz števila obravnavanih incidentov SI-CERT, ki se je od leta 2008 do 2015 povečalo za skoraj šestkrat. Slika 3 kaže povečevanje števila obravnavanih incidentov v SI-CERT.

Slika 3: Število obravnavanih varnostnih incidentov v SI-CERT v letih 2008–2015



Vir: SI-CERT, Poročilo o omrežni varnosti, 2015, str. 20.

Med primeri varnostnih incidentov, ki jih je obravnaval SI-CERT bom izpostavila napad skupine Anonimni v letu 2012 in napad na slovenske banke v 2015.

V januarju 2012 je Slovenija skupaj z drugimi članicami EU podpisala sporazum ACTA (angl. *Anti-Counterfitting Trade Agreement*). Kmalu po podpisu je skupina Anonimni napovedala vrsto napadov in postavila ultimat vladi Republike Slovenije, naj zamrzne ali umakne podpis sporazuma. SI-CERT se je odzval s tehničnimi ukrepi za obrambo Arnes omrežja, preko katerega je povezano omrežje državnih ustanov ter obvestil vse ponudnike v Sloveniji o pričakovanih vrstah napadov in možnih tarčah na omrežjih ter nasveti za obrambo. V obdobju od 4. do 17. februarja 2012 je sledilo več napadov s poplavo podatkov, poskusi vdora v sistem javne uprave in nekaj drugih napadov. S poplavo prometa so bili nekaj časa onemogočeni strežniki Nove Ljubljanske banke, spletne strani nekaterih slovenskih političnih strank ter portala predlagaj.vladi.si. Napadi so izkoristili pomanjkljivosti spletnih aplikacij na javno dostopnih strežnikih državnih ustanov, niso pa povzročili trajne škode, niti niso imeli učinka na državno infrastrukturo. Zaradi neuspešnosti napadov na državne ustanove je skupina Anonimni iskala nove tarče in med njimi Zvezo potrošnikov Slovenije, kjer so za nekaj časa razobličili njihovo spletno stran. Čez nekaj časa so napadi ponehali, resnejših posledic ti napadi niso imeli, so pa vzbudili veliko medijske pozornosti (SI-CERT, 2013, str. 12).

Primer »phishing« napada na slovenske banke je začel obravnavati SI-CERT 23. januarja 2015, ko so prejeli prijavo o sumljivi elektronski pošti, ki je naslovnike usmerjala na lažno spletno stran NKBM banke in se nato razširil na komitente šestih bank v Sloveniji. Napadalci so na črnem trgu pridobili podatke elektronskih naslovov slovenskih uporabnikov (nepreverjenih, nekateri niso bili niti več veljavni) in jim pošiljali sporočila z izmišljenih elektronskih naslovov, pri čemer so bile domene podobne imenu banke, vendar neregistrirane. Ko se «phishing« sporočila odpošljejo, se jih nekaj zaradi neveljavnih

elektronskih naslovov odbije zaradi nameščene zaščite elektronske pošte nazaj na strežnik pošiljatelja. SI-CERT je za uporabnike mreže Arnes začel spremljati dogodke in ugotovil, da prihajajo sporočila le iz nekaj strežnikov, jih identificiral in vsem internetnim ponudnikom v Sloveniji svetoval, da omejijo sprejem pošte s teh strežnikov ter nadalje napotil k razmisleku o zavračanju tudi take pošte, ki pride iz neregistriranih domen. Skozi proces tega dogodka je SI-CERT odkril 30 lažnih spletnih strani in poskrbel za njihovo odstranitev ob sodelovanju z drugimi CERT centri v tujini in sproti o poteku obveščal javnost preko socialnih omrežij in svoje spletne strani. V tednu dni se je napad umiril, raziskava pa je kasneje pokazala, da so bili napadalci verjetno iz Rusije (SI-CERT, 2015, str. 26).

1.4 Sistemi varnostne zaščite informacijskih sistemov

Ko govorimo o sistemih zaščite informacijskih sistemov, pravzaprav mislimo na sisteme, ki zagotavljajo varno rokovanje in upravljanje z različnimi informacijami. Te so lahko ključnega pomena za državo, sistem državne uprave, posameznike in poslovanje družb, zato zagotavljanje informacijske varnosti zaradi vse večje globalne povezanosti in digitalizacije podatkov ter uporabe interneta pridobiva na pomenu.

Primeri takih informacij so na primer strateški načrti razvoja produktov, razvoja poslovanja, informacije o strankah, marketinški načrti in podobno. Posledično družbe stremijo k temu, da dosegajo ustrezno stopnjo varovanja podatkov pred razkritjem in zlorabo (če vzamem za primer napad z namenom razkritja in/ali zlorabe informacij), na drugi strani pa morajo skrbeti tudi za ustrezno varnost svojega informacijskega sistema, da se ubranijo pred na primer zunanjimi poskusi vdora ter obenem vzpostaviti ustrezne notranje procese, ki bodo čimbolj zmanjšali nevarnosti notranjih incidentov, kot so na primer zlonamerne aktivnosti zaposlenih.

V nalogi se bom omejila na informacijske sisteme, ki se nanašajo na družbe, in sicer na njihove notranje informacijske sisteme in proučevanje z njimi povezanih tveganj, ki jih kibernetske nevarnosti prinašajo in lahko ogrozijo sam sistem in informacije, shranjene v sistemu ter s tem vplivajo na poslovanje, doseganje dobička in strateških ciljev družbe. Družbe shranjujejo svoje informacije v svojih notranjih sistemih ter tudi v eksternih sistemih, kot je primer vse bolj razširjenega sistema shranjevanja v oblaku, ki pa ni predmet te naloge.

Družbe imajo vzpostavljen informacijski sistem na način, da družbi zagotavlja čim bolj nemoteno delovanje za doseganje svojih poslovnih ciljev. Pri gradnji sistema se ravnajo po načinu dela, ki je vzpostavljen v družbi, po postavljenih standardih glede neprekinjenega delovanja in glede na obseg sredstev, namenjen informacijskemu sistemu družbe. Slika 4 je prikaz primera strukture informacijskega sistema družbe, ki je odraz dobrih praks s področja informacijskih sistemov. Prikazan sistem vključuje shemo strukture primarne in

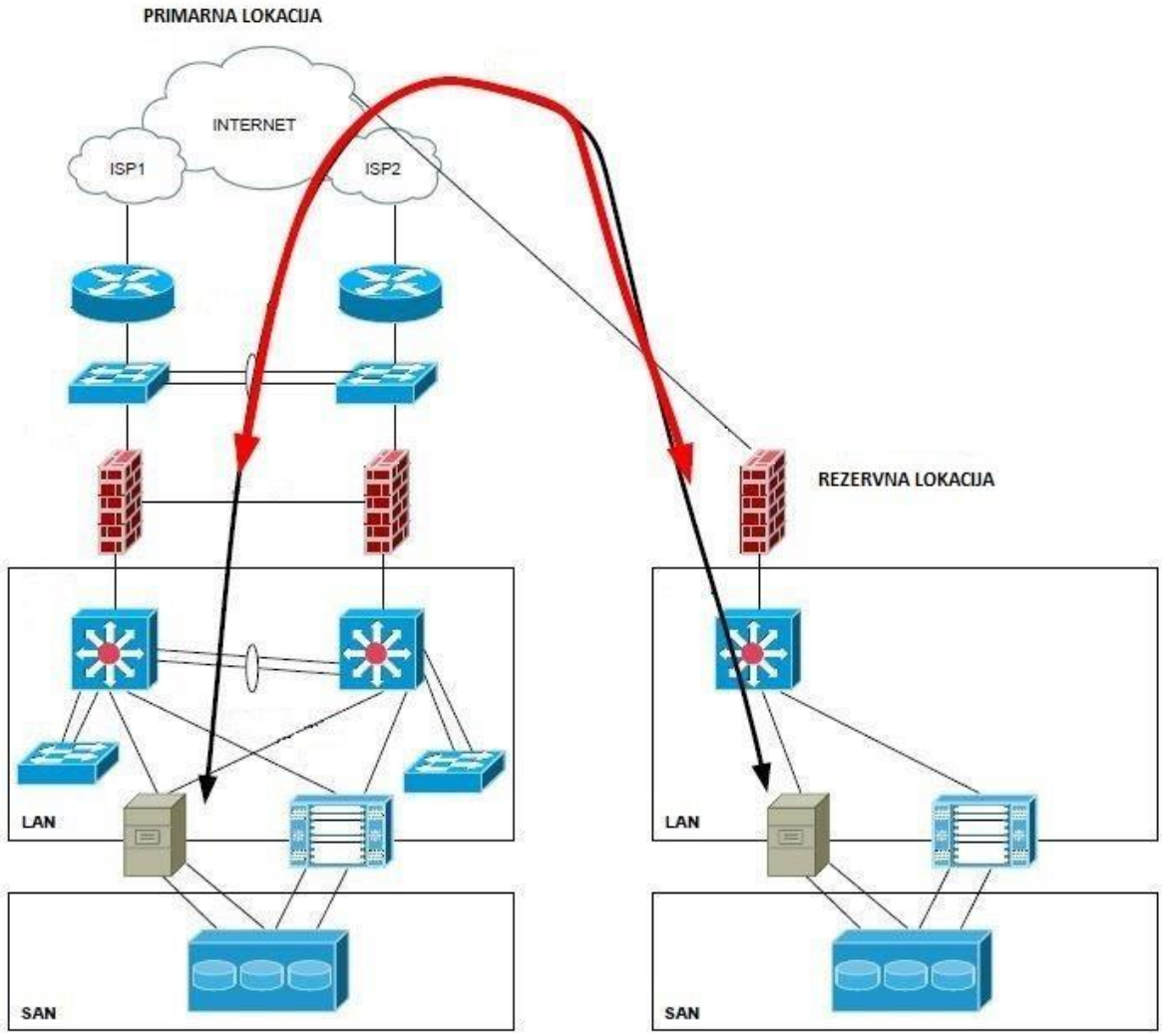
rezervne lokacije. Delovni proces teče na primarni lokaciji, od koder se vsi podatki prenesejo na rezervno lokacijo, kjer lahko zaposleni nadaljujejo delo v primeru izpada primarne lokacije. Običajno so rezervne lokacije namenjene za omogočanje družbi, da nadaljuje s svojo dejavnostjo tudi v primeru katastrofalnih dogodkov, ki uniči primarno lokacijo. Dobre prakse opredeljujejo, da ima družba dva ponudnika internetnih storitev, informacijski sistem zagotovi avtomatski preklop na drugega, če prvi ne more več zagotavljati storitev.

Za namen ponazoritve povezav v informacijskem sistemu sem izbrala primer internetnega uporabnika, ki želi dostopiti do internetne strani družbe. Z vstopom na internet in izbiro internetne strani družbe, steče povezava od internetnega ponudnika proti sistemu družbe, preko stikal, ki usmerjajo internetni promet proti požarni pregradi, ki uporabnika preveri in v kolikor ni v nasprotju z varnostnimi standardi, gre uporabnik lahko naprej v območje mreže (na sliki LAN), kjer ga razdelilci mreže preko uporabniških stikal usmerijo v smer, kamor mu je vstop dovoljen glede na vnaprej opredeljene pravice vstopa (ločeno za goste in domače uporabnike, tj. zaposlene v družbi). Na sliki sta prikazani dve omari v območju mreže, in sicer se nahajata v strežniški sobi. Ena predstavlja fizični strežnik, druga virntualni strežnik. Najprej je pomembno, da sta dva zaradi zamenljivosti v primeru nedelovanja enega od njiju. Dodatno se je družba v tem primeru tudi odločila, da bo eden od njiju virtualen zato, ker je to že potrebno izhodišče za morebitni kasnejši prenos podatkov v oblak. Strežniki so naprej povezani z diskovnim poljem (na sliki SAN), kjer so shranjeni podatki družbe in uporabniki dostopajo do njih skladno z dodeljenimi pravicami.

V nadaljevanju je v Sliki 5 podrobnejši prikaz povezav znotraj mreže družbe (LAN). Družba ima nameščene varnostne sisteme preko namestitve požarne pregrade, internetne poti, preko katere spremlja, nadzira in zaustavi sumljiv promet in internetno pošto s pomočjo opredeljenih protokolov dostopa in antivirustnih programov in drugih programov za prepoznavo škodljivih elementov. Uporabnik s svojo identifikacijsko kodo vstopi v sistem (oznaka na sliki z xxx.xxx.xxx.xxx) preko internetne povezave, nadaljuje vstop po varnostnem testiranju preko požarne pregrade, kjer ga v primeru dostopanja do spletne strani družbe sistem usmeri na spletno stran, za katero se v ozadju nahajajo strežniki v demilitarizirani coni (okrajšava DMZ) in so nujni za delovanje spletne strani (strežnik za delovanje spletne strani je obarvan oranžno). V tej coni so tudi strežniki, ki omogočajo tok internetnega prometa in pošte (angl. *web gateway* in *email gateway*), ki ima sistemsko opredeljene vrste škodljivega prometa/pošte, ki se v tem primeru tu ustavi in je v karanteni za namen analize in se v primeru neprimernosti odstrani. Med strežniki v demilitarizirani coni se nahaja tudi datotečni strežnik, v katerega se lahko skladno z vnaprej določenim protokolom prenosa podatkov odložijo datoteke za nadaljnjo obdelavo (na primer vprašalnik zavarovanca, ki ga zavarovanec odloži za namen nadaljnje analize zavarovalnice) in je v podobni funkciji kot je to pri oblaku. V sistemu je zagotovljen tudi oddaljen dostop uporabnikov, tu gre za zaposlene družbe, kjer vsak s svojo identifikacijo dostopa do sistema preko požarne pregrade naprej preko glavnega stikala, ki usmeri

uporabnike do svojih delovnih postaj, v tem delu so tudi opredeljeni dostopi do brezžičnega omrežja, ločeno za goste in ločeno za zaposlene, s pripadajočimi pravicami dostopa.

Slika 4: Prikaz primera notranjega informacijskega sistema družbe z rezervno lokacijo



Iz glavnega stikala je dostop do strežniškega okolja, ki se fizično nahaja v strežniški sobi, opremljeni in zaščiteni po strogih varnostnih standardih glede varovanja, nivoja temperature, vlage v prostoru in drugih tehničnih zahtevah za zagotovitev nemotenega delovanja. Možni vdor v sistem bi bil teoretično tudi preko vdora v strežniško sobo, vendar nisem zasledila informacij o tovrstnih napadih, verjetno predvsem zato, ker tak napad terja veliko več sredstev in tveganj za napadalce v primerjavi z ostalimi načini. V strežniški sobi je predvideno tudi dodatno napajanje preko baterije za zagotovitev varnostnega izklopa v primeru prekinitve dobave električnega toka (na sliki oznaka UPS). V strežniškem okolju so različni fizični strežniki, ki pokrivajo različna področja in na katerih tečejo tudi virtualni strežniki, zaradi zagotovitve rezerve v primeru okvare fizičnega strežnika (na sliki oznake

ESX). Tu je tudi nadzorni strežnik, preko katerega administrator informacijskega sistema spremlja dogajanje in delovanje sistema preko kontrolnih lučk.

V naslednjem koraku uporabnik, v kolikor mu njegove dodeljene pravice to omogočajo, dostopa do različnih strežnikov, preko katerih tečejo poslovni procesi družbe. V sliki je prikazan primer gručnega strežnika (na sliki označena kot dva strežnika oranžne barve, ki sta povezana), ki je rezerva za primer prenehanja delovanja osnovnega strežnika. Ta rešitev je priporočena za vse ključne procese v družbi, na sliki so le-ti označeni z oranžno, zelena barva predstavlja aplikacijski strežnik, modri z oznako HW so fizični strežniki, ostali brez oznake tečejo preko fizičnih, ki jih je več, da zagotavljajo rezervo za primer nedelovanja.

Za varnostno zaščito je uveljavljen izraz informacijska varnost (angl. *information security*) in se uresničuje preko elementov kot so zaupnost, celovitost in razpoložljivost (angl. *confidentiality, integrity, availability*). Zaupnost se nanaša na lastnost, da informacija ni razkrita nepooblaščenim deležnkom, celovitost se nanaša na lastnost, da ostajajo informacije popolne in pravilne in se ne morejo brez ustreznih protokolov spremeniti, razpoložljivost pa je lastnost, ki označuje to, da je na primer sistem na voljo za uporabo na zahtevo pooblaščenih deležnikov.

Za dosego učinkovite informacijske varnosti je potrebno pri izgradnji sistema informacijske varnosti upoštevati naslednje:

- informacijsko infrastrukturo,
- varnostno politiko, standarde in postopke,
- izobraževanje in osveščanje uporabnikov,
- zagotavljanje skladnosti,
- ocenjevanje varnosti.

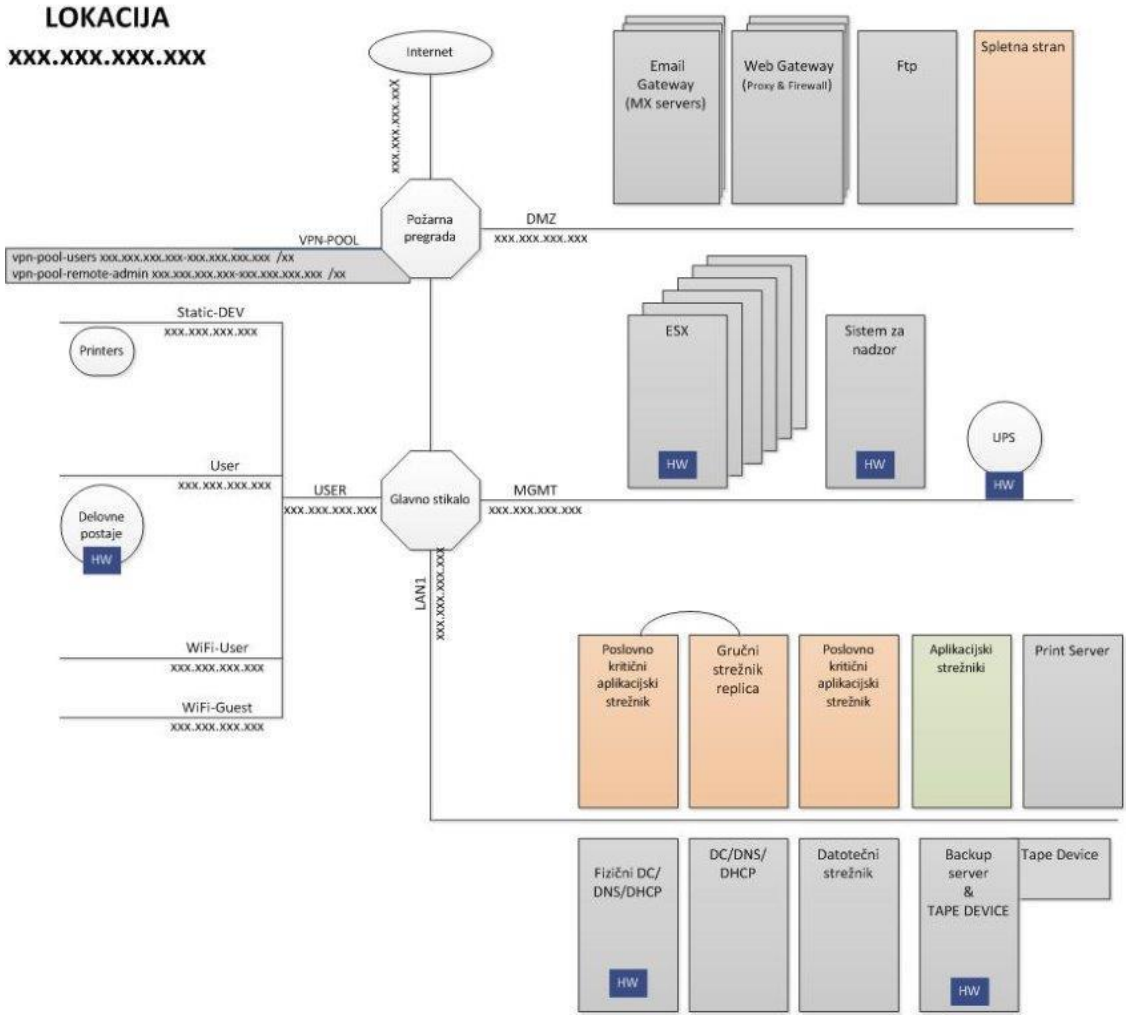
Pri izgradnji ustreznega sistema informacijske varnosti so družbam v pomoč uveljavljeni mednarodni standardi, ki so plod dela strokovnjakov in znanstvenih institucij in predstavljajo dogovor glede kvalitete, varnosti in zanesljivosti (Disterer, 2013, str. 92). Za področje varnostne zaščite informacij in informacijskih sistemov so aplikativni standardi družine ISO 27000, ki veljajo za standarde najboljših praks in med katerimi še posebej izpostavljam standarde ISO/IEC 27000, ISO/IEC 27001 in ISO/IEC 27002, ki vsebujejo nabor zahtev in usmeritev za dosego ustrezne informacijske varnosti in so bili razviti v sodelovanju z »International electrical Commission« (IEC), vodilno institucijo pri sprejemu mednarodnih standardov iz področja elektronike in elektroniki sorodnih tehnoloških vej (Disterer, 2013, str. 92).

ISO/IEC 27001 je bil objavljen leta 2005 in se nanaša na zahteve glede sistemov upravljanja z informacijsko varnostjo (angl. *Information Security Management System*) s cljem, da se vzpostavi politika planiranja, implementacije, upravljanja, nadzora in

izboljšave sistema upravljanja z informacijsko varnostjo. Standard je osovan na sistemu kontrol, katerim mora družba zadostiti in so opredeljene kot sledi (Disterer, 2013, str. 95–96):

- varnostna politika,
- organizacija informacijske varnosti,
- upravljanje s sredstvi,
- varnost povezana s človeškimi viri,
- fizična zaščita sredstev in informacij družbe, okoljska zaščita,
- upravljanje s komunikacijami in izvajanjem dejavnosti družbe,
- kontrola dostopa,
- pridobitev, razvoj, vzdrževanje informacijskih sistemov,
- upravljanje z varnostnimi incidenti v okviru informacijske varnosti,
- skladnost.

Slika 5: Prikaz primera mreže notranjega informacijskega sistema družbe



ISO/IEC 27002 je bil izdan leta 2007 in je nadaljevanje in razširitev standarda ISO/IEC 27002 v obliki kodeksa za vodenje informacijske varnosti in podaja nabor varnostnih kontrol.

ISO/IEC 27000 je bil sprejet leta 2009 in vsebuje pregled standardov družine ISO 27000 in razlago pripadajoče terminologije. Standardi družine ISO 27000 združujejo zahteve in usmeritve glede vzpostavitve sistemov upravljanja z informacijsko varnostjo, pod skupnim nazivom »Informacijska tehnologija – varnostne tehnike«.

Sledeči so standardi iz družine 27000, od katerih so nekateri še v izdelavi in še niso objavljeni (ISO standards, b.l.):

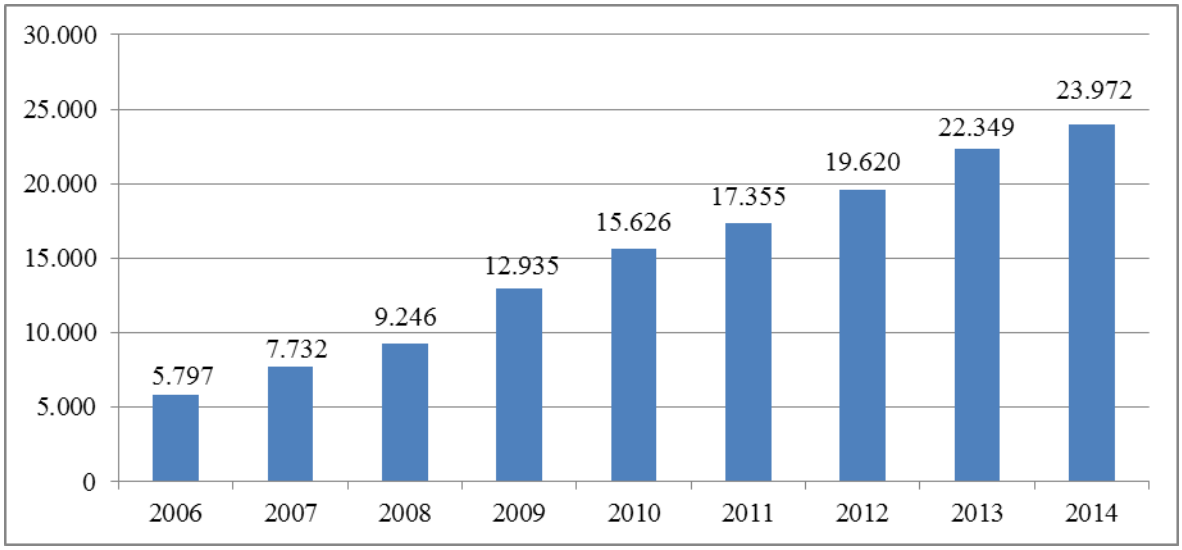
- ISO/IEC 27000 (2009) je pregled in uvod v družino ISO 27000 standardov in slovar izrazoslovja;
- ISO/IEC 27001 (2005) določa zahteve sistema za upravljanje z informacijsko varnostjo, specifikacije po katerih lahko organizacije pridobijo certifikat;
- ISO/IEC 27002 (2007) je kodeks za upravljanje varovanja informacij, z naborom varnostnih kontrol, ki so sprejete kot dobra praksa;
- ISO/IEC 27003 (2010) bo prispeval dodatno pomoč pri uvedbi standarda ISO/IEC 27001;
- ISO/IEC 27004 (2009) predlaga kazalce za pomoč pri izboljšavi učinkovitosti upravljanja z informacijsko varnostjo;
- ISO/IEC 27005 (2011) se nanaša na upravljanje z varnostnim tveganjem;
- ISO/IEC 27006 (2011) je vodič glede postopka za pridobitev certifikata;
- ISO/IEC 27007 (2011) je vodič za revizijo sistema upravljanja z informacijsko varnostjo s poudarkom na upravljanju sistema;
- ISO/IEC 27008 (2011) je vodič za revizijo sistema upravljanja z informacijsko varnostjo s poudarkom na varnostnih kontrolah;
- ISO/IEC 27010 (2012) je vodič sistema upravljanja z informacijsko varnostjo glede komunikacije med oddelki;
- ISO/IEC 27011 (2008) je vodič sistema upravljanja z informacijsko varnostjo za telekomunikacijske organizacije;
- ISO/IEC 27013 (2015) je vodič za integracijo uvedb ISO/IEC 20000-1 in ISO/IEC 27001;
- ISO/IEC 27014 (2013) se nanaša na vodenje informacijske varnosti;
- ISO/IEC 27015 (2012) bo vodič sistema upravljanja z informacijsko varnostjo za finančne organizacije in zavarovalnice;
- ISO/IEC 27031 (2011) se nanaša na neprekinjeno poslovanje;
- ISO/IEC 27032 (2012) je vodič za Internetno informacijsko varnost;
- ISO/IEC 27033 (2015) se nanaša na IT mrežno varnost;
- ISO/IEC 27034 (2011) je vodič za varnost aplikacij;

- ISO/IEC 27035 (2011) se nanaša na upravljanje varnostnih incidentov;
- ISO/IEC 27036 (2013) je vodič za zunanje izvajanje varnosti;
- ISO/IEC 27799 (2008) določa specifične zahteve standarda ISO/IEC 27002 za zdravstveni sektor.

Zanimiv je tudi pregled števila izdanih certifikatov po letih. V Sliki 6 je prikaz gibanja števila izdanih certifikatov ISO/IEC 27001 za vse države sveta v obdobju od 2006–2014. Opaziti je skromen porast skupnega števila certifikatov v letu 2014 glede na 2013, in sicer se je povečalo skupno število izdanih certifikatov le za 7 % (porast v 2013 glede na 2012 v višini 14 %).

Regijska razporeditev izdanih certifikatov ISO/IEC 27001 kaže, da je največ certifikatov v letu 2014 izdanih v Vzhodni Aziji, in sicer na račun Japonske, ki ima tudi v svetovnem merilu največje število izdanih certifikatov v vseh letih prikazanega obdobja. Na drugem mestu je Evropa, kjer je vodilna država po številu izdanih certifikatov Velika Britanija, sledijo ji Italija, Romunija, Španija, Nemčija, če navedem le prvih pet. Slovenija se nahaja na enaindvajsetem mestu z 58 izdanimi certifikati.

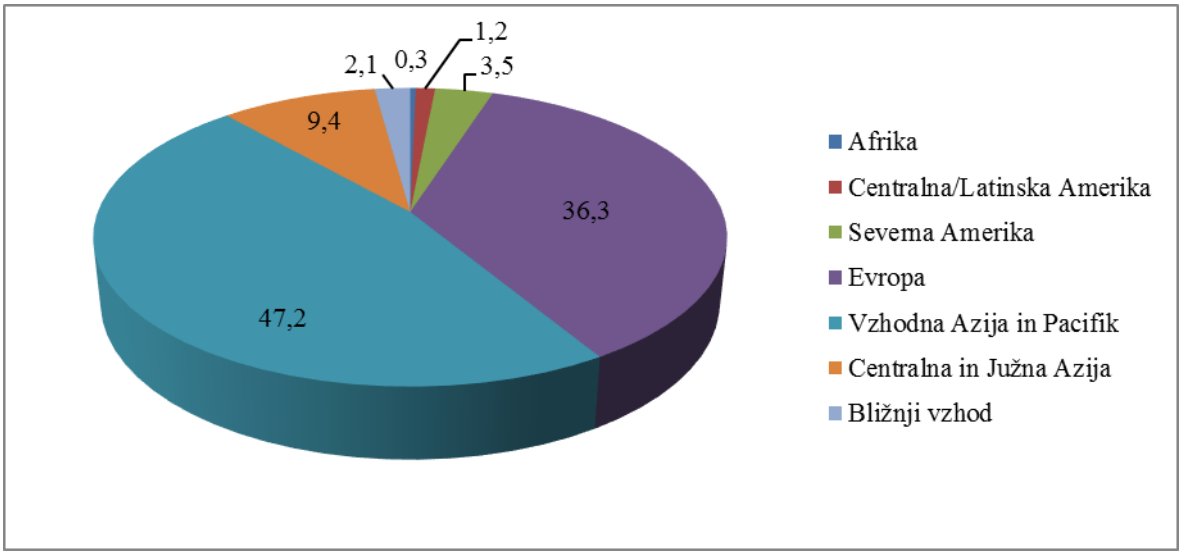
Slika 6: Število izdanih certifikatov ISO/IEC 27001 v letih 2006–2014



Vir: ISO Survey Report, 2014, tabele s podatki.

V Sliki 7 je prikaz deleža izdanih certifikatov v letu 2014 po regijah.

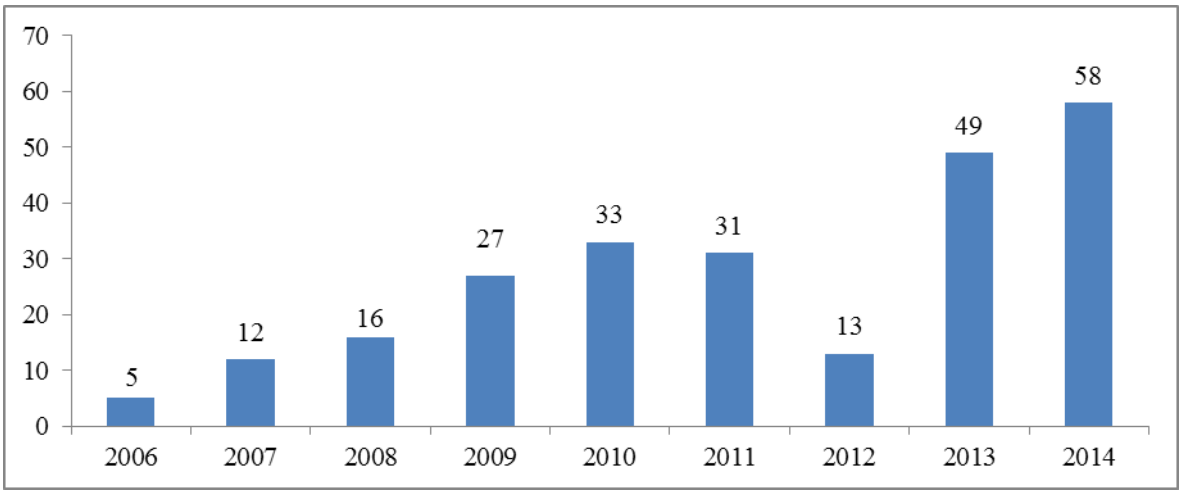
Slika 7: Izdani certifikati ISO/IEC 27001 v odstotkih po regijah sveta v letih 2006–2014



Vir: ISO Survey Report, 2014, tabele s podatki.

Slika 8 prikazuje število izdanih certifikatov ISO/IEC 27001 v Sloveniji.

Slika 8: Število izdanih certifikatov ISO/IEC 27001 v Sloveniji v letih 2006–2014



Vir: ISO Survey Report, 2014, tabele s podatki.

2 TVEGANJA, POVEZANA S KIBERNETSKIMI NEVARNOSTMI

2.1 Kibernetske nevarnosti kot varnostno tveganje in povezava z operativnim tveganjem

V prejšnjem poglavju sem navedla najpogostejše kibernetske nevarnosti, ki pretijo gospodarskim družbam zaradi vse večje medsebojne povezanosti in s tem odvisnosti od

informacijskih sredstev in tehnologij. Nevarnosti, katerim so uporabniki le-teh izpostavljeni, prinašajo različna varnostna tveganja, kot na primer nedelovanje informacijskih sredstev in tehnologije, kraja in zloraba zaupnih podatkov in posledično je lahko bolj ali manj ogrožen poslovni proces gospodarskih družb, ki ga sredstva in tehnologija podpirajo in s tem tudi uspešnost gospodarske družbe.

Tudi definicija operativnega tveganja, kot je opredeljena v okviru režima Solventnosti II, zajema tveganja nastanka škode zaradi neustreznih internih procesov ali odpovedi internih procesov, kot posledica neustreznih aktivnosti zaposlenih ali neustreznega sistema, ali kot posledica zunanjih dogodkov (CEIOPS, 2009, str. 5), kamor torej lahko uvrstimo tudi tveganja, ki jih prinašajo kibernetske nevarnosti.

Operativna tveganja, ki izhajajo iz kibernetskih nevarnosti razvrstita avtorja Cebula in Young (2010, str. 3) na štiri kategorije glede na izvor nevarnosti:

- aktivnosti ljudi:
  - nenamerne aktivnosti
  - namerne aktivnosti
  - odsotnost aktivnosti
- odpovedi sistemov in tehnologij:
  - odpovedi strojne opreme
  - nedelovanje programske opreme
  - odpovedi ostalih sistemov
- odpovedi internih procesov:
  - odpoved postavitve in izvajanja procesa
  - odpoved kontrol procesa
  - odpoved podpornih procesov
- zunanji dogodki kot so:
  - katastrofalni dogodki
  - regulativa
  - poslovni dogodki
  - odvisnost od zunanjih storitev

V nalogi sem opisala nekaj primerov odmevnejših varnostnih incidentov, ki jih lahko umestimo v gornje kategorije in glede na rezultate številnih raziskav globalnih nevarnosti, ki kažejo na porast varnostnih incidentov, tako po številu kot tudi po obsegu. Mnogi varnostni incidenti sodeč po rezultatih raznih raziskav izvirajo iz dejanj zaposlenih, kamor so uvrščene tako nenamerna dejanja, kot so razne napake pri delu, pa tudi zlonamerna dejanja zaposlenih ali celo bivših zaposlenih, nekdanjih poslovnih partnerjev družbe. V okviru varnostnih sistemov zaščite informacijskih sistemov sem v prvem poglavju naloge navedla mednarodne standarde s področja informacijske varnosti, ki so družbam v pomoč

pri obvladovanju tveganj, ki jih kibernetske nevarnosti prinašajo. Obenem zaradi mnogih primerov incidentov, do katerih je prišlo zaradi zlonamerne ali nenamerne aktivnosti zaposlenih pomen operativnih tveganj vse bolj pridobiva na pomenu in se vse več pozornosti namenja upravljanju z njimi, pri čemer je potrebno izpostaviti pomembno lastnost operativnih tveganj, da se jih lahko preko ustreznih internih procesov in kontrol ter ob ustreznem sistemu celovitega obvladovanja tveganj, katerega del je na primer tudi prenos tveganja na drug subjekt (na primer na zavarovalnico), bistveno zmanjša.

2.2 Zavedanje o obstoju kibernetskih nevarnostih in varnostnega tveganja, ki jih prinašajo

World Economic forum od leta 2006 dalje redno letno objavlja poročilo o globalnih nevarnostih, ki temelji na opravljeni raziskavi percepcije o globalnih nevarnostih v sodelovanju s strokovnjaki iz različnih področij ekspertiz (ekonomske, socialne, politične, tehnološke vede). Zadnje poročilo je bilo izdano v letu 2016 in v raziskavi percepcije globalnih nevarnosti, ki je bila izvedena v jeseni 2015, je sodelovalo 742 udeležencev iz različnih držav. Največ iz Evrope (32 %) in Severne Amerike (18 %), sledijo udeleženci iz držav Južne Amerike (13 %), Vzhodne Azije in Pacifika (12,5 %), držav Podsaharske Afrike (8,8 %), držav Bližnjega Vzhoda (6,5 %), Južne Azije (5,9 %), Osrednje Azije in Rusije (2,3 %) ter druge (WEF, 2016, str. 1).

Ocenjevanje se je nanašalo na 29 izbranih globalnih nevarnosti, ki jih lahko razvrstimo v štiri kategorije:

- ekonomske nevarnosti,
- okoljske nevarnosti,
- geopolitične nevarnosti,
- družbene nevarnosti,
- tehnološke nevarnosti.

Kibernetske nevarnosti so umeščene med tehnološke nevarnosti in percepcija udeležencev raziskave po letih od 2007–2016 je pokazala, da so bile kibernetske nevarnosti v tem obdobju med pet največjimi nevarnostmi le v letih 2007, 2012 in 2014. Rezultate moramo ločiti tudi glede na verjetnost nastanka dogodka in glede na učinek dogodka. Če pogledam podrobneje informacijo iz poročila WEF (2016, str. 11), je razvidno, da je bil zlom ključne informacijske infrastrukture na prvem mestu v razpredelnici globalnih nevarnosti glede na verjetnost nastanka dogodka. V letu 2012 so bili v isti razpredelnici na četrtem mestu kibernetski napadi in v letu 2014 so se kibernetski napadi uvrstili na peto mesto po percepciji udeležencev raziskave. Iz razpredelnice razvoja percepcije globalnih rizikov po učinku dogodka je moč razbrati, da so kibernetski riziki umeščeni v omenjenem časovnem

obdobju le enkrat med pet največjih globalnih nevarnosti, in sicer so bili na petem mestu v letu 2014 nevarnosti zloma ključne informacijske infrastrukture.

V raziskavi so udeležence zaprosili za njihovo oceno globalnih nevarnosti v smislu verjetnosti, da se zgodijo in v smislu učinkov. Možne ocene so bile v razponu od 1–7, pri čemer 1 pomeni, da ni verjetno, da bi se nevarnost dejansko uresničila ali imela učinek, 7 pa, da je velika verjetnost, da se nevarnost zgodi in ima močan, celo uničujoč učinek.

V poročilu WEF (2016, str. 11) opredeljuje globalne nevarnosti kot negotov bodoči dogodek, ki, v kolikor do njega pride, povzroči negativni učinek na nacionalna gospodarstva in gospodarske sektorje v naslednjih desetih letih. Na podlagi pridobljenih ocen udeležencev raziskave je bila izračunana povprečna vrednost ocen vseh nevarnosti in ob primerjavi med leti opazimo, da povprečna ocena pri obeh, tako pri verjetnosti nastanka kot tudi pri učinku postopno narašča, največji skok pa je opaziti iz 2014 na 2015. V Tabeli 2 je prikaz gibanja povprečnih ocen po letih 2014–2016, ločeno za verjetnost nastanka in učinek.

Tabela 2: Gibanje povprečne ocene globalnih nevarnosti v letih 2014–2016

	Leto 2014	**Leto 2015**	**Leto 2016**
Verjetnost nastanka dogodka	4,87	4,82	4,31
Učinek dogodka	4,76	4,74	4,56

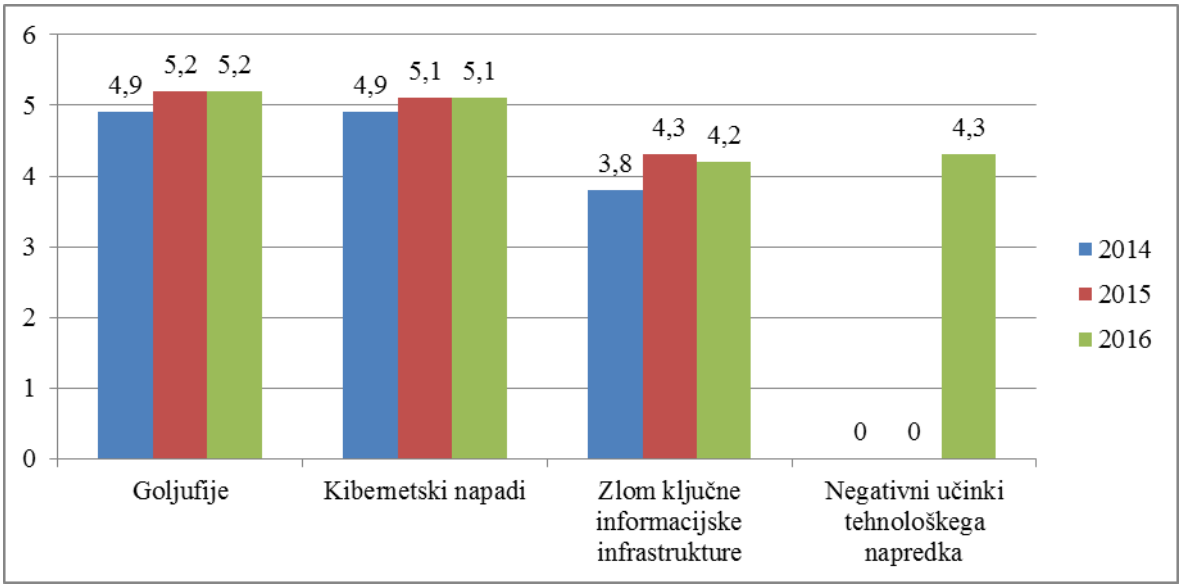
Vir: WEF, Global Risks, 2014, str. 16; WEF, Global Risks 2015, str. 1; WEF, Global Risks 2016, str. 1.

Kibernetske nevarnosti so v poročilu WEF (2016, str. 9) umeščene med tehnološke nevarnosti in v to kategorijo so razporejene naslednje nevarnosti:

- negativne posledice tehnološkega napredka,
- zlom kritične informacijske infrastrukture,
- obsežne varnostne incidente,
- masivne varnostne incidente kraje podatkov oziroma goljufije.

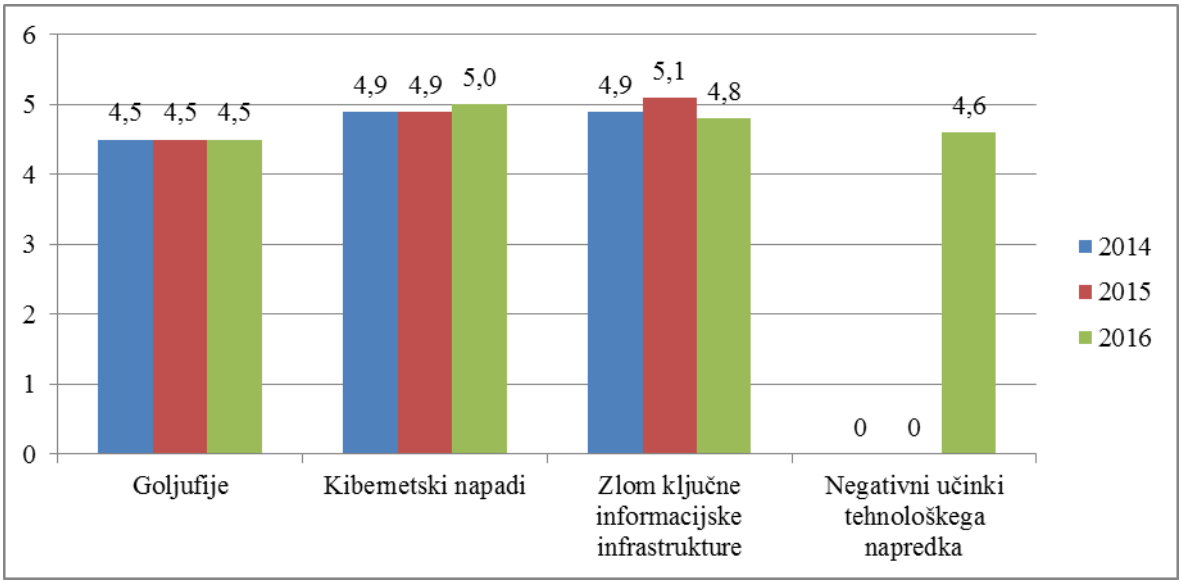
Povprečne ocene zgoraj navedenih kategorij kibernetskih nevarnostih po izvoru po letih 2014–2016 ločeno za verjetnost nastanka in učinek dogodka so prikazane v Sliki 9 in Sliki 10. Pri obeh tabelah je vrednost za negativne učinke tehnološkega napredka prikazana le za leto 2016, ko je bila tudi prvič vključena.

Slika 9: Ocene kibernetskih nevarnosti po izvoru glede na verjetnost nastanka dogodka v letih 2014–2016



Vir: WEF, Global Risks, 2014, str. 16; WEF, Global Risks 2015, str. 1; WEF, Global Risks 2016, str. 1.

Slika 10: Ocene kibernetskih nevarnosti po izvoru glede na učinek dogodka v letih 2014–2016



Vir: WEF, Global Risks, 2014, str. 16; WEF, Global Risks 2015, str. 1; WEF, Global Risks 2016, str. 1.

Poročilo (WEF, 2016, str. 18) navaja, da bo razvoj tehnologij, ki so vezane na internet, po pričakovanjih prinesel družbi največ koristi. Obenem se je potrebno zavedati, da v primeru nerazumevanja nevarnosti, ki jih tehnološki razvoj prinaša, lahko za družbe prinese tudi negativne učinke v velikih razsežnostih. V tej povezavi poročilo nadalje omenja nekaj pomembnih področij nevarnosti, ki se jih morajo gospodarske družbe, oblikovalci politike

in širša družba zavedati, da bodo presegli nevarnosti in iz njih izhajajoča tveganja, ki jih prinaša tehnološki razvoj:

- kibernetske nevarnosti,
- potek izmenjave podatkov,
- spremembe v delovnem okolju,
- večanje neenakosti (neenakomerno porazdeljeno bogastvo, dohodki, socialne neenakosti).

Kibernetske nevarnosti so bile prepoznane v sklopu raziskav WEF v zadnjih letih kot največje po verjetnosti in učinku v Severni Ameriki. Predvsem zaradi napovedanega razmaha ti. interneta stvari (angl. *Internet of things*), ki vodi v še večjo povezanost ljudi in tehnoloških naprav, je po mnenju sodelujočih v raziskavi tretji najpomembnejši trend. Posledično so nevarnosti neke družbe zaradi medsebojne povezanosti povezane z nevarnostmi drugih družb (WEF, 2016, str. 18).

Izmenjava podatkov. Z vse večjo digitalizacijo podatkov in porastom elektronske izmenjave podatkov je izrednega pomena, da je vzpostavljen ustrezen zakonodajni okvir, ki je povečini še nezadostno razvit, predvsem se kritike nanašajo na področja zaupnosti, transparentnosti, intelektualnih pravic (predvsem ob čezmejni izmenjavi in uporabi podatkov).

Spremembe v delovnem okolju. Ob razvoju novih tehnologij se pogosto pojavlja vprašanje, koliko obstoječih delovnih mest bo nadomeščeno z novimi tehnološkimi rešitvami, tj. da ne bo več potrebe po vključitvi človeka za izvajanje določenih delovnih procesov. Poročilo WEF (2016, str. 20) navaja oceno Urada za delovno statistiko iz ZDA, po kateri naj bi bilo do leta 2022 v ZDA 47 % zaposlenih s precejšno verjetnostjo, da je njihovo delovno mesto avtomatizirano (na primer z vključitvijo robotov na določena delovna mesta), kar predstavlja nov izziv za prilagoditev sistemov zaposlovanja.

Večanje neenakosti. Z razvojem novih tehnologij se ocenjuje, da bo neenakost v smislu porazdelitve bogastva, dohodkov in socialna neenakost še večja. Stopnja dostopa do novih tehnologij bo ključni faktor, ki bo še povečal razlike znotraj držav in med državami. Po navedbah WEF (2016, str. 20) je od skupno 7 milijard prebivalcev kar 4 milijarde brez dostopa do interneta, kar posledično pomeni, da se jim bo položaj ob prihodu in uveljavitvi novih tehnologij verjetno še poslabšal. Prevelika neenakost pomeni tudi grožnjo za socialno stabilnost v družbi, kar lahko sproži razmah nasilja in terorizma ter tudi neželeno migracijo. V poročilu WEF (2016, str. 69) so predstavljeni tudi rezultati mnenj vodilnih delavcev, ki jo WEF izvaja že od leta 1979 in predstavlja dodatni pogled k raziskavi percepcije globalnih nevarnosti, ki je bila predstavljena pred tem, z vidika vpliva globalnih nevarnosti na poslovanje gospodarskih družb. Zadnja taka raziskava je bila izvedena spomladi 2015 in v njej je sodelovalo 13.000 vodilnih delavcev iz 140 nacionalnih

gospodarstev. Za izbranih 28 globalnih nevarnosti so podali svoje mnenje, in sicer katerih pet globalnih nevarnosti jim pomeni največjo skrb za naslednjih deset let pri poslovanju v njihovi državi. Nabor 28 globalnih nevarnosti je bil v osnovi vzet iz raziskave percepcije globalnih nevarnosti.

Rezultati raziskave vpliva globalnih nevarnosti na poslovanje gospodarskih družb kažejo po regijah precej različno sliko. V poročilu (WEF, 2016, str. 70) rezultati za Evropo kažejo, da se kibernetske nevarnosti ne pojavljajo med največjimi petimi nevarnostmi, identificiranimi med sodelujočimi iz evropskih držav kot največje nevarnosti za prihodnjih deset let. Se pa pojavijo kibernetski riziki med petimi največjimi nevarnostmi v naslednjih evropskih državah: v Estoniji, Nemčiji, na Nizozemskem, v Švici. Rezultati raziskave za Severno Ameriko so povsem drugačni, saj so udeleženci iz ZDA in Kanade označili kibernetske rizike kot največjo nevarnost v naslednjih desetih letih za gospodarske družbe. Če pogledam še naprej, in sicer katero kategorijo kibernetskih rizikov so udeleženci izpostavili, raziskava navaja, da so v ZDA na prvem mestu varnostni incidenti ter na drugem kraja zaupnih podatkov oziroma goljufija. Udeleženci iz Kanade so na prvo mesto umestili nevarnosti iz naslova cen energentov, na drugo nevarnosti naložbenega balona (angl. *asset bubble*), na tretjem mestu pa so varnostni incidenti. Od drugih regij, navedenih v poročilu WEF (2016, str. 71) bom omenila samo še regijo, ki zajema Vzhodno Azijo in Pacifik, ki na svoji lestvici največjih nevarnosti za poslovanje v naslednjih desetih letih prav kibernetske nevarnosti, konkretneje varnostne incidente umešča na tretje mesto. Na prvem in drugem sta nevarnosti iz naslova cen energentov in nevarnosti naložbenega balona. Zanimiv je še podatek, gledano globalno, vse regije sveta skupaj, da so v raziskavi udeleženci iz le 8 držav (od skupno 140) bili mnenja, da so varnostni incidenti največji izziv za poslovanje gospodarskih družb za prihodnjih 10 let in jih s tem umešča na šesto mesto globalne lestvice.

Tudi v okviru te raziskave WEF (2016, str. 77) z vidika vpliva globalnih nevarnosti na poslovanje gospodarskih družb, je tako kot pri raziskavi percepcije globalnih nevarnosti, izpostavljen internet stvari kot nova tehnološka realnost, ki prinaša nove priložnosti za povečanje učinkovitosti, obenem pa tudi nove nevarnosti zaradi dodatno povečane povezanosti in s tem priložnosti za nove, številčnejše varnostne incidente, usmerjene v gospodarske družbe. Odmevni primeri varnostnih incidentov kažejo na vse bolj kompleksne načine vdorov, ki jih napadalci uporabljajo in se iz leta v leto povečujejo.

WEF želi s pomočjo raziskave prispevati k dvigu zavesti glede obstoja globalnih nevarnosti in dvigu zavesti glede potrebe po ukrepanju v naslednjih smereh:

- okrepitev odpornosti družb za vzdržno poslovanje in uspešno kljubovanje globalnim nevarnostim,
- vzpostavitev sodelovanja med javnim in zasebnim sektorjem z namenom razvoja boljših preventivnih ukrepov s pomočjo vzpostavitve varnostnih standardov tako za

javni kot tudi za zasebni sektor,
- uskladitev mednarodnega pristopa glede vzpostavitve in izvrševanja standardov.

Svetovni gospodarski forum se osredotoča na nevarnosti iz globalne perspektive. V svoji raziskavi glede vpliva globalnih nevarnosti na poslovanje družb poda dodatni pogled, ki je odraz ocene stanja gospodarskih družb, ki se vsakodnevno srečujejo z različnimi nevarnostmi iz okolja in se jim morajo sproti prilagajati, da ohranjajo svoj položaj na trgu. O stopnji zavedanja glede obstoja kibernetskih nevarnosti in z njimi povezanimi tveganji nam veliko pove raziskava, ki jo je izvedel Aon v jeseni 2015 in je zajela 128 klientov Aona iz različnih držav in gospodarskih panog. Vključene so bile tako gospodarske družbe kot tudi zavarovalnice. Z njo so želeli ugotoviti, kako družbe gledajo na kibernetske nevarnosti in kakšen odnos imajo do upravljanja s tveganji, ki jih prinašajo. Zastavljena vprašanja so se osredotočila na naslednje vidike (Aon, 2016, str. 1–4):

- elementi kibernetskih nevarnosti in iz njih izhajajoča tveganja, ki predstavljajo družbam največji izziv,
- ključni faktorji, ki jih družbe upoštevajo pri njihovi oceni potrebnega zavarovalnega kritja,
- percepcija zavarovanja kibernetskih tveganj,
- izbira obsega zavarovalnega kritja kibernetskih tveganj, opredelitev zavarovalnega kritja, proces obdelave škod.

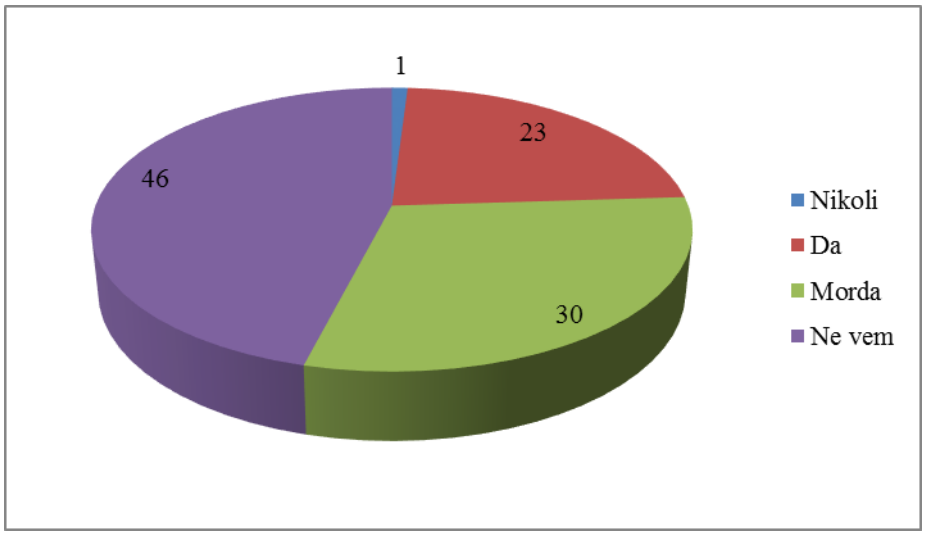
Na podlagi rezultatov raziskave je bil kot glavni prepoznan izziv, ki se nanaša na prekinitev poslovanja kot posledica varnostnih incidentov kršitve zaupnosti podatkov. Materialne škode in telesne poškodbe so udeleženci rangirali zelo nizko z vidika izzivov, ki ga kibernetske nevarnosti prinašajo, vendar je že opaziti porast zavedanja pri obeh, gospodarskih družbah in zavarovalnicah glede možnih nevarnosti, ki jih prinaša razvoj interneta stvari, ki pa trenutno še niso pripoznana v procesih obvladovanja tveganj v družbah in obstoječih kritjih zavarovalnic (Aon, 2016, str. 4). Slika 11 kaže ocene kibernetske nevarnosti po izvoru v letih 2014–2016.

Aon je v svoji raziskavi (2016, str. 14) udeležence povprašal, ali njihova družba uporablja katerega od mednarodnih standardov na področju informacijske varnosti in rezultati so pokazali, da skoraj polovica udeležencev (46 %) ne ve, kako je s tem v njihovi družbi, kar kaže na to, da je skrb za informacijsko varnost v družbah še vedno ločen proces in še vedno pretežno v domeni vodje IT oddelkov, da presojajo o ustreznosti obstoječega informacijskega sistema. Vsled naraščajoče aktualnosti in razsežnosti kibernetskih nevarnosti, ki vplivajo globalno na poslovanje družbe, bi se morali interni procesi v družbah povezati in vključiti tudi zunanjo presojo glede tveganj, ki jih kibernetske nevarnosti za neko družbo prinašajo in obenem presojo ustreznosti in učinkovitosti IT sistema ter nato skupaj poiskati najprimernejšo rešitev. Slika 12 kaže odgovore anketiranih glede zavedanja o uporabi mednarodnih standardov na področju informacijske varnosti.

Slika 11: Ocene kibernetskih nevarnosti po izvoru v letih 2014–2016

Vir: WEF, Global Risks, 2014, str. 16; WEF, Global Risks 2015, str. 1; WEF, Global Risks 2016, str. 1.

Slika 12: Ocena uporabe mednarodnih standardov na področju informacijske varnosti.

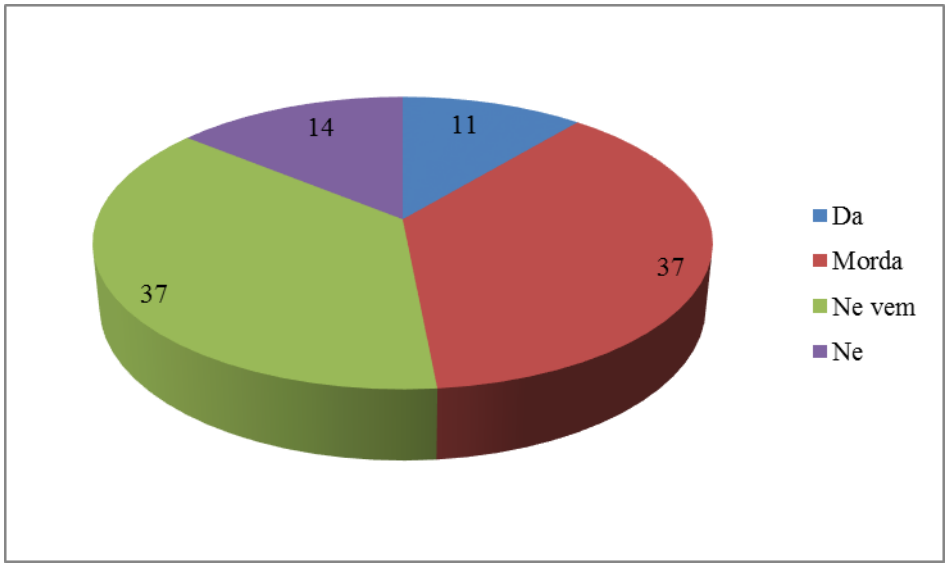


Vir: WEF, Global Risks, 2014, str. 16; WEF, Global Risks 2015, str. 1; WEF, Global Risks 2016, str. 1.

Z raziskavo je Aon (2016, str. 16) skušal priti do mnenj udeležencev glede koristnosti pridobitve ocen kibernetskih tveganj s strani neodvisnih zunanjih specializiranih institucij, ki bi jim bila lahko v pomoč v procesu njihove lastne ocene izpostavljenosti kibernetskim tveganjem. Rezultati kažejo, da slaba polovica udeležencev meni, da bi bila vključitev zunanje institucije v pomoč, druga polovica pa meni, da tega ne potrebujejo, kar je morda tudi posledica tega, da zavest o tveganjih, ki jih kibernetske nevarnosti prinašajo še ni na

zadostni ravni. Slika 13 prikazuje deleže po odgovorih na vprašanje, ali je vključitev zunanje institucije koristna pri oceni izpostavljenosti.

Slika 13: Koristnost vključitve zunanje institucije za oceno izpostavljenosti



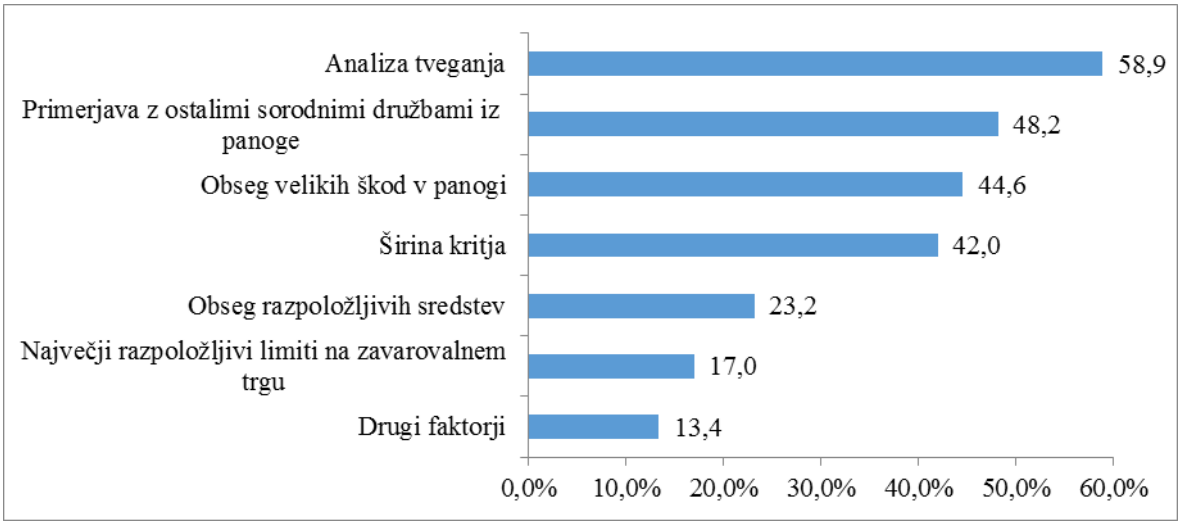
Vir: WEF, Global Risks, 2014, str. 16; WEF, Global Risks 2015, str. 1; WEF, Global Risks 2016, str. 1.

Družbe se različno lotevajo svoje ocene potrebnega zavarovalnega kritja. Iz raziskave Aona (2016, str. 12) izhaja, da približno 59 % udeležencev svojo oceno temelji na analizi tveganj, kar je še vedno nizek odstotek glede na dejstvo, da so kibernetske nevarnosti pripoznane kot hitro razvijajoče in naraščajoče nevarnosti in so za obvladovanje izhajajočih tveganj potrebni napredni analitični pristopi. Pri večjih družbah, s prihodki nad 5 milijardami USD pa se je ta odstotek odrazil na višjem nivoju, v višini približno 67 %. Slika 14 kaže, na podlagi katerih elementov anketiranci bazirajo njihovo odločitev glede potrebne višine zavarovalnega kritja.

Glede percepcije zavarovanja kibernetskih tveganj je raziskava Aona (2016, str. 18) pokazala, da 68 % družb sklene zavarovanje zaradi zaščite njihovih bilanc, takoj za tem pa je uvrščen motiv zadostitve zahtevam skladnosti. Slika 15 kaže odgovore udeležencev glede vzrokov za nakup zavarovalnega kritja.

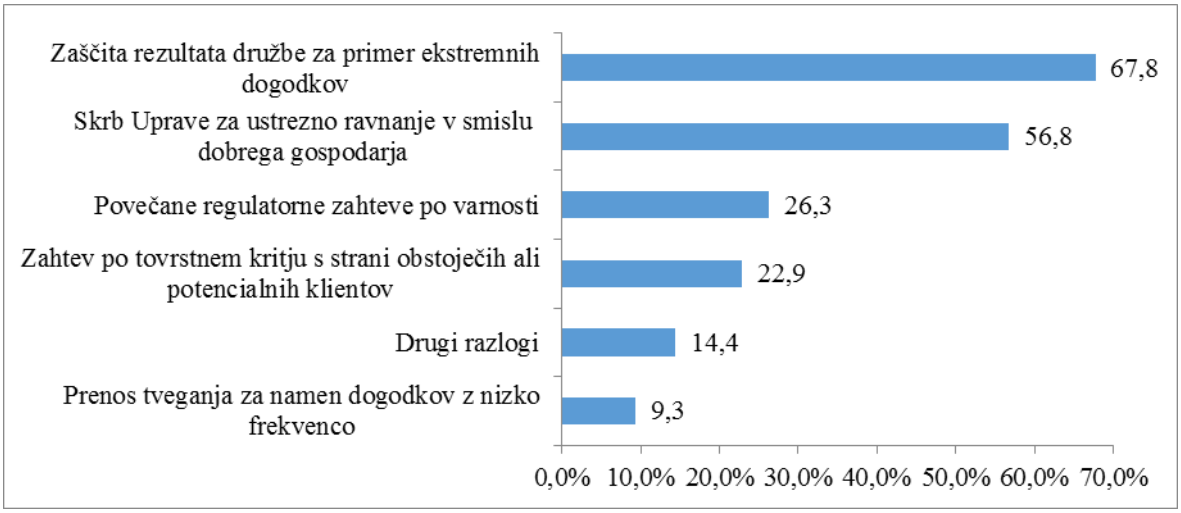
Nadalje so rezultati pokazali, da 60 % velikih družb nima sklenjenega zavarovanja kibernetskih tveganj. Vpogled v gospodarski sektor udeležencev pokaže, da zavarovanje sklene 70 % družb iz sektorja, kjer imajo opravka z veliko podatki in le 17 % družb iz sektorja kritične infrastrukture. To napotuje na sklep, da kljub daljši časovni prisotnosti zavarovanja kibernetskih tveganj na tujih zavarovalnih trgih, to kritje še ni dozorelo. Slika 16 kaže, koliko družb udeležencev ima sklenjeno zavarovanje.

Slika 14: Elementi, ki vplivajo na oceno potrebnega zavarovalnega kritja



Vir: WEF, Global Risks, 2014, str. 16; WEF, Global Risks 2015, str. 1; WEF, Global Risks 2016, str. 1.

Slika 15: Vzroki za sklenitev zavarovanja kibernetskih tveganj



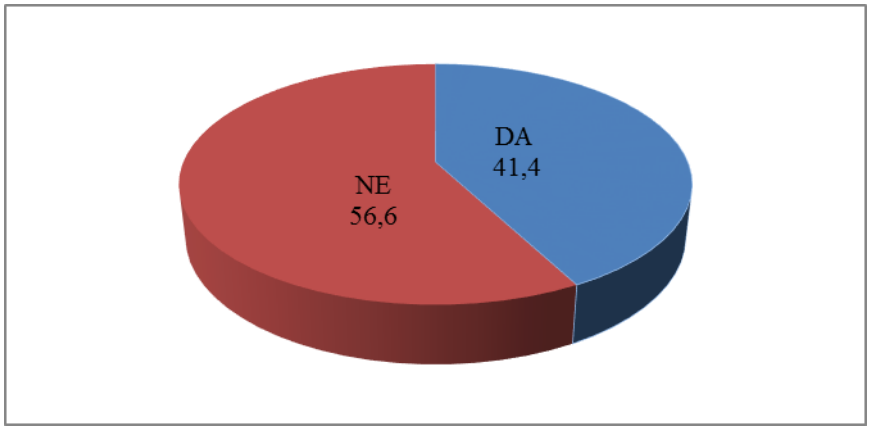
Vir: WEF, Global Risks, 2014, str. 16; WEF, Global Risks 2015, str. 1; WEF, Global Risks 2016, str. 1.

Na vprašanje v raziskavi Aona (2016, str. 22), ali imajo družbe v svojih finančnih virih predvidena sredstva za zavarovanje kibernetskih tveganj, jih je le 47 % odgovorilo pritrdilno, kar kaže na to, da zavedanje o pomenu zavarovanja kibernetskih tveganj še ni doseglo želenega nivoja. Slika 17 kaže delež družb udeležencev z oziroma brez vnaprej določenih sredstev za zavarovanje.

Udeleženci raziskave (Aon, 2016, str. 24) so pri vprašanju glede zavarovalnega kritja, ki trenutno obstaja na zavarovalnem trgu, izpostavili kot najpomembnejši element pogoje zavarovanja (71 % sodelujočih), takoj za tem pa ceno zavarovanja (48 % sodelujočih). To kaže na to, da je pomembno usmeriti dodatne aktivnosti za razumevanje zavarovalnega

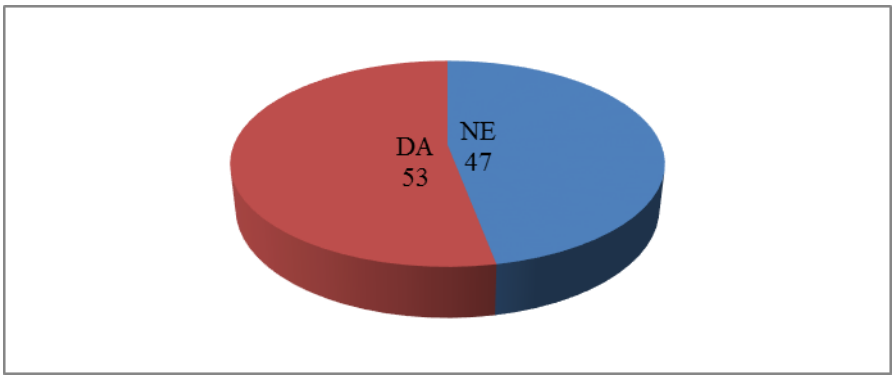
kritja in pogojev, da bi razvoj tega zavarovanja dosegel nov razmah. Med ostalimi elementi zavarovanja je smiselno omeniti še višino kritja, ki so ga kot pomemben element izpostavili udeleženci večjih družb, medtem ko je za manjše pomemben škodni proces, kot kažejo rezultati raziskave. Slika 18 kaže elemente zavarovanja, ki so po mnenju udeležencev raziskave najpomembnejši.

Slika 16: Delež družb brez oziroma s sklenjenim zavarovanjem kibernetskih tveganj



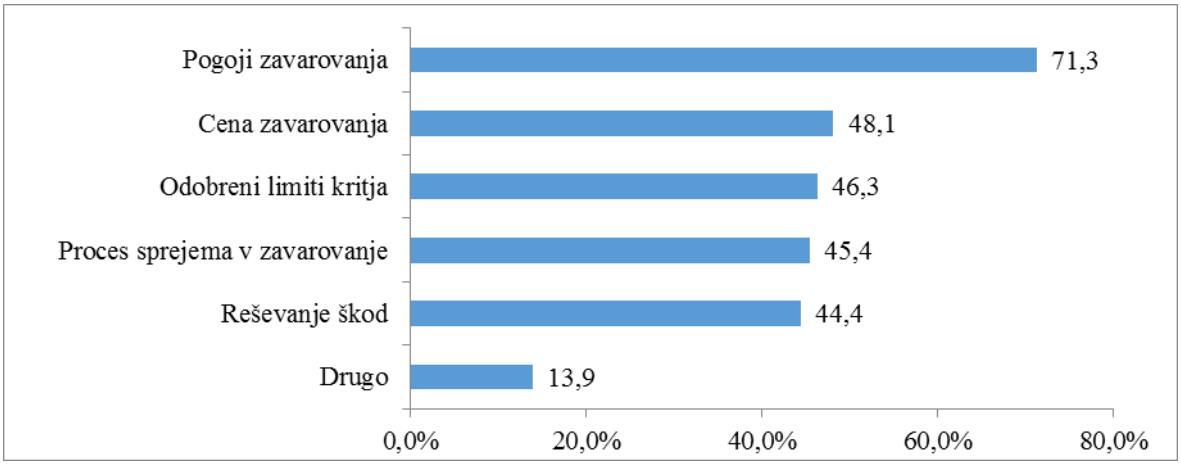
Vir: WEF, Global Risks, 2014, str. 16; WEF, Global Risks 2015, str. 1; WEF, Global Risks 2016, str. 1.

Slika 17: Delež družb brez oziroma z vnaprej določenimi finančnimi sredstvi za zavarovanje



Vir: WEF, Global Risks, 2014, str. 16; WEF, Global Risks 2015, str. 1; WEF, Global Risks 2016, str. 1.

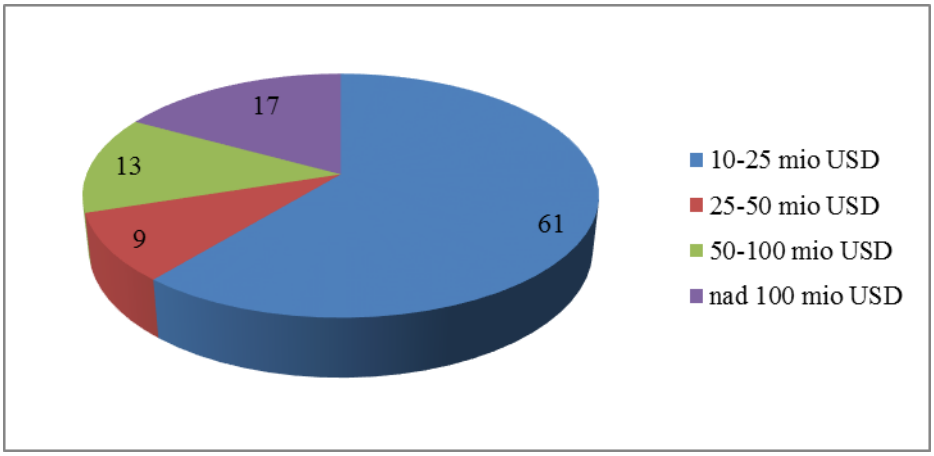
Slika 18: Prikaz najpomembnejših elementov zavarovanja



Vir: WEF, Global Risks, 2014, str. 16; WEF, Global Risks 2015, str. 1; WEF, Global Risks 2016, str. 1.

Glede izbrane višine kritja je največ udeležencev raziskave (Aon, 2016, str. 26) izbralo limit v rangu 10–25 milijonov USD (61 %), kar je nizko v primerjavi z izpostavljenostmi. Samo 17 % udeležencev je izbralo limit nad 10 milijonov USD in večinoma gre za družbe iz kritične infrastrukture. Slika 19 kaže strukturo zavarovanj s prikazom deležev po višini limitov kritja.

Slika 19: Višine limitov kritja za katere se odločajo zavarovanci

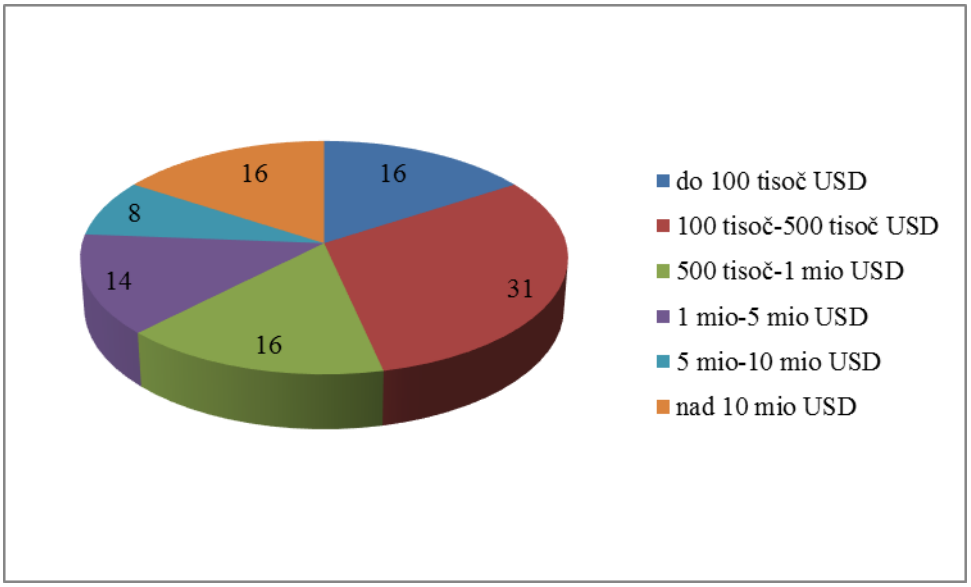


Vir: WEF, Global Risks, 2014, str. 16; WEF, Global Risks 2015, str. 1; WEF, Global Risks 2016, str. 1.

Udeležbe družb v prevzetih tveganjih, torej zneski, ki jih zadržijo v lastnem deležu oziroma samopridržaju, so sodeč po odgovorih udeležencev raziskave Aona (2016, str. 28) zelo različni. V povprečju so največkrat izbrani lastni deleži v višini med 100.000 USD in 500.000 USD in med udeleženci raziskave iz manjših družb je kar 46 % takih. Pri večjih družbah je slika drugačna; 28 % jih je izbralo lastni delež v višini nad 10 milijonov USD, 24 % v rangu med 1 milijonom USD in 5 milijonov USD. Različne izbire napotujejo na negotovost, ki jo udeleženci povezujejo z učinkom kibernetskih nevarnosti na njihovo

poslovanje. Glede na razmah kibernetskih nevarnosti bi se v prihodnosti lahko zgodilo, da bi zavarovalnice od zavarovancev zahtevale višje lastne udeležbe v tveganjih. Slika 20 kaže deleže po višini izbranih samopridržajev zavarovancev pri nakupu zavarovanja.

Slika 20: Višine izbranih samopridržajev zavarovancev



Vir: WEF, Global Risks, 2014, str. 16; WEF, Global Risks 2015, str. 1; WEF, Global Risks 2016, str. 1.

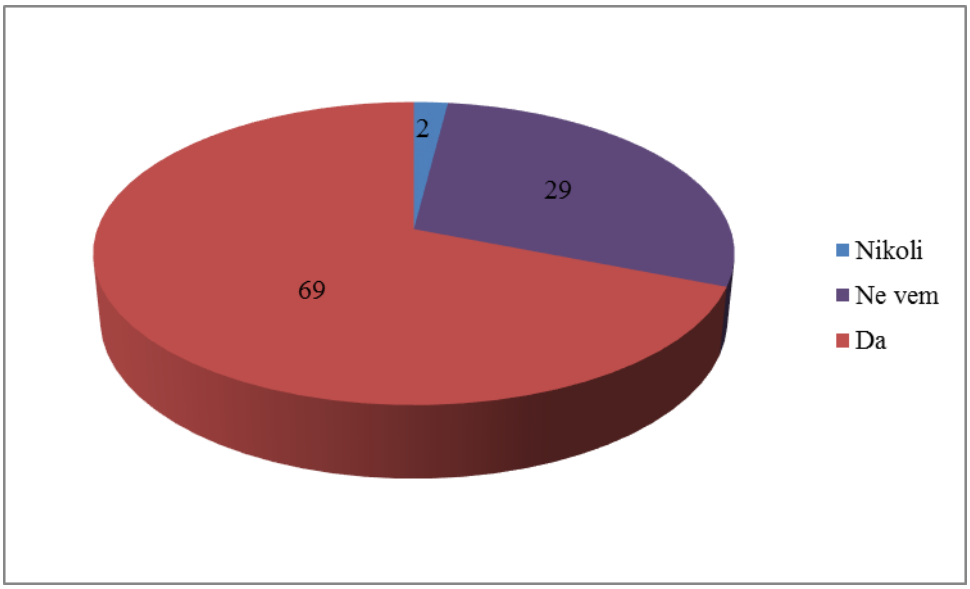
69 % udeležencev raziskave je v zvezi s procesom reševanja kibernetskih škod glede na podane odgovore precej negotovih glede primernosti sedaj uveljavljenega procesa obdelave škod v primeru kibernetskih tveganj in dvomijo v sposobnost zavarovalnic, da ga prilagodijo kompleksnosti kibernetskih nevarnosti (Aon, 2016, str. 36). Slika 21 kaže zbrane odgovore glede korektnosti obdelave in izplačila škod zavarovalnic (z deleži po tipu odgovora).

Njihova negotovost izvira predvsem iz vprašanja interpretacije kritja in zavarovalnih pogojev, kar je jasno razvidno tudi iz odgovorov udeležencev na vprašanje glede tega, kaj bi bilo potrebno najprej zagotoviti za ustrezen škodni proces reševanja škod. 94,4 % udeležencev je na prvo mesto postavilo jasno, transparentno besedilo zavarovalne pogodbe (Aon, 2016, str. 38). Slika 22 kaže elemente, ki so po mnenju udeležencev ključni za ustrezen proces reševanja škod.

Zanimivi so tudi rezultati raziskav Allianza iz let 2014–2016, s katerimi so zbrali mnenja iz srednje velikih in velikih družb, mnenja svetovalcev za tveganja, ocenjevalcev tveganj in specialistov za oceno škod iz Allianza. Raziskave so zajele več kot 30 držav (zadnja raziskava v 2016 je zajela 44 držav) in več kot 400 udeležencev (v letu 2016 je bilo več kot 800 udeležencev). V raziskavi so udeleženci navedli dva gospodarska sektorja, na katera se najbolj spoznajo in navedli tri največje nevarnosti, katere so se jim zdele po njihovem

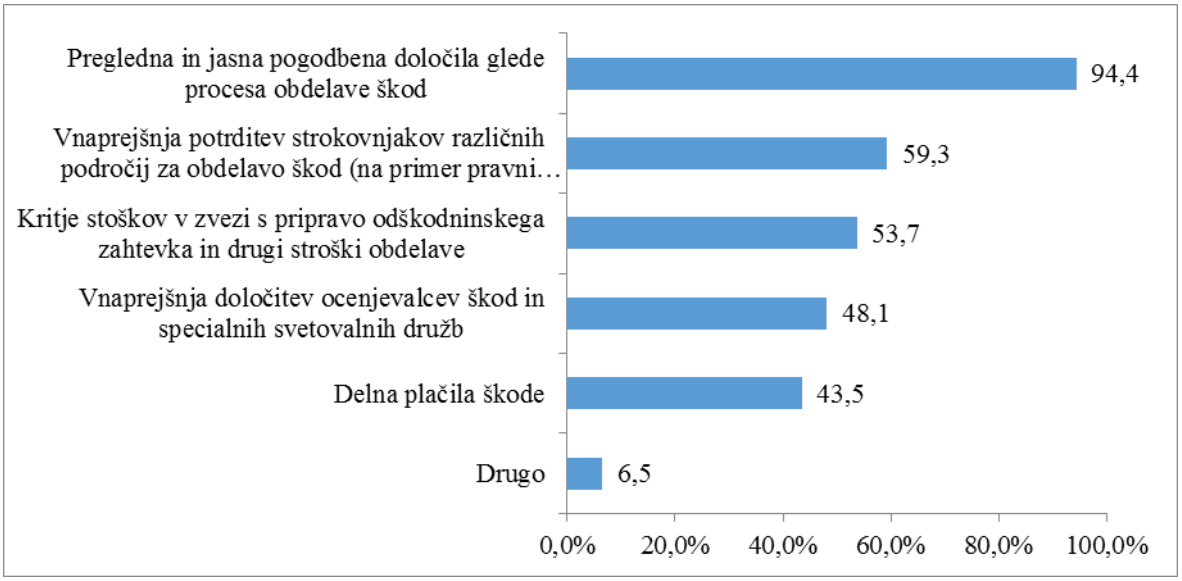
mnenju najpomembnejše za družbe. V komentarju rezultatov se za namen te naloge osredotočim na kibernetske nevarnosti in kako so bile umeščene na seznam največjih nevarnosti po letih.

Slika 21: Odgovori udeležencev glede njihove skrbi glede korektnosti obdelave in izplačila škode



Vir: WEF, Global Risks, 2014, str. 16; WEF, Global Risks 2015, str. 1; WEF, Global Risks 2016, str. 1.

Slika 22: Ocene kibernetskih nevarnosti po izvoru v letih 2014–2016



Vir: WEF, Global Risks, 2014, str. 16; WEF, Global Risks 2015, str. 1; WEF, Global Risks 2016, str. 1.

Skupni rezultat vseh anketirancev po letih je pokazal, da se kibernetske nevarnosti s časom uvrščajo vse višje na lestvici najpomembnejših nevarnosti, kar kaže na povečevanje

zavedanja družb glede pomembnosti kibernetskih nevarnosti za njihovo poslovanje. Tabela 3 prikazuje umestitev kibernetskih nevarnosti po doseženih mestih glede pomembnosti ter delež udeležencev, ki so umestili kibernetske nevarnosti med najpomembnejše.

Tabela 3: Kibernetske nevarnosti po doseženem mestu glede na pomembnost za družbe z deleži udeležencev v letih 2014–2016

	2014	**2015**	**2016**
Doseženo mesto na lestvici Top 10 nevarnosti	8. mesto	5. mesto	3. mesto
Delež udeležencev (v %)	12	17	28

Vir: Allianz Global Corporate & Specialty, Allianz Risk Barometer 2014, str. 1; Allianz Global Corporate & Specialty, Allianz Risk Barometer 2015b, str. 1; Allianz Global Corporate & Specialty, Allianz Risk Barometer 2016, str. 1.

Raziskava Allianza nadalje pokaže razvrstitev rezultatov tudi po regijah sveta, kar je prikazano v Tabeli 4, ki vsebuje podatke o doseženem mestu kibernetskih nevarnosti po posamezni regiji s pripadajočim deležem udeležencev. V regiji Azija, Pacifik in Avstralija so bile kibernetske nevarnosti uvrščene med Top 10 najpomembnejših nevarnosti za družbe šele v letu 2016. Evropa ter Bližnji vzhod in Afrika so bile v raziskavi ločeno prikazane prvič v 2016.

Tabela 4: Kibernetske nevarnosti po doseženem mestu glede na pomembnost za družbe in deleži udeležencev v letih 2014–2016

	2014		**2015**		**2016**	
	Mesto na lestvici	**Delež udeležencev (v%)**	**Mesto na lestvici**	**Delež udeležencev (v%)**	**Mesto na lestvici**	**Delež udeležencev (v%)**
Evropa, Bližnji vzhod in Afrika	9	11	4	20	/	/
Evropa					3	40
Bližnji vzhod in Afrika					5	30
Severna in Latinska Amerika	8	11	4	25	2	46
Azija, Pacifik in Avstralija	/	/	/	/	5	32

Legenda: / kibernetske nevarnosti niso bile uvrščene med Top 10.

Vir: Allianz Global Corporate & Specialty, Allianz Risk Barometer 2014, str. 6; Allianz Global Corporate & Specialty, Allianz Risk Barometer 2015b, str. 2; Allianz Global Corporate & Specialty, Allianz Risk Barometer 2016, str. 2.

Če pogledam še odgovore udeležencev na nekatera vprašanja iz raziskave Allianza, je razbrati, da se udeleženci zavedajo pomanjkljivosti družb, ki kažejo na premajhno razumevanje kibernetskih rizikov in obenem se zavedajo potencialnih nevarnosti za

njihovo poslovanje. V letu 2016 je prekinitev poslovanja že četrto leto zapored na vrhu lestvice kot najpomembnejša nevarnost za poslovanje družbe. V letu 2016 so udeležencem zastavili vprašanje, katere nevarnosti bodo v prihodnosti predstavljale nevarnost za nastanek dogodka prekinitve poslovanja in 59 % jih je bilo mnenja, da bodo to kibernetske nevarnosti, na drugem mestu pa globalizacija in medsebojna povezanost (52 % udeležencev).

Na podlagi dosedanjih izkušenj SI-CERT ob varnostnih incidentih v Sloveniji kaže, da so večje družbe že začele razmišljati v smeri nujnosti po vzpostavitvi učinkovitega notranjega sistema informacijske varnosti, medtem ko se male in srednje velike družbe po njihovem mnenju še vedno ne zavedajo dobro, da so kibernetske nevarnosti in z njimi povezana tveganja postala realnost in da je potrebno sistematično pristopiti k iskanju rešitev za zagotavljanje informacijske varnosti družbe. SI-CERT se preko obravnave varnostnih incidentov srečuje z družbami, jim pomaga pri reševanju incidenta, opozarja na novo nastale spletne mehanizme in tehnike, ki jih napadalci uporabljajo pri svojih aktivnostih ter strokovno svetuje glede možnih smeri vzpostavitve informacijske varnosti. Zaskrbljujoča je informacija SI-CERT (2015, str. 40), da se je v letu 2015 prvič zgodilo (gledano od leta 2008 dalje), da je zabeleženo večje število goljufij in prevar kot tehničnih napadov. Pri goljufijah in prevarah gre predvsem za izsiljevalske viruse, »phishing« napade, prevare pri spletnem nakupovanju in druge goljufije, ki pravzaprav ne zahtevajo od napadalca visokega tehnološkega znanja, temveč izkoriščajo povezave preko socialnih omrežij in to kaže na trenutno nizko stopnjo osveščenosti slovenskih uporabnikov interneta.

V začetku februarja 2016 je bila v Sloveniji sprejeta strategija kibernetske varnosti, s katero bo Slovenija okrepila svoj sistem zagotavljanja kibernetske varnosti preko različnih ukrepov, ki jih strategija opredeljuje. Med ukrepi so svoje mesto dobili tudi programi za osveščanje državljanov in družb ter spodbujanje razvoja in vpeljave novih tehnologij na področju kibernetske varnosti (Strategija kibernetske varnosti, 2016, str. 11), kar je dodatni signal, da kibernetske nevarnosti terjajo resno obravnavo na vseh nivojih in pri vseh subjektih družbe.

2.3 Ekonomske razsežnosti in stroškovni vidik varnostnih incidentov

Poročila različnih institucij so si enotna v stališču, da so kibernetske nevarnosti v porastu in podatki raziskav to jasno kažejo. Narašča število, razsežnost in tudi stroški odprave posledic varnostnih incidentov. V poročilu ENISE (2015, str. 7) je prepoznan trend rasti incidentov, vezanih na zlonamerno kodo, različnih načinov vdorov v sistem z namenom pridobitve oziroma razkritja podatkov, vohunjenja in izsiljevanja. Pretežno se incidenti nanašajo na kibernetski kriminal oziroma na zlonamerna dejanja napadalcev, zato je tudi v literaturi najti predvsem podatke o ocenah ekonomskih učinkov tovrstnih varnostnih incidentov. Po ocenah poročila McAfee & CSIS (2014, str. 2) je ocena stroška za globalno svetovno ekonomijo v višini 400 milijard USD (pri tem je minimalna ocena podana v

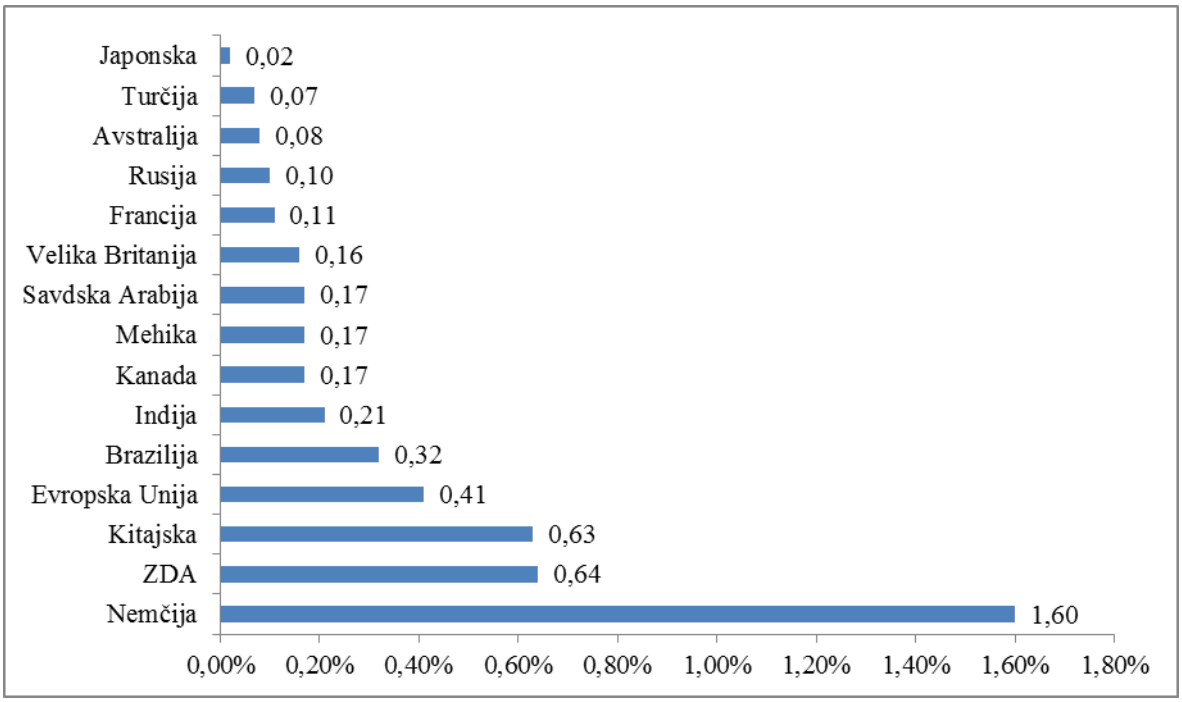
višini 375 milijard USD in maksimalna v višini 575 milijard USD). McAfee & CSIS v svojem poročilu (2014, str. 5) navajata, da se večina učinka zlonamernih napadov odrazi na državah skupine G20, in sicer je skupna ocena škode za štiri največje države te skupine (ZDA, Kitajska, Japonska, Nemčija) v višini 200 milijard USD in glede na napovedi, bo ta znesek še bistveno zrasel glede na razmah internetnega poslovanja, razvoja mobilnih platform in drugih novih tehnologij. Zanimiva je tudi ocena deleža škod iz naslova zlonamernih kriminalnih napadov od bruto družbenega produkta (v nadaljevanju BDP), ki temelji na raziskavi McAfee & CSIS (2014, str. 8–9), kjer so izvedli intervjuje z različnimi državnimi institucijami po državah, z Evropsko komisijo ter mnogimi specializiranimi institucijami za kibernetske nevarnosti. V okviru raziskave so se med državami pokazale precejšnje razlike pri ocenjevanju zneskov škod, kar so pokazale tudi druge raziskave. Vsem pa je bilo skupno, da so v ZDA zneski izgube najvišji. Nadalje je potrebno omeniti tudi razhajanja pri podatkih za posamezne evropske države in Evropsko Unijo, kar še dodatno potrjuje problem celovitosti in verodostojnosti podatkov o incidentih in posledično vpliv na nezanesljivost podanih ocen ekonomskih učinkov incidentov.

Bogatejše države so logična izbira za napadalce, vendar druge države po predvidevanjih ne bodo zaostajale, predvsem na račun hitrega globalnega prenosa tehnologij, tu so mišljene predvsem mobilne platforme, kjer so kibernetski napadi v porastu, predvsem v državah v razvoju. Kar se tiče povezanosti, so mobilne platforme prva izbira, zato je moč pričakovati porast kibernetskih napadov tudi tam. Slika 23 prikazuje stroške zlonamernega kriminala v deležu od BDP po državah skupine G20. Izrazito odstopanje v primerjavi z ostalimi državami je opaziti pri Japonski (0,02 %) ter v drugo smer pri Nizozemski (1,5 %) in Nemčiji (1,6 %), kar McAfee & CSIS v poročilu pojasnjujeta z razlikami med uporabljenimi metodologijami ocen stroškov škod po državah, obenem pa tudi s težavami pri pridobivanju podatkov od družb po državah. Informacija iz Japonske je izpostavila tudi vpliv nerazumevanja japonskega jezika kot njihovo naravno varovalko pred napadi in tudi zato posledično tako nizek delež ocenjenih stroškov.

Slika 24 prikazuje stroške zlonamernega kriminala v deležu od BDP po državah izven skupine G20.

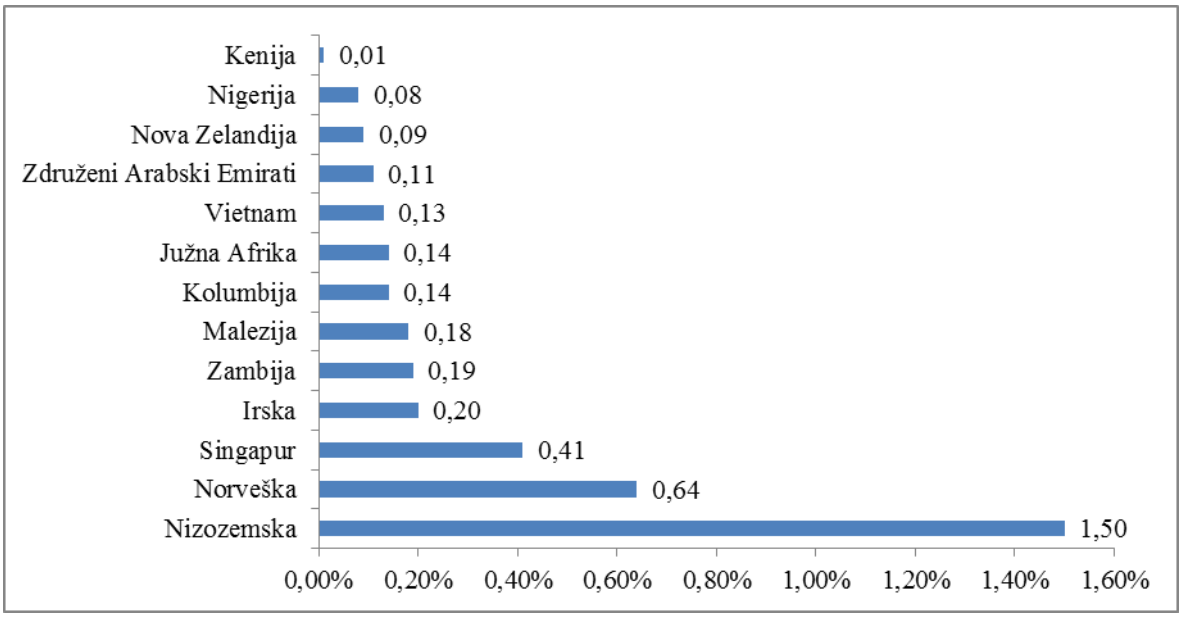
Pri oceni stroškov varnostnih incidentov in vpliva na nacionalno ekonomijo trčimo na vprašanje merjenja in ovrednotenja, kar je v neposredni povezavi z razpoložljivimi podatki o incidentih. Pomanjkanje informacij tako glede zadostnega števila verodostojnih podatkov o incidentih, kot tudi vprašanje metodologije ovrednotenja, je še vedno eno bistvenih vprašanj, s katerim se ukvarjajo različni IT specialisti, zavarovalnice in raziskovalne institucije, zato je težko priti do točnega zneska, s časom pa se razvijajo pristopi, ki omogočajo vedno boljše ocene. Pomembna pri tem je tudi vloga države, ki lahko preko regulative vpliva na sistemsko poročanje o varnostnih incidentih in s tem omogoči verodostojno podlago vsem deležnikom pri svojem delovanju.

Slika 23: Deleži stroška kibernetskega kriminala od BDP po državah skupine G20



Vir: McAfee & CSIS, Net Losses: Estimating the Global Cost of Cybercrime, 2014, str. 9.

Slika 24: Deleži stroška kibernetskega kriminala od BDP po državah izven skupine G20



Vir: McAfee & CSIS, Net Losses: Estimating the Global Cost of Cybercrime, 2014, str. 9.

Primerjava je podana v poročilu (McAfee & CSIS, 2014, str. 11) tudi z deleži drugih vrst kriminala in škod in je prikazana v Tabeli 5.

Tabela 5: Deleži stroška po vrsti aktivnosti v deležu od BDP

Aktivnost	Strošek v % od BDP
Pomorsko piratstvo	0,02 (globalno)
Mednarodni kriminal	1,20 (globalno)
Ponarejanje	0,89 (globalno)
Kraje	1,50 (ZDA)
Avtomobilske nesreče	1,00 (ZDA)
Narkotiki	0,90 (globalno)
Kibernetski kriminal	0,80 (globalno)

Vir: McAfee & CSIS, Net Losses: Estimating the Global Cost of Cybercrime, 2014, str. 11.

McAfee & CSIS (2013, str. 8) sta se v svojem poročilu lotila ocene ekonomske škode varnostnih incidentov na način, da sta ločila zlonamerne aktivnosti na več vrst po tipu dejanja:

- kraja intelektualne lastnine in zaupnih informacij,
- kibernetski kriminal,
- kraja zaupnih poslovnih informacij s komponento potencialne manipulacije na kapitalskih trgih,
- oportunitetni stroški vezani na incident, vključno z vplivom na delovanje družbe in njenih zaposlenih,
- dodatni stroški glede sistemske zaščite, nakupa zavarovanja, obnove v prvotno stanje,
- škoda povzročena ugledu družbe.

Med naštetimi v poročilu McAfee & CSIS (2013, str. 8) ocenjujeta, da največja škoda nastane v primerih kraje intelektualne lastnine in zaupnih informacij ter kraje zaupnih poslovnih informacij. Pri obeh je poseben izziv postaviti verodostojno oceno, kar je posledica včasih nejasne ločnice med tem, kaj je opredeljeno kot intelektualna lastnina in kaj kot pomembna, zaupna poslovna informacija ter tudi zaradi neslutenih razsežnosti, ki jih tak incident lahko ima.

Pri kraji intelektualne lastnine lahko pri oceni škode na primer izhajamo iz prihodkov, ki jih na primer nek proizvod prinaša in pričakovanih prihodkov, ki jih bo prinesel v prihodnosti. Obenem je potrebno poudariti še časovno komponento te izgube, tj., da lahko preteče precej časa med nastankom incidenta in trenutkom, ko se na primer na trgu pojavi produkt kot produkt konkurenta, kar pomeni, da je učinek kraje lahko takojšen (oziroma v kratkem času po incidentu), v kolikor gre za tak produkt, da ga lahko konkurent hitro postavi na trg, ali pa šele čez dalj časa, torej lahko mine tudi več let. V kolikor gre za situacijo, ko dalj časa ni učinka, je vprašanje, če se oškodovana družba sploh zaveda, da je prišlo do kraje in v tem primeru sploh ne more postaviti ocene škode za nekaj, za kar sploh nima registrirane izgube. Če na primer predpostavimo, da je bil v ozadju za napadom

konkurent (torej lahko govorimo o ekonomskem vohunjenju), je posledica take kraje konkurentova predstavitev novega produkta ali vsaj znižanje stroška konkurenta, ki ga nameni za raziskave in razvoj. Dodatno lahko konkurentova prednost postane še večja, če ima na voljo državne subvencije ali zaščitno politiko države, ki drugim postavlja vstopne prepreke in s tem znižajo konkurenčnost vstopnim družbam. Zgodovinsko gledano na pretekle incidente, so bile nemalokrat v ozadju tudi države, ki so imele interes za pridobitev raznih vojaških informacij ali informacij vezane na napredne tehnologije (McAfee & CSIS, 2013, str. 10–11).

Kraja pomembnih zaupnih poslovnih informacij ima za razliko od kraje intelektualne lastnine takojšen učinek na poslovanje oškodovane družbe. Tak primer je lahko na primer kraja insiderske informacije, ki jo lahko napadalec takoj vnovči na kapitalskih trgih. Drugi pa s krajo pomembne informacije lahko prepreči na primer sklenitev nekega posla.

V poročilu McAfee & CSIS (2014, str. 3) navajata, da ima varnostni incident kriminalnega dejanja v razvitih država močan vpliv na zaposlenost. Zaradi kraje intelektualne lastnine lahko na primer družba utrpi tako veliko škodo zaradi oslabljenega položaja na trgu, da pride celo do krčitve števila zaposlenih. Za ZDA je v poročilu McAfee & CSIS navedena ocena, da bi ta vpliv lahko znašal upad v višini 200.000 delovnih mest, kar bi bilo približno 1 % upad stopnje zaposlenosti. Enaka ocena za Evropo pravi, da bi bil učinek incidenta lahko upad približno 150.000 delovnih mest, kar bi pomenilo približno 0,6 % nižjo stopnjo zaposlenosti. Stopnja zaposlenost vpliva naprej na prihodke na nacionalni ravni, kar verjetno kaže na to, da so ocene stroškov varnostnih incidentov podcenjene.

Poročilo McAfee & CSIS (2013, str.10) glede **kibernetskega kriminala** izpostavlja predvsem napade z namenom pridobitve dostopa do finančnih sredstev posameznikov in druge oblike goljufije. Po ocenah United Nations Office on Drugs and Crime (v nadaljevanju UNODC) se največji strošek nanaša na krajo identitete in to znaša po njihovi oceni letno okoli 1 milijardo USD na globalnem nivoju (McAfee & CSIS, 2013, str. 10).

Podatki glede drugih finančnih stroškov niso dostopni, UNODC (v McAfee & CSIS, 2013, str. 10) pa nadalje omenja, da se po njihovi oceni incidentov v ZDA, letni strošek giblje med 300 milijoni USD in 500 milijoni USD in povečini finančne institucije smatrajo ta strošek kot strošek poslovanja, čeprav sploh ni zanemarljiv.

Tudi napadi z učinkom zavrnitve storitve in izsiljevalski napadi v smislu blokade dela sistema napadene družbe, glede na poročilo McAfee & CSIS (2013, str. 10) nima pomembnejših učinkov na nacionalno ekonomijo. Predstavlja pa seveda večjo ali manjšo motnjo za družbo, ter določene stroške povezane s povrnitvijo v prvotno stanje.

Glede »phishing« napadov so ocene stroškov večih raziskav zelo različne in se gibljejo od 178 milijonov USD na letnem nivoju po raziskavi Univerze Cambridge (v McAfee &

CSIS, 2013, str. 11) do 2 milijardi USD letno, kar je spet dokaz o različnih predpostavkah ocenjevanja stroškov incidentov.

Oportunitetni stroški varnostnega incidenta predstavljajo vrednost izpadlih aktivnosti in priložnosti družbe na račun stroškov, ki jih je povzročil incident. Naslednji so stroški, ki opredeljujejo učinke kibernetskega kriminala (McAfee & CSIS, 2014, str. 17): znižane investicije v raziskave in razvoj, povečane investicije v zaščito svojega sistema, tvegana uporaba interneta. V velikih družbah je največji strošek znesek, ki ga investirajo v zaščito svojega informacijskega sistema, kar kaže ne le na povečano rabo interneta, temveč tudi na nivo zavedanja glede kibernetskih nevarnosti. Po navedbah poročila McAfee & CSIS (2014, str.7) se preko internetnega poslovanja ustvari približno 2–3 bilijone USD in obseg še narašča. Po ocenah poročila Mc Afee & CSIS (2014, str. 7) kibernetski kriminal predstavlja med 15 % in 20 % prihodkov internetnega poslovanja, kar tudi lahko gledamo kot eden od vidikov ocene oportunitetnih stroškov.

Stroški, povezani s povrnitvijo v prvotno stanje se v času povečujejo, še posebej, če govorimo o napadih z goljufijami in kraji podatkov. V teh primerih sicer po dosedanjih podatkih napadalci ne bodo dosegli finančnega učinka v celoti, v primeru kraje intelektualne lastnine pa mora družba predpostaviti in ravnati tako, kot da bi napadalci lahko v celoti izpolnili finančni učinek. Učinek varnostnega incidenta ima lahko učinek v obliki **izgube ugleda** na primer blagovne znamke in ugleda na splošno in se odrazi v slabšem odnosu s strankami in pogosto pride do javnih objav z objavo namere povrnitve določenih stroškov partnerjem in strankam. Posledično lahko družbe utrpijo tudi znižanje vrednosti na kapitalskih trgih, ki po ocenah poročila (McAfee & CSIS, 2014, str. 18) lahko znaša med 1 % in 5 %. Poročilo omenja pomembne elemente, ki bi lahko bistveno vplivali na izboljšanje položaja družbe v tem primeru. Poudarek je na uporabi najboljših praks in standardov glede zaščitnih sistemov in vzpostavitvi regulative glede poročanja incidentov.

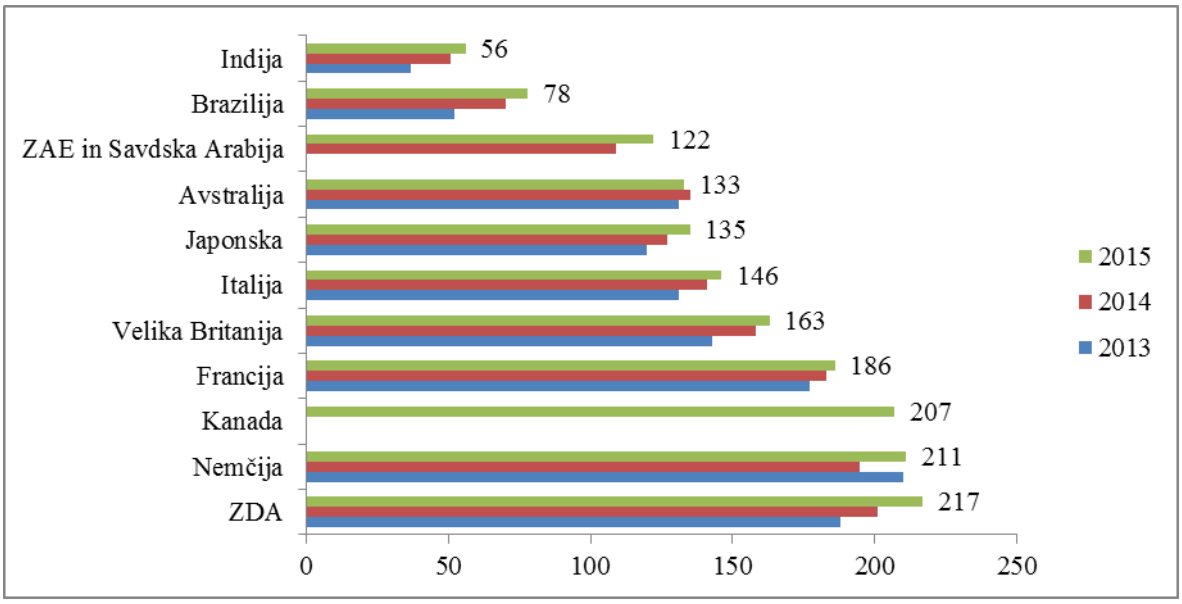
Z vidika obravnave varnostnega incidenta z namenom neavtoriziranega dostopa do podatkov, njihovo razkritje in/ali zloraba, bi omenila študijo IBN in Inštituta Ponemon, ki temelji na izkušnjah strokovnjakov za IT, skladnost in informacijsko varnost iz 350 družb iz 11 držav na podlagi izkušenj incidentov. V poročilu raziskave je nekaj zanimivih izsledkov odgovorov sodelujočih glede skupnih stroškov družbe, stroškov po ogroženem podatku, pomenu vključitve uprave družbe v proces izbire varnostne strategije družbe in načinov ublažitve stroškov preko mehanizma zavarovanja, ki jih predstavim v nadaljevanju.

Slika 25 prikazuje povprečni strošek na enoto razkritega podatka po državah v obdobju 2013–2015. Konsolidiran povprečni znesek stroška na enoto razkritega podatka za vse države je znašal 154 USD, v raziskavi preteklega leta je bil ta v višini 145 USD. Državi z najvišjim zneskom sta ZDA (217 USD) in Nemčija (211 USD), najnižji je ta strošek v Indiji (56 USD) in Braziliji (78 USD).

V Sliki 26 je prikazan povprečni skupni strošek razkritja podatkov družbe v obdobju 2013–2015, iz katere je razvidno, da je bil v obravnavanem obdobju največji porast v ZDA, sledi ji Nemčija. Zneskovno so stroški spet najnižji v Indiji in Braziliji.

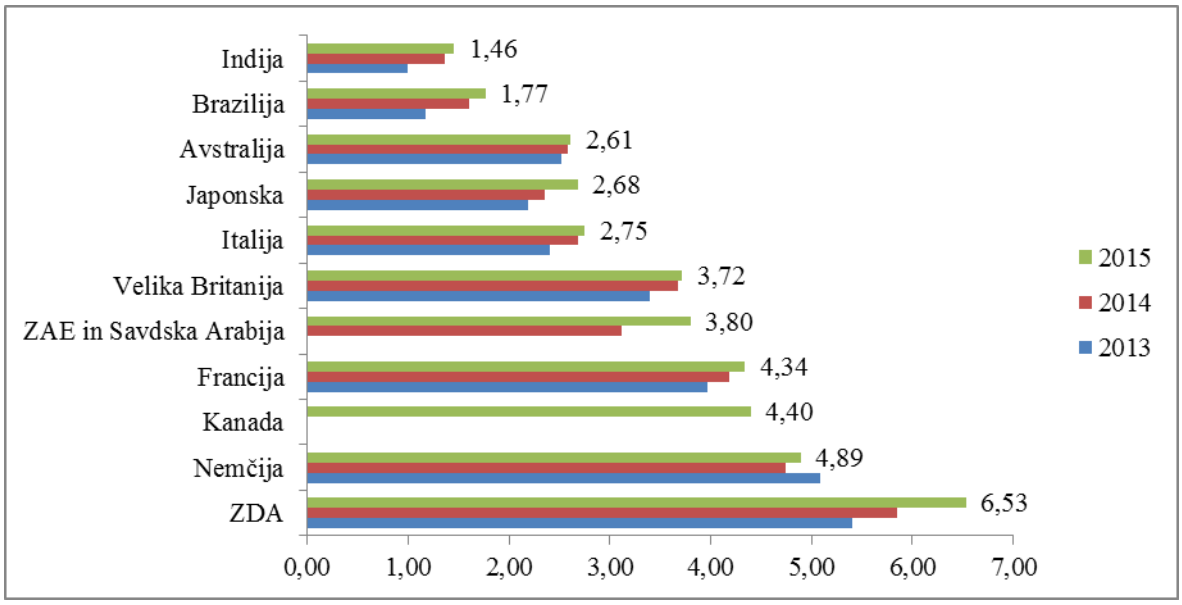
V sliki 27 je razporeditev varnostnih incidentov, zajetih v raziskavi (Ponemon Institute, 2015, str. 10) glede na vir izvora. Zlonamerni oziroma kriminalni napadi predstavljajo največji delež globalno. V primeru kriminalnih napadov je povprečni strošek na enoto razkritega podatka 170 USD (leto prej 159 USD), kar je bistveno več kot so vrednosti stroška razkritja enote podatka zaradi sistemske napake (142 USD), kamor so uvrščene napake IT sistema in procesne napake ter zaradi človeške napake (137 USD), kamor spadajo tako zaposleni kot tudi pogodbeni partnerji.

Slika 25: Povprečni strošek na enoto razkritega podatka v USD v obdobju 2013–2015



Vir: Ponemon Institute, 2015 Cost of Data Breach Study: Global Analysis, 2015, str. 5.

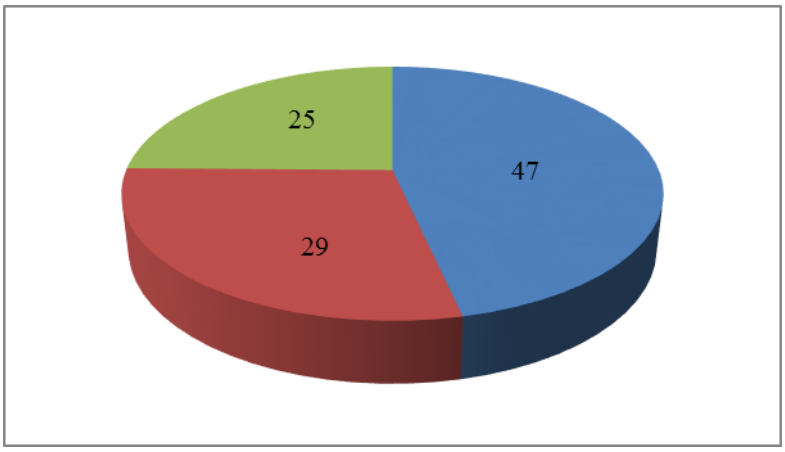
Slika 26: Povprečni skupni strošek družbe iz naslova razkritja podatkov v mio USD v obdobju 2013–2015



Vir: Ponemon Institute, 2015 Cost of Data Breach Study: Global Analysis, 2015, str. 7.

SI-CERT v svojem poročilu (2015, str. 23; 2014, str. 15) navaja, da v Sloveniji glede na prijavljene incidente izhaja, da je v porastu povprečni strošek oškodovanca pri spletni goljufiji in sicer je v letu 2014 znašal 500 evrov (v nadaljevanju EUR), v 2015 pa 1.140 EUR.

Slika 27: Delež napadov z namenom razkritja podatkov glede na vir izvora v letu 2015



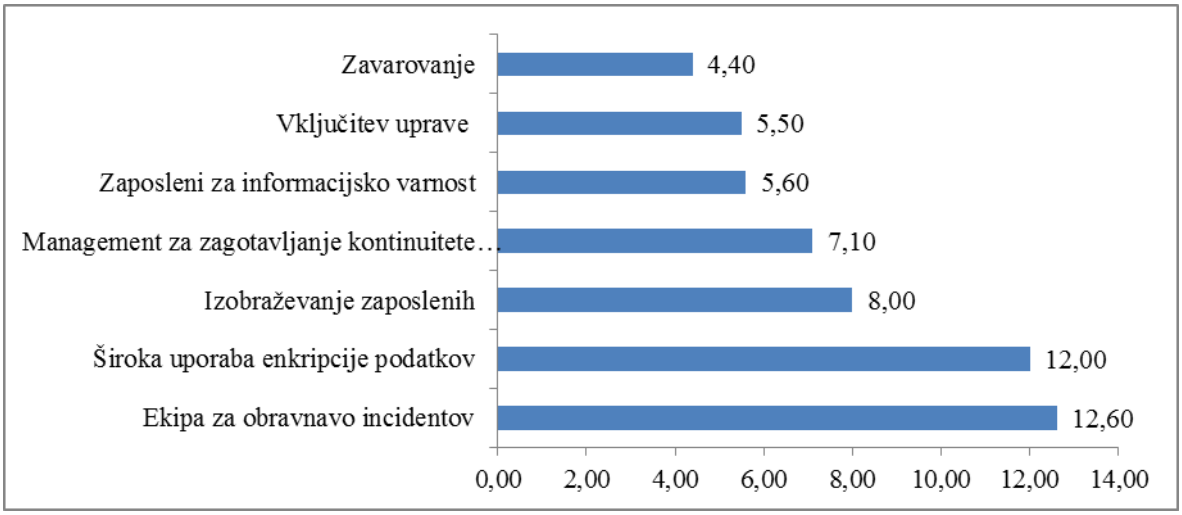
Legenda: modra: zlonamerni ali kriminalni napad; rdeča: sistemska napaka; zelena: človeška napaka

Vir: Ponemon Institute, 2015 Cost of Data Breach Study: Global Analysis, 2015, str. 10.

Raziskava je preverjala tudi izkušnje anketiranih družb glede faktorjev, ki vplivajo na povprečni strošek enote razkritega podatka. Od navedenih 11 faktorjev je 50 %

udeležencev pripisalo največji pomen pri vplivu na strošek izobraževanju zaposlenih, 50 % udeležencev vključenosti uprav družb v primeru nastanka varnostnega incidenta. 48 % udeležencev je umestilo pomen vzpostavitve ekipe za obvladovanje varnostnih incidentov na tretje mesto, 45 % je bilo takih, ki so umestili imenovanje zaposlenega za informacijsko varnost na četrto mesto in na petem mestu je bil uvrščen faktor široke uporabe enkripcije podatkov, zanj je glasovalo 44 % udeležencev. Iz rezultatov raziskave nadalje izhaja tudi, da vključenost uprav, ekipa za obvladovanje incidentov, široka uporaba enkripcije podatkov, zaposleni za informacijsko varnost, uprava družbe za zagotavljanje kontinuitete poslovanja in nakup zavarovalnega kritja vplivajo na znižanje stroška incidenta, medtem ko drugi faktorji kot so vključitev svetovalcev ter ostalih tretjih oseb v incident in izgube/kraje informacijskih sredstev ne vplivajo na znižanje stroška, ampak ga povečujejo. V Sliki 28 je prikaz finančnega učinka na znižanje stroška razkritja enote podatka v USD po posameznem faktorju.

Slika 28: Pozitivni finančni učinek v USD na višino stroška razkritja enote podatka po faktorjih



Vir: Ponemon Institute, 2015 Cost of Data Breach Study: Global Analysis, 2015, str. 13.

Iz prikazanih rezultatov raziskav je razvidno, da gre predvsem za ocene ekonomske škode in je še vedno težko oceniti vrednost učinka incidenta na poslovanje družbe in identificirati vse možne smeri učinkov, zato v tem trenutku težko govorimo o verodostojnih ocenah, kljub temu, da gre za raziskave, ki so jih izvedle renomirane institucije. So pa vsekakor indikator razsežnosti incidentov, kar se je v nekaterih dejanskih primerih incidentov tudi pokazalo kot realni scenarij. Zanimivo je tudi, da nekateri vidijo kibernetske nevarnosti kot običajni strošek poslovanja, ki je vezan na internetno poslovanje kot nekaj samoumevnega, vendar se ti verjetno ne zavedajo možnih razsežnosti incidentov in morda tudi še niso imeli lastne izkušnje z incidentom. Za dosego verodostojnih podatkov o ekonomskih učinkih varnostnih incidentov je zato izrednega pomena uveljavitev regulative glede poročanja incidentov.

3 OBVLADOVANJE TVEGANJ, POVEZANIH S KIBERNETSKIMI NEVARNOSTMI

3.1 Razvoj ustrezne strategije obvladovanja varnostnih tveganj

Znano je dejstvo, da zaščita, ki jo nudijo različni varnostni sistemi, ki vključujejo zaščitne zidove, protivirusne programe, kriptografiranje in druge tehnike zaščite, kljub nenehnemu razvoju in izboljševanju nikoli ne more biti popolna, kar dokazujejo varnostni incidenti. In poleg tega je kljub tehnološkemu razvoju opazen trend rasti varnostnih incidentov in včasih se zdi, da so kibernetski napadalci ves čas v prednosti. Najodmevnejši varnostni incidenti so bili pretežno posledica širitve virusov, vgradnje zlonamernih kod, razkritja zaupnih podatkov. Mnogo je tudi takih incidentov, ki se nanašajo na dejanja notranjih zaposlenih in pogosto niso niti evidentirani, zato je pomembno, da pri vzpostavitvi sistema informacijske varnosti v družbi vključimo vsa področja in vse nivoje družbe s ciljem vzpostavitve učinkovitega notranjega procesa obvladovanja kibernetskih tveganj.

V literaturi so izpostavljeni štirje stebri kot temelj učinkovitega obvladovanja kibernetskih tveganj (CRO Forum, 2014, str. 3): priprava, zaščita, odkritje in izboljšanje.

Priprava pomeni sistematično razdelati možne izvore kibernetskih tveganj in opredeliti, katere so kibernetske nevarnosti, ki lahko pretijo družbi in katere so ključni sistemi in ključni podatki za njeno poslovanje. Verizon (2016, str. 22) je opredelil devet izvorov kibernetskih nevarnosti, ki so se pokazala kot stalno ponavljajoči se vzorec preko njihovih raziskav varnostnih incidentov zadnjih nekaj let. Iz njihovih rezultatov izhaja, da je 90 % varnostnih incidentov posledica sledečega:

- napada z učinkom zavrnitve storitve,
- vgradnje zlonamerne programske opreme,
- kraje ali izgube informacijskega sredstva, podatkov,
- zlorabe pooblastil (interna zloraba s strani zaposlenih),
- različnih nenamernih napak,
- napada na spletne strani,
- kibernetskega vohunjenja,
- vdora v POS terminale z namenom kraje podatkov na prodajnih mestih,
- namestitve snemalnih naprav z namenom kraje podatkov iz bančnih kartic.

S proučitvijo gornjih in ob upoštevanju še drugih, za družbo relevantnih nevarnosti, zgradi družba profil tveganj, za katera pripravi različne scenarije incidentov, ki bi lahko družbo prizadeli tako z vidika njenih ključnih sistemov kot tudi z vidika ključnih podatkov in oceni verjetnost nastanka ter učinek na poslovanje družbe. Nato na tej osnovi določi sprejemljiv nivo tveganja, ki ga lahko sama zadrži. Pri tem je pomembno, da so vključeni

vsi ključni procesi družbe, ki se testirajo preko različnih scenarijev (CRO Forum, 2014, str. 14). Nadalje v prispevku CRO Forum poudarja, da so v prvi vrsti za učinkovit sistem obvladovanja kibernetskih tveganj pomembni zaposleni družbe, ki se dnevno srečujejo na primer s sumljivo elektronsko pošto, spletnimi stranmi in je potrebno vlagati v sprotno izobraževanje glede obstoječih kibernetskih nevarnosti in načinov prepoznave le-teh. Služba za upravljanje s tveganjem vedno bolj dobiva na pomenu, saj je ključno gonilo za izvajanje zastavljenih procesov, spremljanje njihove učinkovitosti in po potrebi dopolnjevanje. Služba za upravljanje s tveganji mora vpeljati sistem obvladovanja tveganj na način, da celovito zajame vse ključne procese družbe, skrbi za osveščenost zaposlenih vseh nivojev glede možnih nevarnosti in razumevanje le-teh ter vplivov na poslovanje družbe.

Zaščita. Družba mora zagotoviti zanesljive sisteme glede nadzora dostopov do informacijskih sistemov in sredstev družbe, sisteme nadzora delovanja zaščite sistemov in sisteme procesov zaščite podatkov (CRO Forum, 2014, str. 14). Pri tem je mišljen tako vidik notranjih zaposlenih kot tudi zunanjih partnerjev, na primer preko pogodb o izločenih poslih. Nadalje kot pomembno izhodišče vzpostavitve sistema obvladovanja kibernetskih tveganj avtorji Pace, Shapella in Vernaci (2015, str. 11) izpostavljajo vzpostavitev in vzdrževanje sistemske higiene v družbi, ki se odraža preko naslednjega:

- vzdrževanje popisa informacijskih sredstev,
- vzdrževanje popisa programske opreme,
- razvoj in zagotavljanje varne konfiguracije vseh naprav sistema,
- kontinuirno izvajanje ocene ranljivosti sistema družbe in njegova sanacija,
- aktivno upravljanje in nadzor nad uporabo pravic za administriranje sistema.

Za dobro zaščito je potrebno najprej imeti opredeljena ključna sredstva za poslovanje družbe, opredeliti možne kibernetske nevarnosti in možne vire, torej od kod in kdo so možni kibernetski napadalci. To omogoči družbi, da ustrezno pripravi načrt obrambe in odziva na kibernetski napad. Na podlagi profila možnih scenarijev napadov družba oceni obstoječe sisteme zaščite in jih glede na profilirane nevarnosti prilagodi in dopolni. Zaradi kontrole učinkovitosti postavljene zaščite je vsekakor priporočljivo tudi testiranje odpornosti, kar se lahko izvede le s simulacijo napadov. Po navedbah CRO Foruma (2014, str. 15) so se v nekaterih državah že začeli pogovori med zakonodajnimi organi in specialističnimi organizacijami glede uvedbe ti. etičnega »heking« testiranja, kar bi se lahko razvilo v učinkovit način testiranja odpornosti sistemov družb proti pretečim kibernetskim nevarnostim, ki jih je vedno več in so še naprej v porastu in jim zato posamezna družba sama v celoti težko sledi. Nadalje je potrebno jasno opredeliti procese glede prepoznave in odziva na varnostni incident. Preko izobraževalnih programov v družbi se zaposleni seznanijo z možnimi nevarnostmi in razumejo tveganja, ki jih prinašajo in so zato sposobni incident prepoznati, če do njega pride. Prav tako mora biti vnaprej

pripravljen tudi načrt odziva na incident, kjer je potrebno zajeti sledeče (CRO Forum, 2014, str. 16):

- opredelitev postopkov v primeru eskalacije incidenta,
- načrt komuniciranja z upravo družbe, javnostjo,
- načrt odziva na incident glede na vrsto kibernetskega napada in časovni okvir odziva
- načrt transparentnega protokola za identifikacijo napada, ranljivosti ter za čim hitrejšo povrnitev v prvotno stanje,
- opredelitev scenarijev za testiranje potencialnih nevarnosti za namen kontrole postopkov načrta odziva na incident in za namen rednega testiranja.

Odkritje. Je izredno pomemben steber v procesu obvladovanja kibernetskih tveganj, saj lahko pravočasna zaznava anomalij lahko prepreči varnostni incident ali ga vsaj omeji. V ta namen mora družba vzpostaviti ustrezne mehanizme za spremljanje informacijskih sredstev in zaznati anomalije in nevarnosti, ki jim pretijo. Spremljava zajema na primer preverjanje internetne pošte za slučaj »spam« pošte s škodljivimi priponkami, spremljava obnašanja zaposlenih z namenom preprečitve notranjih zlorab podatkov. Izobraževanje lahko bistveno doprinese k osveščanju zaposlenih in njihovi pozornosti ob prejemu sumljive pošte ter tudi ob »phishing« napadih, kjer zaposleni lahko že sami preprečijo vdor, če so ustrezno informirani.

Izboljšanje. Družbe si morajo na osnovi lastnih izkušenj z varnostnimi incidenti zgraditi bazo podatkov, ki naj vsebuje poleg večjih incidentov tudi manjše in take, ki so se skoraj zgodili (angl. *near-miss incidents*). Tovrstni podatki so dragoceni vir, ki družbi razkriva ranljivosti in so osnova za izboljšave in nadgradnjo obstoječega sistema obvladovanja kibernetskih tveganj. Na podlagi preteklih incidentov dobi družba tudi informacijo o poteku procesa povrnitve v prvotno stanje in za to potrebnem času in ji je v pomoč pri izboljšavah obstoječih procesov (CRO Forum, 2014, str. 17).

Družbe morajo pri vzpostavitvi sistema obvladovanja kibernetskih tveganj najprej opredeliti nabor njenih ključnih sredstev in ključnih nevarnosti, ki jim je izpostavljena ter vzpostaviti celoviti sistem obvladovanja kibernetskih tveganj, ki bo zaobjel vse nivoje družbe in mora biti fleksibilen in sproti prilagajati procese glede na lastne izkušnje, spremembe v okolju in naravo tveganj. Poleg tehnološkega razvoja je vedno bolj pomemben tudi človeški faktor, zato je izrednega pomena stalna skrb za izobraževanje zaposlenih za dvig osveščenosti in pomena kibernetskih nevarnosti, da bo družba lahko zagotavljala visok nivo informacijske varnosti in dosegala svoje strateško zastavljene cilje.

3.2 Možni načini za prenos tveganja na druge subjekte

Za doseganje čim višje stopnje informacijske varnosti ima tako poleg vzpostavitve celovitega sistema obvladovanja varnostnih tveganj in iskanja optimalnih tehnoloških

rešitev pomembno vlogo tudi prenos tveganja, ki se sproti prilagaja razvoju družbe, njenim potrebam in tveganjem, s katerimi se sooča pri svojem poslovanju.

V literaturi so navedeni štirje načini obvladovanja tveganj (Majuca, Yurcik, & Kesan, 2006, str. 2–3):

- izognitev tveganju,
- zadržanje tveganja,
- zmanjšanje tveganja,
- prenos tveganja v zameno za neko ceno.

Prvi način je v realnem življenju praktično neizvedljiv, ker pomeni, da se kibernetskim tveganjem izognemo na način, da nismo vezani na uporabo računalnikov, interneta. Druga možnost pomeni, da se družba odloči kibernetsko tveganje zadržati, kar pomeni, da sprejema morebitno škodo, ki bi lahko nastala in sprejema tudi izhajajoče učinke na poslovanje družbe. Pri tem se takoj pojavi vprašanje, kakšen obseg teh učinkov je za družbo dejansko ekonomsko sprejemljiv in mogoč. Tretja možnost pomeni, da družba obvladuje kibernetska tveganja na način, da vzpostavi proces, preko katerega s pomočjo ljudi in tehnologije zaznava nevarnosti, oceni iz njih izhajajoča tveganja in sprejema ustrezne ukrepe za njihovo obvladovanje oziroma zmanjševanje (ker je dejstvo, da se družbe tovrstnim tveganjem ne morejo v celoti ogniti), kar sem podrobno opisala v predhodnem poglavju. Četrta možnost je prenos kibernetskega tveganja na tretjo osebo, za namen naloge bom govorila o prenosu na zavarovalnico za ceno premije.

Običajno se družbe odločijo za neko kombinacijo gornjih načinov in s tem optimirajo svoj strošek obvladovanja kibernetskih tveganj.

Smolka (v Eling & Wirfs, 2016, str. 31) navaja pet nosilcev tveganja:

- lastnik tveganja,
- zavarovalnica,
- pozavarovalnica,
- kapitalski trgi,
- država.

Lastnik tveganja običajno preko svojih notranjih procesov upravljanja s tveganji oceni svojo sposobnost glede zadržanega obsega tveganja. V svetu so uveljavljena interesna združenja, ti. »pooli« in ta izraz bom uporabljala tudi naprej v nalogi, ker je tudi sicer razširjen in se uporablja v zavarovalniški stroki. Uveljavljeni so ti. zasebni »pooli«, ki delujejo na način, da se več lastnikov združi in s tem zagotovijo medsebojno delitev tveganj in diverzifikacijo. Obstajajo tudi »pooli« na nivoju gospodarskega sektorja, ki so

običajno večji in imajo več članov kot zasebni »pooli« in tudi postavljajo neke osnovne minimalne standarde varnostne zaščite.

Druga možnost je nakup zavarovanja. Po navedbah avtorjev Bijelić, Jerovšek in Novak (1998, str. 3) različne definicije zavarovanja v bistvu govorijo o zavarovanju kot zaščiti gospodarstva pred določenimi nevarnosti, ki predstavljajo grožnjo premoženju in osebam. Pri zavarovanju gre za sklenitev zavarovalne pogodbe med zavarovancem in zavarovalnico, poimenovano tudi kot primarni zavarovatelj. Pri sklenitvi zavarovanja za kritje kibernetskih tveganj je običajno sklenjena ločena zavarovalna pogodba, nekatera kibernetska tveganja pa so vključena tudi v okviru drugih zavarovalnih kritjih kot na primer zavarovalno kritje prekinitve poslovanja, kjer je krita tudi prekinitev poslovanja zaradi varnostnega incidenta vdora v informacijski sistem družbe. Tudi zavarovalnice se lahko povezujejo v »poole« in to je značilno predvsem v primerih izredno velikih nevarnosti. Vse članice so udeležene na prevzetem tveganju in skupaj dogovorijo pogoje prevzema tveganja, ki veljajo za vse članice »poola«. Na ta način se poveča kapaciteta zavarovalnega kritja (ki bi bila sicer nižja, v kolikor bi vsaka zavarovalnica delovala zase), slabost pa je v tem, da so vse članice zavezane k enakim pogojem, morda pa bi lahko posamezna članica dosegla zase boljše pogoje, v kolikor bi delovala izven poola. Primer zavarovalnega »poola« v Sloveniji je nuklearni »pool«. Zavarovalnice pa včasih v primeru ekstremnih ali neobičajnih/nestandardnih nevarnosti sklenejo tudi sozavarovalni dogovor z drugo zavarovalnico in vsakič ob aktualnem primeru potrebe po sozavarovanju dogovorita pogoje sprejema tveganja.

Zavarovalnice svoje presežke tveganj običajno prenesejo na pozavarovalnico, kar dejansko pomeni, da je pozavarovalnica zavarovalnica zavarovalnice. Po Bijeliću et al. (1998, str. 327) je pozavarovanje opredeljeno kot zavarovanje presežkov, ki jih je zavarovalnica prevzela v zavarovanje in ki presegajo njeno lastno izravnavo. Ker gre za prevzem tveganj od primarnega zavarovatelja, govorimo o sekundarni porazdelitvi tveganj. Pri pozavarovalni pogodbi gre za pravni odnos med zavarovalnico (cedent) in pozavarovalnico in pozavarovalnica nima direktnega odnosa z zavarovanci. Po obliki sklepanja ločimo pozavarovalne pogodbe na obligatorne in fakultativne, po načinu sklepanja pa na sorazmerne (proporcionalne) in nesorazmerne (neproporcionalne) (Bijelić et al., 1998, str. 327). V kolikor se zavarovalnica odloči za nakup pozavarovalnega kritja za njen celotni zavarovalni portfelj, govorimo o obligatornem pozavarovanju, kjer se medsebojno dogovorita, da so avtomatsko vsa tveganja dogovorjenega portfelja sprejeta oziroma cedirana v pozavarovanje. Fakultativno pozavarovanje se običajno nanaša na pozavarovanje individualnih tveganj, ki odstopajo od ostalega portfelja in terjajo individualno obravnavo. Fakultativni dogovor med zavarovalnico in pozavarovalnico omogoča zavarovalnici, da se sama odloči, katera tveganja ponudi v pozavarovanje, pozavarovalnica pa ima pravico sprejeti ali zavrniti ponujeno tveganje. Proporcionalno pozavarovanje pomeni, da se zavarovalne vsote oziroma iz njih izhajajoče premije in škode delijo med zavarovalnico in pozavarovalnico po vnaprej določenem razmerju, ki velja tako

za premije kot tudi za škode. Med proporcionalno pozavarovanje umeščamo kvotno pozavarovanje (angl. *quota share*) in vsotno-presežkovno pozavarovanje (angl. *surplus*). Kvotno je običajno primernejše za homogeno strukturirane portfelje, vsotno-presežkovno pa za portfelje z različno velikimi zavarovalnimi vsotami. Neproporcionalno pozavarovanje pomeni, da je pozavarovalnica udeležena le na škodah zavarovalnice nad vnaprej določenim zneskom in v višini vnaprej določenega zneska kritja. Med neproporocionalna pozavarovanja vključujemo škodno-presežkovno pozavarovanje (angl. *excess of loss*), pozavarovanje letnega presežka škod (angl. *stop loss*) in pozavarovanje kumulacije škod (angl. *aggregate loss cover*). Tudi pozavarovalnice lahko sklenejo pozavarovalne pogodbe z drugimi pozavarovalnicami in ta prenos tveganja se imenuje retrocesija (angl. *retrocession*).

Kapitalski trgi kot priložnost za prenos tveganja - na tem mestu se osredotočim predvsem na prenos tveganja s pomočjo instrumentov jamstva ILS (angl. *insurance-linked securities*). Za cedente tveganja ta instrument potencialno lahko poveča kapaciteto zavarovalnega trga zaradi vključenih kapitalskih trgov, kar omogoča boljšo razpršitev tveganj za zavarovalnice oziroma lastnike tveganj. Običajno so ILS strukturirani kot posebni nosilci (angl. *special purpose vehicle*), ki nudi cedentu kritje (cedent je tu lahko primarni zavarovatelj ali pozavarovatelj) in se financirajo z izdajo vrednostnih papirjev na kapitalske trge in dobičke investirajo v visoko kvalitetne vrednostne papirje (na primer državne obveznice). V primeru škodnega dogodka ti posebni nosilci izplačajo sredstva kot dogovorjeno s pozavarovalno pogodbo. ILS instrumenti se uporabljajo za kritje premoženjskih in odgovornostnih škod, škod življenjskih zavarovanj. Primer za kritje premoženjskih škod so katastrofalne obveznice (angl. *cat bonds*) (Eling & Wirfs, 2016, str. 38).

Vloga države v zavarovalništvu se običajno povezuje z ekstremnimi škodnimi scenariji in škodnimi dogodki. Nekatere nevarnosti so lahko tako specifične in ekstremne (običajno glede velikosti učinka, ki jo ima škodni dogodek), da je zato vloga države lahko ključna za zagotavljanje gospodarske varnosti na nivoju nacionalnega gospodarstva ali pa kot dopolnitev zasebnemu zavarovalnemu trgu. Tak primer so na primer naravni katastrofalni dogodki, nuklearne nevarnosti in terorizem. Država je običajno vključena tudi pri shemah za zagotavljanje socialne varnosti. OECD (v Eling & Wirfs, 2016, str. 40) ločuje dve vrsti intervencije države. Prva je posredna, kjer država ne zagotavlja svojih lastnih kapacitet, temveč vzpodbudi nastanek okolja za rast zasebnega zavarovalnega trga. Druga je neposredna, kjer država prevzame tveganje, lahko v celoti ali pa gre za javno-zasebno partnerstvo:

- država v vlogi primarnega zavarovatelja – država v celoti prevzame tveganje in opravlja vlogo zavarovalnice, ker zasebni zavarovalni trg ne zagotavlja kritja;
- država v vlogi pozavarovatelja kot zadnja možna rešitev – država prevzame tveganje za najvišje nivoje nevarnosti, medtem ko zavarovalnice krijejo srednje in male škode.

Zanimiv je tudi naslednji pogled na vlogo države, ki izhaja iz ekonomske teorije in jo povzema Labonte v svojem prispevku (2010, str.13), ki pravi, da država potencialno lahko izboljša učinkovitost gospodarstva, če obstaja tržna neučinkovitost. Opredeljena je z naslednjimi elementi: javne dobrine, splošne dobrine, monopol, vplivi na druge deležnike v gospodarstvu, asimetričnost informacij, neoptimalne odločitve (Labonte, 2010, str. 14–17). Če pogledamo nanje z vidika kibernetskih nevarnosti (Eling & Wirfs, 2016), bi bila na primer kibernetska varnost lahko opredeljena kot javna dobrina, ker se lahko zgodi, da zasebniki nimajo vsi enakega interesa investirati v kibernetsko varnost in so zaradi vedno večje medsebojne povezanosti ogroženi vsi subjekti v gospodarstvu, kar bi lahko bil razlog za vključitev države, da poseže na primer z ukrepom, ki predpisuje minimalne varnostne standarde vsem gospodarskim subjektom. Obenem lahko rečemo tudi, da ima to pozitivni vpliv na ostale subjekte v gospodarstvu. Med ostalimi elementi, pri katerih se lahko pojavlja tržna neučinkovitost sta monopol in neoptimalne odločitve, ki pa nista zelo povezana in primerna za primerjavo s kibernetsko varnostjo, zato ju na tem mestu ne izpostavljam. Glede asimetričnosti informacij, ki je bila že v prejšnjih poglavjih izpostavljena kot ključni faktor, ki vpliva na nizko stopnjo zavarovaljivosti, avtorja Eling in Wirfs (2016, str. 117) ugotavljata, da bi lahko zaradi neenakih informacij glede izpostavljenosti kibernetskim nevarnostim in izhajajočim tveganjem in posledično možnost moralnega hazarda in negativne selekcije to lahko zavrlo interes zavarovalnic za prevzemanje tovrstnih rizikov. Zato bi v tem primeru lahko vstopila država in preko različnih mehanizmov spodbudila želeno obnašanje in s tem vplivala tudi na apetite zavarovalnic in/ali po potrebi v primeru ekstremnih scenarijev vstopila v partnerstvo z zavarovalnicami in tudi prevzela del tveganja.

Zaenkrat se zdi, da državna intervencija v smeri direktne vključitve z udeležbo na delu tveganja še ni potrebna, če pogledam trenutno zavarovalno ponudbo in povpraševanje po kritju kibernetskih tveganj. Prvi pomemben korak s strani države bo implementacija nove evropske direktive, kar bo po mnenju zavarovalnega trga pozitivno vplivalo na stopnjo zavarovaljivosti in s tem na rast zavarovalnega trga. Skozi čas pa bo bolj jasno, kakšne so lahko razsežnosti varnostnih incidentov in ali bo potrebna aktivna vloga države tudi z direktno udeležbo na tveganju.

4 ZAVAROVANJE KIBERNETSKIH TVEGANJ V SVETU

4.1 Razvoj zavarovalnega/pozavarovalnega trga in produkta zavarovanja kibernetskih nevarnosti v svetu

Zavarovanje kibernetskih tveganj je na svetovnem nivoju v porastu. To je posledica javno objavljenih odmevnih varnostnih incidentov, večanja števila in obsega incidentov ter s tem postopno dvigovanje zavesti družb glede obstoja kibernetskih nevarnosti in tveganj, ki jih prinašajo. Tudi pri pripravi strategij obvladovanja tveganj družbe vse več pozornosti

namenijo obvladovanju tveganj in v definicijo premoženja, ki je predmet obravnave z vidika zavarovanja, vse bolj vključujejo tudi informacijska sredstva in informacijski sistem s podatki. V tabeli 6 je prikaz obsega kosmate zavarovalne premije v letu 2014 po ocenah Swiss Re po širših skupinah zavarovanja ter regijah, kjer je razvidno, da je zavarovanje kibernetskih tveganj še na začetku razvoja in v smislu doseženih obsegov kosmate zavarovalne premije ostalih zrelih zavarovalnih produktov velik potencial za rast v prihodnosti. Zneski so v milijardah USD.

Tabela 6: Obseg kosmate zavarovalne premije po skupinah zavarovanj v letu 2014 v milijardah USD

Skupina zavarovanj	**ZDA**	**Evropa**	**Azija**	**Skupaj**
Avtomobilska zavarovanja	246	161	77	484
Druga premoženjska zavarovanja	169	113	28	310
Odgovornostna zavarovanja	90	41	23	154
Zavarovanje kibernetskih tveganj	2	0,2	0,1	2,3

Vir: M. Bundt, The Reinsurance perspective, Swiss Re, 2016, str. 4.

Iz podatkov je razvidno, da je trg zavarovanj kibernetskih tveganj daleč najbolj razvit v ZDA, v drugih regijah pa se je pravzaprav šele začel razvijati. Po navedbah PricewaterhouseCoopers (v nadaljevanju PwC) se 90 % globalne zavarovalne premije nanaša na zavarovanja, sklenjena v ZDA, vendar je zanimivo, da se le tretjina družb odloči za sklenitev zavarovanja kibernetskih tveganj. Tudi pogled na deleže sklenjenih zavarovanj po gospodarskih panogah kaže zelo različno sliko. Največ družb, ki se odločijo za nakup zavarovalnega kritja, in sicer kar 50 %, je iz zdravstvenega sektorja, sektorja tehnologije in sektorja maloprodaje. Družb iz proizvodnjega sektorja je le 5 % (PwC, 2015, str. 10).

Zavarovanje kibernetskih tveganj ima po navedbah Marsha (2014) svoje začetke v ZDA, v letu 1996, ko so se pojavili prvi produkti za zavarovanje kibernetskih tveganj. Najprej je bila regulativa vzpostavljena leta 2003 v državi Kalifornija, s katero je bilo zahtevano poročanje o kršenju osebnih podatkov, kmalu zatem je bila tovrstna zakonodaja sprejeta tudi v 47 drugih zveznih državah ZDA (od skupno 50), kar je bilo ključno za rast zavarovanj kibernetskih tveganj in v letu 2014 je sklepalo tovrstna zavarovanja že 60 zavarovalnic.

V Evropi začetki povpraševanja po zavarovanju kibernetskih tveganj segajo v leto 2000, po predvidevanjih zaradi povečane odvisnosti od informacijske tehnologije in nekaj primerov odmevnih varnostnih incidentov, kar je spodbudilo zavarovalni trg, da je začel intenzivneje raziskovati kibernetske nevarnosti in izhajajoča tveganja. V letu 2012 je Evropska Unija pripravila reformo direktive o varstvu podatkov (v nadaljevanju direktiva), leta 2013 je napovedala direktivo o kibernetski varnosti, v letih 2013/2014 zavarovalni sektor s centrom na londonskem zavarovalnem trgu (25–30 zavarovalnic) razvije

zavarovalna kritja za obvladovanje kibernetskih tveganj z nadgraditvijo podobnih obstoječih kritij, kot na primer kritje za tehnološke napake, v proces so se vključile tudi specialistične IT družbe, forenzične družbe in pravne pisarne s ponudbami za sodelovanje z zavarovalnicami pri oceni tveganj, preventivnih ukrepih, post-incident ukrepih. (Guy Carpenter, 2014). V letu 2015 so se v proces vključile tudi pozavarovalnice, ki so svojo priložnost videle ne le v prevzemu dela tveganja od zavarovalnic, temveč tudi v ponudbi kritja direktno v primeru velikih globalnih korporacij s potrebami po večjih kapacitetah, tj. nad 500 milijonov britanskih funtov (v nadaljevanju GBP) (Barn, 2016). V letu 2016 zavarovalnice izpostavljajo problematiko maloštevilnih in neverodostojnih podatkov o incidentih, ki niso zadostna podlaga za verodostojne ocene rizika in določitev ustrezne premije, problem akumulacije tveganj in vprašanje smiselnega nivoja absorbcije kibernetskih tveganj v zavarovalnicah.

Z večanjem števila varnostnih incidentov in njihovih razsežnosti se postopno dviguje stopnja zavedanja o kibernetskih nevarnostih, kar na eni strani vpliva na vedno večje število podjetij, ki se odločijo za nakup zavarovanja ter s tem omogočajo rast zavarovalnega trga, na drugi strani pa se od družb preko regulative zahteva poročanje in razkritja glede varnostnih incidentov, s katerimi so se soočile. V ZDA že dolgo preko različnih mehanizmov spodbujajo družbe k vzpostavitvi, vzdrževanju in nadgrajevanju sistemov informacijske varnosti za čimboljše obvladovanje kibernetskih tveganj. Na ravni Evropske Unije je bila v aprilu 2016 sprejeta prenovljena direktiva o varstvu osebnih podatkov (angl. *General Data Protection Regulation*), ki prinaša kar nekaj novosti glede ravnanja s podatki. Zajema dva dela, in sicer se prvi nanaša na splošno uredbo o varstvu podatkov, drugi pa na uredbo o varstvu podatkov za policijo in organe pravosodja. Prva bo državljanom omogočila boljši pregled in nadzor nad svojimi osebnimi podatki, obenem bo preglednost pravil omogočila bolj učinkovito ravnanje s podatki, ki jih prinaša digitalizacija podatkov. Drugi del, ki se nanaša na policijo in organe pravosodja bo udeležencem v preiskavah, žrtvam, pričam kaznivih dejanj zagotovila varstvo njihovih osebnih podatkov in olajšala čezmejno sodelovanje za bolj učinkovit boj proti kriminalu (European Commission, 2012, str. 1). Direktiva bo vzpostavila poenotenje pravnega okvira znotraj Evropske Unije in uvedla tudi nove ukrepe, ki se nanašajo na poročanje o varnostnih incidentih in zahtevajo poročanje o nastalem varnostnem incidentu v okviru 72 ur. Vse organizacije, ki rokujejo z osebnimi podatki posameznikov, bodo zavezani k odstranitvi le-teh, v koliko ne bodo pridobili soglasja lastnikov. Direktiva se nanaša tudi na vse organizacije s sedežem izven Evrope, ter opravljajo storitve v Evropski Uniji. Uvaja tudi visoke kazni v primeru neskladnosti z določili, in sicer lahko tudi do višine 4 % letnega prometa ali 20 milijonov EUR. Direktiva stopi v veljavo v dveh letih od sprejema, tj. spomladi 2018.

Po mnenju mnogih zavarovalnic in pozavarovalnic bo v Evropi sprejem regulative prispeval k dvigu zavesti družb glede obstoja kibernetskih nevarnosti in spodbudil potrebo po upravljanju s tveganji, ki jih prinašajo ter s tem posredno vplival na dvig povpraševanja

po zavarovalnem kritju in pospešil rast tovrstnih zavarovanj na evropskem zavarovalnem trgu. V Sliki 29 je prikazano gibanje rasti kosmate zavarovalne premije na globalnem nivoju z ocenami za leta 2014–2025, zneski so v milijardah USD.

Betterley (2015, str. 4) v svojem poročilu o raziskavi zavarovalnega trga, ki jo je izvedel, ugotavlja, da produkt zavarovanja kibernetskih tveganj kljub začetkom v letu 2000 šele sedaj začenja pridobivati na pomenu, predvsem pa je nov kot produkt v smislu izpostavljenosti sprejetih kibernetskih tveganj na zavarovalnem trgu, ki so šele v zadnjih letih začela naraščati.

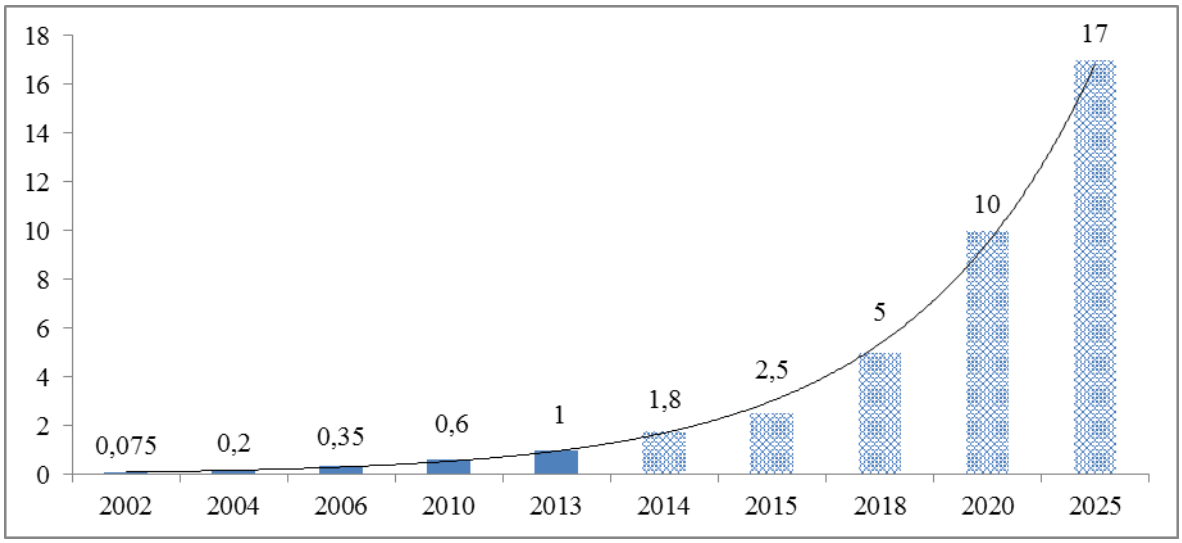
Posledično zavarovatelji in pozavarovatelji namenjajo vse več pozornosti oceni tveganj, primernosti premij in opredelitvi zavarovalnega kritja. Nadalje poročilo (Betterley, 2015, str. 5) ugotavlja, da so male in srednje velike družbe (tj. družbe z obsegom letnega prometa do 100 milijonov USD) prepoznane kot pomemben vir za bodočo rast tega produkta. Veliko povpraševanja iz njihove strani je posledica pogojevanja s strani njihovih poslovnih partnerjev za sklenitev posla. Povpraševanje raste tudi v segmentu zdravstva.

Z raziskavo je Betterley (2015, str. 6) ugotovil tudi, da premijske stopnje od 2015 rastejo, predvsem za velike družbe (tj. družbe z obsegom letnega prometa nad 1 milijardo USD), družbe iz zdravstvenega sektorja in maloprodaje, in sicer gre za povečanja v rangu 5 %–50 %, pretežno pa 10 %–25 %. V primeru preteklih škod pa lahko po navedbah raziskave povišanje znese tudi do 200 %. Kar se tiče majhnih in srednje velikih družb, raziskava kaže, da ni takih trendov povečanj, da so premijske stopnje ugodnejše, kar je odraz tudi tega, da ponavadi iščejo nižje zneske kritja in imajo pretežno (doslej) boljšo statistiko preteklih škod kot velike družbe in omenjeni sektorji maloprodaje in zdravstva.

Glede zneskov kritja, po katerem povprašujejo družbe, Betterley (2015, str. 8) v raziskavi povzema, da velike družbe, ter družbe iz sektorjev maloprodaje in zdravstva težje pridobijo visoke zneske kritja, predvsem za tveganja razkritja oziroma zlorabe podatkov, kar je posledica predvsem preteklih škod in zavarovalnice večinoma podlimitirajo zavarovalno kritje za tovrstna tveganja. Na zavarovalni trg pa vstopajo nekatere zavarovalnice s konceptom zavarovanja presežka nad osnovnim kritjem, kar dodatno razširja ponudbo zavarovalnega trga in izbiro družb pri odločanju glede nakupa zavarovanja. Tudi samopridržaji družb oziroma franšize se povečujejo, včasih kot pogoj za sklenitev zavarovanja, včasih pa zaradi dosega nižje cene zavarovanja.

V svetu približno 60 zavarovalnic nudi zavarovanje kibernetskih tveganj kot samostojno kritje. Če naštejem le nekaj pomembnejših, so med njimi AIG, ACE, Allianz, ANV Beazley, Britt, Chubb, Liberty, Lloyds, Munich Re, QBE, SCOR, Swiss Re, Zurich, (Fort, 2016).

Slika 29: Rast globalne kosmate zavarovalne premije zavarovanj kibernetskih tveganj v letih 2002–2025 v milijardah USD



Legenda: Zneski za leta 2014–2025 so ocene

Vir: Aon Risk Solutions, Cyber –The fast moving target, 2016, str. 1; M. Bundt, The Reinsurance perspective, Swiss Re, 2016, str. 5.

Na podlagi tehnološkega razvoja, razširjenosti internetnega poslovanja in vse večje medsebojne povezanosti družb se skozi čas postopno razvija tudi produkt zavarovanja kibernetskih tveganj. V ZDA je zavarovalni trg dosegel že visoko stopnjo zrelosti, v Evropi je zavarovalni trg kljub vsemu še v začetni fazi razvoja, če sodimo po zneskih kosmate zavarovalne premije. Glede na napovedi zavarovalnega trga so pričakovanja glede rasti velika, obenem pa se zavarovalnice na podlagi že sprejetih zavarovanj in škodnih izkušenj vse bolj zavedajo razsežnosti, ki jih ta zavarovalna vrsta prinaša tudi na strani škod in zato se zavedajo pomena verodostojnih aktuarskih analiz, ki so osnova za ustrezno oceno rizika in določitev primerne premije. Kot odgovor na škodno statistiko in trenutno stanje glede pomanjkanja verodostojnih podatkov o varnostnih incidentih, se zavarovalnice previdno odločajo glede višine, strukture in cene zavarovalnih kritij. Z vzpostavitvijo verodostojnih osnov za oceno tveganj in razvojem tehnik modeliranja in analiziranja nekateri viri ocenjujejo, da bi v desetih letih lahko zavarovanje kibernetskih tveganj postala ena večjih zavarovalnih vrst (Aon, 2015, str. 15).

4.2 Značilnosti in zavarovaljivost kibernetskih tveganj

4.2.1 Kriteriji zavarovaljivosti in značilnosti kibernetskih tveganj

Mnoge značilnosti kibernetskih tveganj predstavljajo ovire, ki preprečujejo večjo rast zavarovalnega trga in zavirajo tako rast premije kot tudi obseg zavarovalnega kritja, ki so ga zavarovalnice pripravljene ponuditi.

V literaturi so kriteriji zavarovaljivosti po Berlinerju (v Eling & Wirfs, 2016, str.27) sledeči:

- slučajnost škodnih dogodkov,
- maksimalni možni znesek škode,
- povprečni znesek škode po škodnem dogodku,
- škodna izpostavljenost,
- informacijska asimetrija,
- zavarovalna premija,
- limiti zavarovalnega kritja,
- javna politika,
- pravne omejitve.

Glede obravnave navedenih kriterijev z vidika kibernetskih tveganj, so najbolj problematični naslednji: slučajnost škodnih dogodkov, informacijska asimetrija in limiti zavarovalnega kritja.

Da bi bil izpolnjen kriterij slučajnosti, mora veljati, da je škodni dogodek neodvisen in predvidljiv. Pri naključnosti škodnih dogodkov je težava v tem, da varnostni incidenti niso vedno neodvisni in drugo, tudi niso predvidljivi, kar se tiče škodne izpostavljenosti za nek varnostni incident. Razlog za to je v tem, da se škode zaradi pomanjkljivih podatkov o preteklih škodah težko izmeri. Tudi v primeru razpoložljivosti zgodovinskih škodnih podatkov težava vsaj delno še vedno ostaja, ker se lahko vprašamo, koliko je relevantna pretekla škodna statistika za namen ocenjevanja prihodnosti v primeru kibernetskih tveganj, ki so podvržena hitremu spreminjanju.

Pri informacijski asimetriji gre v bistvu za anti-selekcijo, kar se kaže v tem, da bodo družbe, ki so že doživele varnostni incident verjetnejši kupec zavarovanja kibernetskih tveganj. Zavarovalnice se skušajo temu ubraniti preko postopkov ocene kibernetskih tveganj neke družbe, ki vsebuje na primer revizijo stanja v družbi pred sklenitvijo, zahtevo za izpolnitev obsežnih vprašalnikov glede vzpostavljenih sistemov informacijske varnosti in sistema upravljanja z informacijsko varnostjo. Na drugi strani pa je tu še efekt moralnega hazarda in se kaže kot sprememba obnašanja po sklenitvi zavarovanja. Tak primer je upad interesa družbe za vzpostavitev učinkovitega sistema upravljanja z iformacijsko varnostjo. Na to skušajo zavarovalnice vplivati preko mehanizma franšiz in limitov kritja. Dodatno nevarnost in vir za moralni hazard predstavlja tudi sodobna medsebojna povezanost družb, kar pomeni, da ni nujno, da je varnostni incident posledica ranljivosti lastnega informacijskega sistema, ampak je lahko posledica ranljivosti sistema druge družbe, s katero smo povezani in zato izpostavljeni tveganju prenosa učinka incidenta v naš sistem.

Limiti zavarovalnega kritja v primeru kibernetskih tveganj se gibljejo, kot izhaja iz različnih raziskav, največ v rangu od 10 milijonov do 50 milijonov USD in le nekaj v višini do 100 milijonov USD. Dodatno zavarovalnice navedejo tudi seznam izključitev kritja, kot na primer terorizem, samopovzročene škode ter tudi izguba ugleda, ki je indirektna škoda in je težko merljiva, zato je običajno izključena. Zaradi različnih dodatnih določil zavarovalne pogodbe in tudi zaradi dinamike spreminjanja kibernetskih nevarnosti in posledično kibernetskih tveganj, so zavarovanci pogosto nesigurni glede vsebine zavarovalnega kritja, kar vpliva tudi na odločanje o nakupu zavarovanja.

V literaturi so navedene naslednje značilnosti kibernetskih nevarnosti, ki dodatno vplivajo na stopnjo zavarovaljivosti in so pomembne pri oceni tveganj, ki jih prinašajo (Eling & Wirfs, 2016, str. 29):

- škoda iz naslova kibernetskega napada ima lahko učinek na kratek rok ali na dolgi rok,
- škode kibernetskega napada lahko povzročijo škodo direktno napadeni družbi in lahko povzročijo škodo tudi tretjim osebam, ki terjajo napadeno družbo za povračilo učinkov škode, ki so lahko tako materialni kot tudi nematerialni (telesne poškodbe),
- kibernetske škode niso neodvisne,
- majhen zavarovalni trg za zavarovanje kibernetskih tveganj,
- negotovost glede razpoložljivosti in verodostojnosti podatkov,
- negotovost glede metodologije za modeliranje škod,
- spreminjanje kibernetskih nevarnosti skozi čas,
- oteženo ocenjevanje ekstremnih škodnih scenarijev,
- omejitev zavarovalnega kritja (franšize in limiti kritja),
- velik pomen instrumentov za zmanjšanje tveganja.

Škode iz kibernetskih tveganj imajo lahko takojšen učinek oziroma kmalu po incidentu, ali pa šele čez dalj časa. Primer takojšnjega učinka je na primer incident zavračanja storitve, ki takoj onemogoči delovanje internetne strani neke družbe. Primer učinka čez daljši čas po napadu je kraja intelektualne lastnine, ko se lahko šele čez več let izkaže, da je prišlo do incidenta, in sicer s tem, ko je konkurent vstopil na trg z novim (starim) produktom, pred tem pa družba morda niti ni zaznala, da je do napada prišlo oziroma ni bilo opaziti učinka.

Rezultat kibernetskega napada je lahko škoda, ki nastane direktno na informacijskih sredstvih ali informacijskem sistemu družbe in povzroči stroške družbi v zvezi z vzpostavitvijo v prvotno stanje, lahko pa so rezultat napada tudi škode iz naslova tretjih oseb. Pri tem gre lahko tako za materialne škode, povzročene tretjim osebam, kot tudi za škode iz naslova odgovornosti napadene družbe do tretjih oseb. Tak primer so lahko škode, ki izvirajo iz napada z zlonamerno škodo, kjer se lahko zgodi, da se zaradi medsebojne povezanosti zlonamerna koda prenese iz napadene družbe naprej tudi na vse ostale, ki so z njo povezane in s tem na primer ogrozi podatke vseh vpletenih družb. Posledično se lahko

zgodi, da so družbe podvržene tožbam lastnikov podatkov, ki so bili ogroženi, za kar je v tem primeru odgovorna prva družba, ki je bila napadena in lahko to zanjo predstavlja velik finančni učinek na poslovanje ter morda tudi oškodovanje ali celo izgubo ugleda na trgu. Še bolj kot za velike družbe, so razsežnosti finančnih učinkov predvsem iz naslova odgovornosti do tretjih oseb lahko ključne za poslovanje malih in srednje velikih družb, v delu tudi zato, ker napadalci izkoristijo medsebojno povezanost družb in izberejo male in srednje družbe kot vstopni kanal do velikih družb. Če predpostavimo, da manjše družbe manj vlagajo v informacijsko varnost, je več možnosti, da imajo manjše družbe večjo stopnjo ranljivosti in imajo zato napadalci manj stroškov in več možnosti za vdor, finančni učinek vdora in izhajajočih posledic pa je lahko za male in srednje velike družbe lahko tudi usoden za njihovo poslovanje.

Iz podanega primera škode iz prejšnjega odstavka lahko izvedem eno najpomembnejših značilnosti kibernetskih škod, ki ima velik vpliv na stopnjo zavarovaljivosti in to je korelacija škod. Böhme in Kataria (2006, str. 4) ločujeta dve vrsti korelacij. Ena je korelacija škod znotraj družbe in druga je globalna, zunanja korelacija med škodami različnih družb. V kolikor se zgodi na primer okvara nekega informacijskega sredstva v družbi, ni pričakovati, da se to prenese na druga informacijska sredstva v družbi ali celo na informacijska sredstva drugih družb (razen v primeru, da gre za napako v produktu, kar pa je predmet drugih tveganj). Zato lahko govorimo o nizki korelaciji znotraj družbe in izven nje. Notranje zlorabe imajo po drugi strani večji vpliv na informacijski sistem in informacijska sredstva družbe, ker lahko povzročijo škodo širše kot neka tehnična napaka na računalniku, in sicer gre za obseg škode v okviru uporabniških pravic ki so nekemu uporabniku dodeljene, zato je tudi korelacija v primeru notranje zlorabe višja, nima pa tak incident vpliva na zunanje korelacije škod, zato je za zunanje nizka. Je pa za zunanje visoka za primere, ko gre za »phishing« napade, ker se širi z interakcijo uporabnikov. Sicer se učinek »phishing« napadov pokaže tudi v internih sistemih, vendar je vseeno pri tem smiselno predpostaviti, da v internem sistemu ne bo toliko neprevidnih uporabnikov, se jih bo našlo v vsaki družbi nekaj, zato bi pri teh predpostavkah lahko rekli, da je pri tovrstnih napadih za interne sisteme nizka korelacija škod, za zunanje pa visoka. Situacija, kjer je visoka korelacija škod pri obeh, notranjem in med zunanjimi sistemi, nastopi v primeru virusov in črvov, ker so po navadi sproženi iz različnih mrež, ki jih uporabljajo oziroma so povezani z njimi tako notranji sistemi kot tudi zunanji.

Trg za zavarovanje kibernetskih tveganj je, če se osredotočim na evropski trg, zaenkrat še na začetku razvoja, kar kaže tudi obseg zbranih premij, kar je na eni strani posledica še vedno nizke stopnje osveščenosti, na drugi pa omejen apetit zavarovalnic zaradi specifik kibernetskih tveganj, ki se posledično odrazi v nižji stopnji zavarovaljivosti.

Nadalje je pomemben faktor zavarovaljivosti razpoložljivost in verodostojnost podatkov o varnostnih incidentih, ter iz tega izhajajoče vprašanje izbire primerne metodologije za oceno bodočih škod in rezultatov te zavarovalne vrste. Šele primeren obseg verodostojnih

podatkov in prave metodologije za aktuarsko analizo, omogoča korektno oceno tveganja in določitev ustrezne cene, zato se ocene tveganja in premije sproti prilagajajo po sistemu učenja iz novih situacij incidentov, ter vključujejo znaten del pribitka zaradi navedenih negotovosti. To posledično vpliva na dostopnost zavarovanja, še posebej za male in srednje velike družbe ter s tem onemogoča rast zavarovalnega trga. Če med negotovosti dodamo še hitro spreminjanje kibernetskih nevarnosti in vpliv na oceno tveganj, se pojavi še vprašanje ustreznosti preteklih podatkov o varnostnih incidentih za napoved bodočega razvoja škod.

Scenariji varnostnih incidentov z ekstremnimi učinki so poseben izziv za zavarovalnice, ker je zanje značilna majhna frekvenca, vendar z velikim učinkom. To predstavlja precejšen problem v zvezi z oceno škode za primer najslabših možnih scenarijev in sicer glede ocene največje verjetne razsežnosti takega dogodka. Po navedbah v poročilu Lloyd's in Cambridge Centre for Risk Studies do leta 2015 še ni bilo tovrstnega katastrofalnega kibernetskega napada, ki bi zaobjel več družb in zavarovalnic hkrati (2015, str. 4). V svojem poročilu (2015, str. 4) so predstavili rezultate hipotetičnega primera katastrofalnega kibernetskega napada, in sicer napad z zlonamerno kodo, ki v sistem električnega omrežja ZDA vgradi virus, ki na omrežje deluje na način, da pride do napetostnega zloma in več kot 90 milijonov ljudi ostane v temi. Scenarij je predvidel učinek takega incidenta v povečanju števila mrtvih zaradi zloma zdravstvenega in varnostnih sistemov, prekinitev dobave vode, zlom druge infrastrukture, komunikacij, transporta ter prekinitev dobave različnih energentov. Posledično bi prišlo do izpada dohodka mnogih dobaviteljev iz različnih sektorjev gospodarstva in motenj dobave blaga in storitev. Skupna ocena stroškov tega scenarija je ocenjena na 243 milijard USD. Simulacija tega primera vključuje tudi oceno učinkov za zavarovalnice, po kateri naj bi bile v skupni škodi udeležene v višini 21 milijard USD (ter v ekstremnem primeru 71 milijard USD) in bi se akumulirale iz različnih vrst zavarovalnih kritij.

Zavarovalnice se z uporabo različnih instrumentov, kot je na primer franšiza in omejitev zneska kritja, zaščitijo pred ekstremnimi škodnimi dogodki, medtem ko razlika nad tem obremeni zavarovance, zato je v prihodnosti potrebno iskati rešitve tako glede vzpostavitve minimalnih standardov informacijske varnosti kot tudi glede zavarovalnega kritja v smeri, da se čim bolje oceni tveganje in zagotovi potrebno zavarovalno kritje, po potrebi tudi ob podpori drugih deležnikov na nacionalni ravni, ker se še posebej v primeru katastrofalnih dogodkov učinki prelijejo na celotno narodno gospodarstvo.

4.2.2 Načini za izboljšanje stopnje zavarovaljivosti kibernetskih tveganj

Avtorja Eling in Wirfs (2016, str. 121) sta izpostavila naslednje ukrepe, ki bi jih bilo smotrno po njunem mnenju obravnavati pri iskanju rešitev za doseganje višje stopnje zavarovaljivosti kibernetskih nevarnosti:

- formiranje skupne podatkovne baze varnostnih incidentov,

- opredelitev minimalnih standardov za zmanjševanje kibernetskih tveganj,
- implementacija zahtev glede poročanja o varnostnih incidentih,
- spodbuditi razvoj tradicionalnih načinov prenosa tveganj,
- vključitev države v primeru katastrofalnih scenarijev varnostnih incidentov.

Avtorja (Eling & Wirfs, 2016, str. 121) sta mnenja, da je najlažje uresničljiv cilj skupna podatkovna baza podatkov in obeta največ koristi za zavarovalni trg. S tem ukrepom bi razpolagali s prepotrebnimi podatki za aktuarsko modeliranje in analize in na podlagi tega zmanjšali negotovost glede podatkov in posledično izboljšali ocene bodočih škod in določitev ustrezne zavarovalne premije.

Z opredelitvijo minimalnih standardov za zmanjševanje kibernetskih tveganj se lahko pozitivno vpliva na zmanjšanje moralnega hazarda, ki je lahko sicer prisoten v smislu, da zavarovanci po sklenitvi zavarovanja izgubijo interes za vzpostavitev učinkovitega sistema informacijske varnosti v družbi. Tudi vzpostavitev regulative v smislu minimalnih varnostnih standardov bi pripomogla ne le k bolj varnemu poslovanju posamezne družbe, temveč tudi gospodarstva kot celote. Nadalje je izrednega pomena vzpostavitev obveznosti za poročanje o varnostnih incidentih in v letu 2016 sprejeta direktiva o varstvu osebnih podatkov na ravni Evropske Unije je že odraz zavedanja glede pomena kibernetskih nevarnosti in zbiranja tovrstnih podatkov.

V zavarovalništvu je že poznana ideja o združevanju zavarovalnic v ti. zavarovalni »pool«, s katerim se doseže boljša diverzifikacija škod, ki je majhni portfelji zavarovalnic ne omogočajo. Tudi v primeru kibernetskih nevarnosti se zdi to zaradi razsežnosti tveganj, do katerih lahko pride, smiselna pot v iskanju primerne rešitve na zasebnem zavarovalnem trgu in sicer bodisi za izbrane nevarnosti znotraj širokega nabora kibernetskih nevarnosti bodisi za ekstremne scenarije varnostnih incidentov. Na drugi strani bi morda lahko država preko kapitalskih olajšav in olajšav glede politike rezerviranja spodbudila pozavarovalnice, da zagotovijo dodatne kapacitete za presežna tveganja zavarovalnic (Eling & Wirfs, 2016, str. 122).

Če pogledam situacijo pri podobnih ekstremnih nevarnostih kot so na primer nuklearne nevarnosti, nevarnosti naravnih katastrof, terorizma, vidimo, da je privatni zavarovalni sektor bolj ali manj uspel zagotoviti kritja, vsaj kar se tiče nekih verjetnih pričakovanih scenarijev. Na trgu obstajajo nuklearni »pooli«, prav tako pozavarovalnice za kritje naravnih katastrof zagotavljajo kapacitete, po katerih povprašujejo zavarovalnice, obstoji tudi kritje terorističnih rizikov. Seveda bi bila v primeru ekstremnih katastrofalnih scenarijev in odsotnosti kapacitet zasebnega zavarovalnega trga verjetno še vedno država tista, ki bi vstopila s svojimi kapacitetami.

4.3 Zavarovalni produkti za kritje kibernetskih tveganj

Zavarovanje kibernetskih tveganj je relativno mlada vrsta zavarovanja, ker pa se gospodarsko okolje in tehnologija hitro razvijata, se tudi zavarovalni trg skuša sproti prilagajati s strukturo in obsegom kritja. Nekatere zavarovalnice na primer nudijo le kritje materialne škode / povračilo stroškov v zvezi z povrnitvijo v prvotno stanje (odvisno od vrste kritja), druge nudijo tudi odgovornost do tretjih oseb. Nekatere nudijo samo odgovornost do tretjih oseb, razlikujejo se tudi izključitve, zato bom tu prikazala ponudbe zavarovalnic kot zbir kritij, ki jih ponujajo sicer v različnih kombinacijah osnovnih in dodatnih kritij. Pomembno vlogo imajo tudi dodatne storitve, ki jih zavarovalnice nudijo v okviru produkta zavarovanja kibernetskih tveganj in so lahko ključne pri odnosu z zavarovancem, obenem pa nudijo zavarovalnici kontrolo nad škodnim dogajanjem. Tovrstne storitve so nekatere zavarovalnice (večje) že do določene mere vpeljale, bo pa potrebno sprotno razvijanje in prilagajanje potrebam, kot jih bo narekoval razvoj produkta. Take storitve so na primer svetovanje zavarovancem v smeri preventive, kot na primer glede vzpostavitve sistema informacijske varnosti, načrtovanja aktivnosti po kibernetskem napadu, storitve hitre pomoči preko klicnih centrov (Betterley, 2015, str. 13).

4.3.1 Produkti za zavarovanje kibernetskih tveganj kot samostojno kritje

Produkti so pri različnih zavarovalnicah sestavljeni na različne načine. Kritje se lahko nanaša na škode, nastale pri zavarovancu kot posledica kibernetskega napada in/ali na škode, nastale pri tretjih osebah (tj. škode iz naslova odgovornosti do tretjih oseb zaradi varnostnega incidenta pri zavarovancu). Na začetku razvoja produkta zavarovanja kibernetskih tveganj škode iz naslova odgovornosti do tretjih oseb (materialna škoda in telesne poškodbe) še niso bile vključene v kritja zavarovalnic, sčasoma pa je tega vedno več in postaja standard. Povečuje se tudi zanimanje za kritje odgovornosti iz naslova klevetanja v medijih, ki se tudi začenja pojavljati med kritji zavarovalnic, vendar zaenkrat bolj kot dodatno, izjemoma dogovorjeno kritje.

Če pogledam produkte najprej z vidika škode, ki nastane pri družbi, ki je bila tarča incidenta, zavarovalnice ponujajo kritje za naslednje škode, ki nastanejo kot posledica realiziranih kibernetskih tveganj (Aon, 2016; Guy Carpenter, 2016; Eling & Wirfs, 2016, str. 23):

- kritje zlonamernih napadov na informacije in informacijska sredstva družbe:
  - kritje stroškov nastalih zaradi okvare ali uničenja informacijskih sredstev (vključujejo stroške obnove informacijskih sredstev in stroške forenzičnega pregleda); nekje sem zasledila celo možnost kritja telesnih poškodb;
- kritje prekinitve poslovanja in zaščite podatkov (preko napada nezagotavljanja storitve, vdora v sistem, uničenja, okvare informacijskih sredstev in programske opreme):

  - kritje stroškov, nastalih zaradi razkritja zaupnih podatkov (vključujejo stroške obvestila lastnikov podatkov, javne objave, stroške forenzičnega pregleda),
  - kritje dodatnih stroškov, ki nastanejo zaradi prekinitve poslovanja (stroški obnovitve podatkov, stroški obnovitve intelektualne lastnine kot na primer programska oprema);
- kritje napadov izsiljevanja z namenom razkritja ali prenosa zaupnih podatkov ali tehnologije, z namenom spremembe, okvare ali uničenja informacij ali tehnologije, z namenom motenja ali prekinitve izvajanja storitev:
  - kritje stroškov plačila odkupnine in/ali stroškov preiskave za namen prerečitev izsiljevanja.

Kritje iz naslova odgovornosti do tretjih oseb večinoma zavarovalnice ponujajo za naslednje škode, ki nastanejo kot posledica realiziranih kibernetskih tveganj:

- kritje razkritja zaupnih podatkov, nastalih zaradi malomarnosti, namernih dejanj zaposlenih kot so kraja, izguba podatkov:
  - kritje sodnih stroškov obrambe, stroškov kazni, stroškov obveščanja lastnikov podatkov, stroškov preiskave in forenzičnih stroškov, stroškov za komuniciranje z javnostjo;
- kritje škode tretjim osebam zaradi sledečih dejanj: nenamerne instalacije virusa v informacijska sredstva, nepooblaščenega vstopa zavarovanca, motnje dostopnosti pooblaščenih komitentov zavarovanca, neupravičene prilastitve intelektualne lastnine:
  - kritje stroškov povrnitve v prvotno stanje, nekje sem zasledila celo možnost za kritja telesnih poškodb,
  - kritje stroškov sodnega procesa;
- kritje kršenja uporabe programske opreme, blagovne znamke, javno blatenje dobrega imena, ugleda:
  - kritje stroškov sodne obrambe, stroški kazni.

Po razpoložljivih informacijah pozavarovalnega trga so pogoste naslednje izključitve: kraja intelektualne lastnine, škoda nastala na blagovni znamki, oškodovanje ugleda, izsiljevanje kot samostojno kritje (to pomeni, da zavarovalnice krijejo ta dogodek le, če se zavaruje skupaj z ostalimi tveganji), samostojno kritje pogojne prekinitve poslovanja, kibernetska vojna (tj. politično motiviran napad na informacijske sisteme in informacije neke države) (Bundt, 2016).

V ZDA kot najbolj razvitem trgu za zavarovanje kibernetskih tveganj, je najbolj razširjen produkt s kritjem razkritja zaupnih podatkov, kar je posledica predvsem dolgoletne regulative glede varstva zdravstvenih podatkov in poročanja o incidentih z razkritjem zaupnih podatkov, ki je sprejet v 47 državah ZDA (American Bankers Association, 2016, str. 3). V Evropi je slika drugačna. Po razpoložljivih informacijah pozavarovalnic iz leta

2016 je največ povpraševanja evropskih družb po kritju prekinitve poslovanja. Glede na sprejeto direktivo Evropske unije v 2016 glede varstva osebnih podatkov pa se pričakuje, da bo ta spodbudila povpraševanje tudi po zavarovanju tveganja razkritja zaupnih podatkov.

Na zavarovalnem trgu se kot odgovor na nizko stopnjo osveščenosti malih in srednje velikih družb pojavljajo tudi produkti, ki so usmerjeni v ta segment družb, ker so, kot sem izpostavila v prejšnjih poglavjih, prav te lahko zelo ranljive in običajno podcenjujejo možne učinke varnostnih incidentov na njihovo družbo. Tovrstni zavarovalni produkti nudijo kritje v rangu do 5 milijonov EUR in vključujejo tudi celotno podporo zavarovancu v smislu ocene tveganja ob pomoči vključenega IT strokovnjaka za hitro in učinkovito podporo ob varnostnih incidentih.

Limiti kritja na zavarovalnem trgu so po splošni oceni še vedno nizki, kar kažejo tudi raziskave, omenjene v prejšnjih poglavjih. Predvsem za velike maloprodajne družbe in sektor zdravstva rezultati raziskav kažejo, da težje dobijo višje limite kritja, zaradi škodne zgodovine, še posebej to velja za kritje kršitve zaupnosti podatkov, kjer zavarovalnice pogosto omejijo kritje s podlimiti (Betterley, 2015, str. 8). V poročilu Marsha (2016, str. 3) so prikazani limiti kritja na globalnem zavarovalnem trgu v letu 2015. Če pogledam povprečne zneske limitov kritja na globalnem nivoju, so bili v višini 16,9 milijona USD. V primeru velikih družb, s prometom nad 1 milijardo USD, je povprečni limit znašal 39,2 milijona USD, v primeru velikih telekomunikacijskih, tehnoloških, medijskih družb je povprečni limit znašal 86,7 milijona USD in v primeru finančnih institucij 61 milijonov USD.

Franšize in samopridržaji se povečujejo, kar je posledica na eni strani dvigovanja premijskih stopenj in na ta način dosežejo zavarovanci nižjo ceno, po drugi strani pa tudi odraz pogojev, ki jih zavarovalnice postavijo glede na njihovo oceno tveganj, ki je bolj ali manj kompleksna, odvisno od želenega obsega kritja in sektorja dejavnosti zavarovanca (Betterley, 2015, str. 8).

4.3.2 Obstoječi produkti drugih zavarovalnih vrst in potencialno kritje / izključitev kibernetskih tveganj

Ob poznavanju vsebine tradicionalnih premoženjskih zavarovanj in odgovornostnih zavarovanj se danes mnogo zavarovalnic ukvarja z vprašanjem, koliko njihovih obstoječih tradicionalnih zavarovalnih pogodb vsebuje v dogovorjenem kritju elemente kibernetskih tveganj in ali bi lahko prišlo do tovrstnih škod iz naslova tradicionalnih zavrovalnih kritij in celo do akumulacije med njimi. Zavarovalnice niso enotne pri tolmačenju obstoječih pogojev kritja glede vprašanja kibernetskih tveganj, zato ga rešujejo vsaka posebej in se lahko zgodi, da bi bile nekatere škode lahko krite tudi v okviru tradicionalnih pogodb, v kolikor niso posebej izključene. Z razvojem specialnega produkta zavarovanja kibernetskih

tveganj so zavarovalnice začele eksplicitno izključevati kibernetska tveganja iz obstoječih tradicionalnih zavarovanj in ga opredeljujejo kot samostojno zavarovalno kritje.

Zanimivo je, da nekatere zavarovalnice zaradi možnosti prekrivanja kritja med tradicionalnimi zavarovalnimi vrstami in kibernetskim zavarovanjem ubirajo pristop, da se v primeru škode najprej črpa kritje tradicionalne zavarovalne police in nato morebitni presežek iz zavarovanja kibernetskih tveganj (Betterley, 2015, str. 11).

Po vrstah zavarovanj bom navedla primerjavo med kritjem tradicionalnih zavarovanj in zraven možnosti glede manjkajočega možnega kritja iz naslova kibernetskih tveganj, ki bi lahko učinkovale na tradicionalna kritja zavarovalnih produktov. Zavarovalnice bi morale biti pozorne na te možne vrzeli in jih ustrezno transparentno izključiti iz tradicionalnih kritij in jih ponuditi v okviru samostojnega produkta zavarovanja kibernetskih tveganj (Guy Carpenter, 2016). Tabela 7 prikazuje osnovno kritje po tradicionalnih zavarovalnih kritjih in možne vrzeli glede kibernetskih nevarnosti.

Tabela 7: Kritja po tradicionalnih produktih zavarovanja in možna manjkajoča kritja vezana na kibernetske nevarnosti

Zavarovalni produkt	**Namen zavarovalnega kritja**	**Potencialno manjkajoče kritje kibernetskih nevarnosti / izključitve**
Premoženje	materialna škoda na stvareh, materialnih sredstvih	Izključitev kibernetskih napadov in kritja materialne škode na stvareh, izključitev kritja škode na podatkih in programski opremi (gre za nematerialna sredstva)
Prekinitev poslovanja	Izguba dohodka in povzročeni dodatni stroški zaradi izgube dohodka	Tradicionalno kritje ne zajema kritje za kibernetske napade, ki ne povzročijo materialne škode
Splošna odgovornost	Odgovornost do tretjih oseb za materialno škodo premoženja , telesne poškodbe in odgovornostne škode iz naslova objavljenih vsebin, ki vključujejo kršitev zasebnosti podatkov	Izključitev nepooblaščenega razkritja osebnih informacij
Napake in opustitve aktivnosti / Profesionalna odgovornost	Odgovornost do tretjih oseb iz naslova izvajanja storitev	Kritje je lahko omejeno na odgovornostne škode klienotv družbe, medtem ko odgovornostne škode zaposlenih družbe zaradi razkritja njihovih podatkov pogosto niso krite; možne so izključitve, kot je prenos računalniškega virusa).

Vir: Guy Carpenter, Cyber Insurance Solutions, 2016, str. 6.

4.4 Izzivi zavarovalnic/pozavarovalnic za prihodnost

Kibernetske nevarnosti so dejstvo današnjega poslovanja družb ob uporabi interneta, drugih sodobnih tehnoloških rešitev in vse večji globalni povezanosti. Iz predhodnih poglavij je razvidno, da obstaja kar nekaj ovir za razmah zavarovanj kibernetskih tveganj.

Ključna so vprašanja, ki se tičejo zavarovaljivosti in njihovo reševanje, ki bi omogočile zavarovalnicam, da na eni strani omogočijo varnejše poslovanje družbe ter na drugi strani same dosežejo dodatno rast premije, ki v zadnjih letih raste po padajočih stopnjah. Eden pomembnejših vprašanj zavarovaljivosti je ocena tveganja, ki je povezana z razpoložljivostjo verodostojnih podatkov o varnostnih incidentih. Pričakovanja zavarovalnic so velika v zvezi s sprejeto direktivo EU, kjer pričakujejo, da se bo izboljšalo poročanje o incidentih in kvaliteta poročanih podatkov, kar bo temelj za verodostojne aktuarske analize in korektno oceno škod in cene zavarovanja, ki sedaj zaradi te negotovosti vsebuje določene pribitke in zato višji strošek za zavarovance. Zavarovalnice se delno lahko lotijo tega vprašanja tudi same, v smislu povezovanja preko neke globalne baze podatkov o incidentih, ki bi bile na voljo vsem in prinese pozitivni učinek tudi na globalnem zavarovalnem trgu.

Naslednji element je akumulacija tveganj, kjer so zavraovalnice mnenja, da je potrebno iskati rešitev v bodisi oblikovanju zavarovalnih »poolov« ali v obliki javno-zasebnih partnerstev z državo, še posebej za primere ekstremnih scenarijev varnostnih incidentov, kot je na primer zlom električnega omrežja v državi.

Posebno pozornost bodo morale zavarovalnice na nivoju zavarovalnega trga usmeriti v transparentnost zavarovalnih pogojev in se dogovoriti glede standardizacije procesa ocene rizika. Kot je razvidno iz prejšnjih poglavij, so kibernetska tveganja take vrste, ki delujejo globalno, zato je potrebno spremeniti način razmišljanja tudi pri zavarovalnicah in pozavarovalnicah ter najti temelje za povezovanje in sprejeti minimalne standarde ocene tveganja ter sprejeti dogovor glede opredelitev zavarovalnih kritij in izključitev, ter obenem preveriti prekrivanja s kritji iz drugih zavarovalnih vrst in zagotoviti transparentnost. S časom bo verjetno kot logična posledica vseh različnih kritij izšla potreba po oblikovanju kritja, ki bo zajel vsa različna tveganja, s katerimi se sooča družba, kar je svojevrsten izziv glede na raznolika tveganja, ki so v ozadju.

Poseben izziv prinašajo tudi nove tehnologije in razvoj različnih komunikacijskih orodij, katerim mora zavarovalni sektor slediti, da bo v toku s spremembami, ki so na tem področju še hitrejše kot pri drugih vrstah zavarovanj in imajo lahko zelo različen vpliv na oceno tveganj. V porastu je shranjevanje podatkov v oblaku in vse več se govori o internetu stvari in avtonomnih vozilih, če naštejem bolj odmevne tehnološke inovacije, zato morajo zavarovalnice oblikovati ekipe specialistov, ki se bodo ukvarjali s temi vprašanji, ki se nam danes sicer zdijo še daleč, vendar zaradi kompleksnosti glede ocene

tveganj in možnih večsmernih učinkov terjajo resno obravnavo in pravočasno pripravo. Pomemben element pri zavarovanju kibernetskih tveganj je tudi dodana vrednost zavarovalnic preko drugih storitev. Tu mislim predvsem na asistenco v fazi sklenitve zavarovanja, tako glede ocene ranljivosti sistema informacijske varnosti, svetovanja ustreznih tehnoloških rešitev in internih procesov obvladovanja kibernetskih nevarnosti, določitev ustreznega zavarovalnega kritja, ter nato pomoč ob varnostnih incidentih, korektna obravnava škod in asistenca ob vzpostavitvi v prvotno stanje. Pri tem je ključno povezovanje zavarovalnic s partnerji, IT specialisti, ker zavarovalnice same v pretežni meri še ne razpolagajo s takimi specialnimi znanji v takem obsegu. Pogosto so v procesu obdelave škode vključene tudi forenzične družbe, zato je ta proces za zavarovalnice svojevrstni izziv, kako doseči visoko stopnjo storitve za zavarovanca ob vzdržni premiji, sprejemljivi tudi za zavarovanca.

Poleg odprtih vprašanj glede stopnje zavarovaljivosti in novih prihajajočih nevarnosti je tu še element kibernetske kriminalitete, za katero se zdi, da je ves čas v prednosti. Iz različnih poročil raziskav incidentov izhaja, da so napadalci pri svojih aktivnostih zelo inovativni in kaže, da tudi obstoječi sistemi pregona nimajo uspešnih metod, načinov za odkrivanje storilcev in učinkovitega sistema za sankcioniranje. Nova direktiva EU ureja tudi del, ki se nanaša na pregon storilcev in prinaša rešitve glede izmenjave podatkov med državami, da bi lažje identificirali storilce, vendar je potrebno izhajati predvsem iz osnovnega vprašanja, kako zagotoviti čimbolj učinkovit sistem informacijske varnosti, kar pomeni, da bo potrebno iskati nove, inovativne rešitve, pri čemer so lahko koristne povezave med IT strokovnjaki in zavarovalnicami, kjer lahko različni pogledi prinesejo nove rešitve.

5 SWOT ANALIZA Z VIDIKA VPELJAVE ZAVAROVANJA KIBERNETSKIH TVEGANJ NA SLOVENSKI TRG

V današnjem svetu globalnega povezovanja in hitrega tehnološkega razvoja morajo biti družbe sposobne hitrega prilagajanja novim razmeram na trgu in slediti razvojnim trendom, da bi lahko ohranile konkurenčnost. Iz predhodnih poglavij je razvidno, da se je tudi v evropskem okolju začelo postopno dvigovati zavedanje o kibernetskih nevarnostih in tveganjih, ki jih prinašajo ter intenzivnejše iskanje rešitev tako za načine doseganja čim višje stopnje informacijske varnosti kot tudi glede prenosa dela tveganja na druge subjekte.

V tabeli 8 so predstavljene prednosti, slabosti, priložnosti in nevarnosti za zavarovalnice z vidika vpeljave zavarovanj kibernetskih tveganj na slovenski zavarovalni trg, ki sem jih izpeljala iz obravnavane tematike predhodnih poglavij.

Zavarovalnice imajo že oblikovan portfelj zavarovancev na osnovi sklenjenih polic iz drugih vrst zavarovanj. To lahko predstavlja dobro izhodišče za vpeljavo novega produkta, ki ga zavarovalnice izkoristijo na način, da se predstavi kot komplementarni produkt ostalim, obstoječim kritjem, saj se kibernetska tveganja nanašajo na informacije in

informacijska sredstva in se mora družba vprašati, zakaj še nima tega zavarovanja, ki imajo lahko velik vpliv na njihovo poslovanje, medtem ko je nakup zavarovanja za požar za družbe povsem logičen nakup. Pristop bi bilo verjetno smiselno diferencirati vsaj glede na velikost zavarovancev in glede na lastno presojo zavarovalnic glede primernosti zavarovanca za tak produkt, tudi glede na različne nivoje osveščenosti, če sklepam iz dosedanjih izkušenj SI-CERT pri obravnavanju prijavljenih varnostnih incidentov. Do novih potencialnih zavarovancev bi lahko pristopili v primeru tega specifičnega produkta tudi preko kampanij osveščanja in izobraževanja družb, ki je predviden tudi med ukrepi slovenske strategije kibernetske varnosti (predvidoma v obdobju 2016-2020), že sedaj pa SI-CERT izvaja progam osveščanja preko nacionalnega programa »Varni na internetu« in bi skupaj z izvajanjem ukrepov iz strategije lahko pozitivno spodbudili povpraševanje po zavarovalnih kritjih.

Tabela 8: SWOT matrika

Prednosti	**Slabosti**
• Obstoječa baza zavarovancev	• Manjko specifičnih informacijskih znanj v zavarovalnem sektorju, • Skrito kritje kibernetskih tveganj v obstoječih zavarovanjih
Priložnosti	**Nevarnosti**
• Rast internetnega poslovanja, • Rast premije zavarovalnega trga (nova vrsta), • Razvoj specialističnih družb za podporo in svetovanje družbam, zavarovalnicam, regulatornim organom, • Sprejem direktive EU o varstvu osebnih podatkov, • Sprejem slovenske strategije kibernetske varnosti, • Obstoj kapacitet na privatnem mednarodnem pozavarovalnem trgu	• Nizka stopnja osveščenosti slovenskih družb glede pomena in vpliva kibernetskih tveganj na njihovo poslovanje, • Trend nadaljnjega povečevanja števila varnostnih incidentov, • Narava hitrega spreminjanja kibernetskih tveganj, • Vprašanje stopnje zavarovaljivosti in kvalitetne ocene tveganja, • Akumulacije tveganj (iz obstoječih zavarovanj enega zavarovance in iz naslova večih zavarovancev vključenih v isti dogodek), • Možni negativni učinki na oceno rating agencij

Za zavarovalnice bo pri vpeljavi tega produkta eden ključnih elementov zagotovitev strokovnih kadrov, ki bodo imeli znanja informacijskih sistemov in tehnologij, ki so potrebna za oceno tveganj, ter zagotavljanje ostalih dodatnih storitev zavarovancem (kot na primer asistenca ob škodnem dogodku, ocena stanja in svetovanje za odpravo škode in povrnitev v prvotno stanje). V kasnejših fazah, v kolikor bi ekonomika to dovoljevala in bi se pokazal interes s strani zavarovancev, morda tudi ponuditi preventivno svetovanje. Zavarovalnice bi v ta namen morale oblikovati skupino zaposlenih s potrebnimi znanji, ki bi jih tudi sproti nadgrajevali, saj je ena od značilnosti kibernetskih nevarnosti, da se hitro spreminjajo, zato brez tega ni mogoče pravilno oceniti tveganj. Manjko tovrstnih znanj bi lahko zavarovalnice dopolnile preko povezovanja s specializiranimi IT družbami, kar

predstavlja obenem priložnost tudi zanje, da se na trgu pozicionirajo kot strokovnjaki za kibernetska tveganja in lahko nudijo svoje storitve večim subjektom: zavarovalnicam svetovanje pri oceni tveganja in razvoju novih produktov, zavarovancem asistenco v fazi preventive in ob incidentu ter tudi drugim družbam, potencialnim zavarovalncem in drugim zainteresiranim, na primer tudi regulatornim organom. Aktualno bi bilo lahko svetovanje pri izbiri in vzpostavitvi primernega sistema za vzpostavitev informacijske varnosti družbe ter pri pripravi zakonodajnih zahtev glede informacijske varnosti. Glede slabše osveščenosti malih in srednje velikih družb, bi bila morda priložnost zavarovalnic, da jim ponudijo produkt, ki zaobjame celovito rešitev, in sicer svetovanje glede vzpostavitve sistema obvladovanja kibernetskih tveganj, asistenco ob varnostnem incidentu, reševanje škode ter povrnitvi v prvotno stanje in svetovanje glede aktivnosti po škodnem dogodku.

K dvigu osveščenosti bo po oceni večine tujih zavarovalnic pozitivno vplival tudi sprejem direktive EU glede varovanja osebnih podatkov, ki predpisuje poročanje o varnostnih incidentih ter predvideva tudi visoke kazni za kršitelje. Direktiva je bila sprejeta spomladi 2016 in predvideva njeno uveljavitev čez dve leti, tj. spomladi 2018. To pomeni, da učinki sprejema še ne bodo takojšnji, prinaša pa pomembno spremembo, in sicer sistematično verodostojno zbiranje podatkov o varnostnih incidentih, ki bo omogočila zavarovalnicam korektne aktuarske analize za določitev primerne cene zavarovanja in ocene bodočega škodnega dogajanja. S tem bi se postavila izhodišča za dvig zavarovaljivosti kibernetskih tveganj in s tem rast teh zavarovanj in posledično rast premije. Zavarovalnice na trgih več ne dosegajo visokih rasti, to velja tudi za Slovenijo, zato iščejo nove priložnosti in ob dvigovanju stopnje zavarovaljivosti kibernetskih tveganj se odpirajo možnosti za novo rast zavarovalne premije. Priložnost za rast preko novega zavarovalnega produkta temelji na dejstvu, da je v porastu internetno poslovanje, tako v svetu kot tudi pri nas. Vse več družb je prisotnih na spletu, kar je posledica vse večjega števila uporabnikov interneta, kar družbe uspešno izkoriščajo kot nov kanal za približanje svojih izdelkov in storitev ciljnim kupcem ter s tem učinkovitejše poslovanje in doseganje boljših rezultatov. Poleg tega se družbe preko interneta povezujejo tako notranje kot tudi zunanje. Mnoge večje družbe imajo organizirano svojo notranjo internetno pošto, t.i. intranet, svojim zaposlenim omogočajo oddaljen dostop (na primer za delo od doma ali omogočanje povezljivosti v primeru službenih poti in drugih odsotnosti). Preko interneta se vse bolj povezujejo z drugimi zunanjimi informacijskimi sistemi kot na primer za izvajanje plačilnega prometa z bankami, z državo glede upravljanja s svojimi davčnimi in drugimi obveznostmi, predvsem pa zaradi globalizacije in vse večje digitalizacije podatkov internetno poslovanje vse bolj pridobiva na pomenu, ker prinaša fleksibilnost, odzivnost in večjo učinkovitost družb, kar spodbuja in sili družbe vse bolj k tovrstnim oblikam poslovanja, obenem pa se bodo postopno (če ne drugače, preko lastnih izkušenj z incidenti) vse bolj zavedale tudi tveganj, ki jih kibernetske nevarnosti prinašajo in potrebe po ustreznem upravljanju z njimi.

Zavarovalnice bi lahko dodatno preko povezovanja s specializiranimi IT družbami in regulatorji pomagala pri vzpostavitvi minimalnih standardov informacijske varnosti, ki bi predstavljali orientir tudi pri oceni kibernetskega tveganja in premije ter določitvi ostalih zavarovalnih pogojev. V kolikor bi uspeli doseči dogovor na nivoju zavarovalnega sektorja, še toliko bolje, saj bi preko standardizacije zahtev lažje oblikovali tudi zavarovalne »poole« preko subvencije za družbe, ki bi spoštovale dogovorjeni minimalni standard, še posebej, če pogledamo na kibernetska tveganja z vidika akumulacije, do katere lahko pride. V primeru, da se zgodi napad na neko družbo, ki je povezana naprej preko internetnega poslovanja še z mnogo drugimi, je potencialni učinek napada ne samo škoda ene družbe, temveč več družb naenkrat. To pomeni, da v primeru medsebojnih povezanosti ni dovolj, da ima dobro informacijsko varnost le ena izmed njih, temveč jo morajo imeti vse. Zato bi bila vpeljava minimalnih standardov informacijske varnosti verjetno smiselna pot, najbolje preko zakonodaje, vendar ker so s tem povezani tudi stroški, ki jih nosijo družbe za vzpostavitev takega sistema, je naprej potreben še razmislek, kje postaviti minimalne zahteve, ki so še ekonomsko vzdržne oziroma razmisliti tudi o državnih spodbudah. Kljub strošku, ki bi ga v tem primeru predstavljala subvencija za državo, je pozitivni učinek za družbo in gospodarstvo kot celoto lahko veliko večji. Večja kot je varnost v družbi, večja je varnost v gospodarstvu in mu omogoča okolje za nadaljnji razvoj in rast.

Glede strukture zavarovalnega kritja se mi zdi smiselno, glede na različne raziskave po svetu in v luči nove direktive EU, na začetku predstaviti kritje razkritja zaupnih podatkov ter kritje prekinitve poslovanja zaradi varnostnega incidenta, in sicer pri obeh tako za materialne škode, nastale pri zavarovancu kot posledica incidenta, kot tudi za materialne škode in telesne poškodbe tretjih oseb zaradi incidenta pri zavarovancu. Pomembno se je zavedati, da je produkt zavarovanja kibernetskih tveganj kompleksen produkt in je potrebno pri oblikovanju ponudbe kritja zavarovancu upoštevati vse specifike njegovega poslovanja in tveganj, da se lahko pravilno oceni bodoče obveznosti pogodbe in temu primerno ceno. Seveda je potrebno razmisliti tudi o smiselnih izključitvah, glede na specifiko zavarovanca, njegovo dejavnost in podobno. Na strani zavarovanca je potrebno omeniti še dva elementa, ki pomembno vplivata na stopnjo zavarovaljivosti. To sta asimetričnost informacij in negativna selekcija. Gre za to, da zavarovalnica ne razpolaga z vsemi informacijami zavarovanca in se lahko zgodi, da zavarovanec ob sklenitvi zavarovanja ne posreduje vseh relevantnih informacij ali pa po sklenitvi zavarovanja na primer opusti aktivnost vzdrževanja sistema informacijske varnosti. V izogib sprejema tovrstnih tveganj morajo zavarovalnice oblikovati ustrezne vprašalnike, s katerimi zavarovanec razloži, kako imajo v družbi vzpostavljen sistem obvladovanja kibernetskih tveganj, na osnovi tega nato zavarovalnice presodijo, ali je potrebna ločena ocena sistema (ki je verjetno edina logična izbira pri višjih zavarovalnih kritjih). Vsaka zavarovalnica mora zase predhodno oceniti kakšna zavarovalna kritja bo ponujala glede na aktuarske ocene pričakovanih škod in premijo ter opredeliti svoje maksimalne udeležbe v tveganjih in presežke prenesti naprej na pozavraovalnice. Tudi pri oceni tveganja bi bilo smiselno, da

se doseže nek enotni dogovor oziroma standard med zavarovalnicami, na kakšen način bi se ocenjevalo tveganja, s kakšnimi postopki, v kakšnem obsegu in pri tem računati tudi s tem, da bo zavarovanec že v tej fazi potreboval asistenco pri pripravi odgovorov.

Dodaten vidik, ki morda v tem trenutku še ni tako javno izpostavljen, vsekakor pa ni zanemarljiv in se nanaša na zavarovalnice. Gre za potencialna nevarnost slabše ocene rating agencij zaradi sklepanja zavarovanj kibernetskih tveganj. Pri tem bi imelo pomembno vlogo pozavarovanje, ki bi omogočilo zavarovalnici prenos tveganj naprej in bi na ta način optimirala obseg zadržanih tveganj na način, ki še zagotovi doseganje želene ocene rating agencij.

Zavarovalnice v svetu so že prepoznale možne prekrivanje zavarovalnih kritij med zavarovanjem kibernetskih tveganj in ostalimi vrstami zavarovanj. Podrobneje sem prikazala prekrivanja v ločenem poglavju, tu bi želela izpostaviti, da tudi Slovenija ni izjema in da bi se morale vse zavarovalnice lotiti resnega pregleda vsebine kritij in kjer bi ocenile, da je prekrivanje možno, z ustreznimi klavzulami izključiti škode kot posledico kibernetskih nevarnosti iz tradicionalnega kritja in skleniti novo polico z ločenim kritjem kibernetskih tveganj.

Med elementi, ki vplivajo na zavarovaljivost je tudi razpoložljivost podatkov o varnostnih incidentih in sem ga omenila že v zvezi z novo direktivo EU, ki predpisuje poročanje o incidentih. Dodatno k temu bi bilo smiselno tudi povezovanje zavarovalnic z namenom izmenjave podatkov o incidentih v obliki skupne podatkovne baze, kot je že znan in utečen način dela pri nekaterih drugih vrstah zavarovanja (na tem mestu omenjam kreditna zavarovanja, in sicer primer Bernske Unije, ki je mednarodno združenje privatnih in državnih izvozno-kreditnih zavarovateljev, kjer je že vrsto let vzpostavljen sistem izmenjave podatkov o škodah med članicami). Morda bi bilo smiselno pretehtati možnost glede rešitve preko Slovenskega zavarovalnega združenja, bodisi v smislu centralne baze podatkov o incidentih kot tudi glede usklajevanja standardiziranega pristopa glede minimalnih standardov informacijske varnosti in poenotenja standardov ocene kibernetskih tveganj.

Zaradi jasnega trenda povečevanja števila incidentov, ki je viden tako v tujini kot tudi v Sloveniji in ker je le še vprašanje časa, kdaj bo močneje zadelo tudi nas, bi bilo smiselno, da se različni deležniki vključijo v proces iskanja celovite rešitve, ki bi povezovala družbe, zavarovalnice, pozavarovalnice in tudi državo. Po internih informacijah sodeč je pozavarovalni trg pripravljen ponuditi svoje kapacitete za kritje kibernetskih tveganj, ker tudi pozavarovatelji vidijo to kot novo priložnost za rast, zavarovalnice pa glede na možne razsežnosti incidentov same ne bodo mogle zadržati tveganj v celoti. Tudi država bi verjetno morala spremljati različne scenarije možnih učinkov zloma kritične infrastrukture, kar je s strategijo kibernetske varnosti predvideno, zaradi narave kibernetskih tveganj, ki

niso predvidljiva in se hitro spreminjajo, pa je ključnega pomena prav fleksibilnost glede zaznavanja možnih novih nevarnosti in hitro prilagajanje.

SKLEP

V današnjem svetu globalnega povezovanja in hitrega tehnološkega razvoja morajo biti družbe sposobne hitrega prilagajanja novim razmeram na trgu in slediti razvojnim trendom, da bi lahko ohranile konkurenčnost. Iz statistike incidentov različnih virov je razvidno, da se število varnostnih incidentov veča, pričujoči svetovno odmevni primeri nakazujejo tudi na možen obseg njihovih razsežnosti, kar se postopno odraža tudi v večjem zavedanju glede kibernetskih nevarnosti in pomenu obvladovanja izhajajočih tveganj ter posledično v večjem povpraševanju po zavarovalnem kritju.

Tudi v evropskem okolju, katerega del je tudi Slovenija, se je začelo postopno dvigovati zavedanje o kibernetskih nevarnostih in tveganjih, ki jih prinašajo. Iz poročil SI-CERT lahko vidimo, da se varnostni incidenti že kar nekaj časa dogajajo tudi pri nas, in sicer se je število obravnavanih incidentov od leta 2008 do 2015 povečalo za skoraj šestkrat. Na srečo incidenti še ne dosegajo takšnih razsežnosti, kot jih poznajo v ZDA, kjer so tako kibernetske nevarnosti kot tudi razvoj zavarovalnih produktov v polnem razmahu, obenem pa hekerji sproti odkrivajo nove, inovativne načine napadov, kar terja neprestano nadgrajevanje sistemov informacijske varnosti in prilagajanje zavarovalnih kritij. Po informacijah SI-CERT na podlagi njihovih izkušenj ob reševanju incidentov, slovenske družbe še niso na zadovoljivi stopnji osveščenosti glede obstoja kibernetskih nevarnostih in iz njih izhajajočih tveganj za njihovo poslovanje. Predvsem to velja za male in srednje velike družbe, medtem ko večje družbe že začenjajo bolj intenzivno delati v smeri vzpostavitve procesov obvladovanja tveganj, delno nekatere tudi zaradi lastnih izkušenj z varnostnimi incidenti. Če vzamemo za merilo osveščenosti tudi število izdanih certifikatov ISO, ki se nanašajo na področje varnostne zaščite informacij in informacijskih sistemov, je iz podatkov razvidno, da je v Sloveniji število iz leta 2008 (16 izdanih certifikatov) do leta 2014 bistveno naraslo (58 izdanih certifikatov), kar kaže na pozitivni razvoj zavedanja glede pomena vpeljave standardov najboljših praks v družbi pri obvladovanju kibernetskih tveganj.

S sprejemom nove direktive EU glede varovanja osebnih podatkov ter sprejema slovenske strategije kibernetske varnosti je ponovno izpostavljen pomen obvladovanja kibernetskih tveganj in ta zakonodajni okvir bi lahko vzpostavil izhodišča za izboljšanje zavarovaljivosti kibernetskih tveganj, kar bi spodbudilo zavarovalnice k ponudbi produktov, ki bi zadostili potrebam zavarovancev. Na razvitih trgih je ob že uveljavljenih kritjih kibernetskih tveganj kot so kritje razkritja zaupnih podatkov in učinek varnostnega incidenta na prekinitev poslovanja, vse več povpraševanja tudi po kritju izgube ugleda družbe zaradi varnostnega incidenta ter kraje intelektualne lastnine, ki so sedaj praviloma

izključene iz zavarovalnih kritij. Zaradi mnogih faktorjev, ki vplivajo na zavarovaljivost, ter obenem zaradi razsežnosti, spreminjanja in nastajanja novih kibernetskih tveganj je zato potrebno sodelovanje vseh glavnih nosilcev tveganj, tj. zavarovancev, zavarovalnic, pozavarovalnic in države, da bi lahko ob sodelovanju s strokovnjaki IT našli primerno rešitev, s katero bi omogočili družbam prenos dela tveganja na zavarovalnice in s tem vzpostavili temelje za doseganje informacijske varnosti in pogoje za razvoj in rast poslovanja, za zavarovalnice pa je to nova priložnost za rast zavarovalnega trga. Vključitev zavarovalnice v procesu prenosa tveganj je pozitivna. Poleg prenosa tveganja, ki ga zagotovi s sklenitvijo zavarovanja, zavarovalnica v procesu ocene tveganj razkrije še nerazkrite ranljivosti sistema obvladovanja kibernetskih tveganj zavarovanca in obenem zavarovancu spremeni negotovost glede stroška v informacijsko varnost v gotovost glede kritja v primeru varnostnega incidenta. Če pa upoštevamo še narodno-gospodarski vidik, je učinek informacijske varnosti očiten, zato je izrednega pomena, da je informacijska varnost umeščena visoko na seznamu prioritet strateških ciljev podjetij in države, da lahko zavarovalnice in pozavarovalnice kot specializirane institucije za prevzemanje tveganj odigrajo svojo vlogo pri upravljanju s tveganji in s tem omogočijo čimbolj nemoteno gospodarsko aktivnost in rast. Trenutek za ukrepanje je tu, saj ni več vprašanje, ali bo do varnostnega incidenta prišlo, temveč samo še kako kmalu in s kakšnimi učinki.

LITERATURA IN VIRI

1. Ackerman, G. (2013, 13. junij): Urged to treat cyber attacks as threat to economy. *Bloomberg*. Najdeno 1. maja 2016 na spletnem naslovu http://www.bloomberg.com/news/articles/2013-06-13/g-20-urged-to-treat-cyber-attacks-as-threat-to-economy
2. Allianz Global Corporate & Specialty. (2014). *Allianz risk barometer on business risks 2014*. Najdeno 1. maja 2016 na spletnem naslovu http://www.agcs.allianz.com/assets/PDFs/Reports/Allianz-Risk-Barometer-2014_EN.pdf
3. Allianz Global Corporate & Specialty. (2015a). *A guide to Cyber Risk*. Najdeno 1. maja 2016 na spletnem naslovu http://www.agcs.allianz.com/insights/ white-papers-and-case-studies/cyber-risk-guide/
4. Allianz Global Corporate & Specialty. (2015b). *Allianz risk barometer, Top business risks 2015*. Najdeno 1. maja 2016 na spletnem naslovu http://www.agcs.allianz.com/insights/white-papers-and-case-studies/cyber-risk-guide/
5. Allianz Global Corporate & Specialty. (2016). *Allianz risk barometer, Top business risks 2016*. Najdeno 1. maja 2016 na spletnem naslovu http://www.agcs.allianz.com/assets/PDFs/Reports/AllianzRiskBarometer2016.pdf
6. American Bankers Association. (2016). 2016 Cyber Insurance Buying Guide. Najdeno 2. maja 2016 na spletnem naslovu http://www.aba.com/Tools/Function/Cyber/Documents/2016-Cyber-Insurance-Buying-Guide.pdf
7. Aon Benfield. (2015). Insurance Risk Study – Global Insurance Market Opportunities. Najdeno 2. maja 2016 na spletnem naslovu http://thoughtleadership.aonbenfield.com/Documents/20150913-ab-analytics-insurance-risk-study.pdf
8. Aon Benfield. (2016). Cyber – the fast moving target. Najdeno 2. maja 2016 na spletnem naslovu http://www.aon.com/risk-services/cyber.jsp
9. ARN. (2015). Top 10 most notorious cyber attacks in history. Najdeno 2. maja 2016 na spletnem naslovu http://www.arnnet.com.au/slideshow/341113/top-10-most-notorious-cyber-attacks-history/
10. Association for financial professionals. (2016). AFP Risk Survey. Najdeno 2. maja 2016 na spletnem naslovu http://www.afponline.org/risksurvey/
11. Balkhi, S. (2013). 25 Biggest cyber attacks in history. Najdeno 2. maja 2016 na spletni strani http://list25.com/25-biggest-cyber-attacks-in-history/
12. Barn, D. (2016). The development of cyber insurance. Najdeno 3. maja 2016 na spletnem naslovu http://www.cyberriskinsuranceforum.com/content/development-cyber-insurance Barn
13. Betterley. (2010). Understanding the Cyber Risk Insurance and Remediation Services Marketplace: A Report on the Experiences and Opinions of Middle Market CFOs. Najdeno 2. maja 2016 na spletnem naslovu http://betterley.com/samples.php
14. Betterley. (2015). The Betterley Report – Cyber/Privacy Insurance Market Survey 2015. Najdeno 2. maja 2016 na spletnem naslovu http://betterley.com/samples/cpims15_nt.pdf

15. Bijelić, M., Jerovšek, O., & Novak, D. (1998). *Zavarovanje in pozavarovanje*. Ljubljana: Art agencija.
16. Böhme, R., & Kataria, G. (2006). Models and Measures for Correlation in Cyber-Insurance. Working Paper. Workshop on the Economics of Information Security (WEIS). Najdeno 2. maja 2016 na spletnem naslovu https://archive.nyu.edu/bitstream/2451/14997/2/Infosec_ISR_Bohme%2bKataria.pdf
17. Bundt, M. (2016, april). The reinsurance perspective. Prezentacija na dogodku *Cyber risk too big to insure?*, Ruschlikon, Švica.
18. Cebula, J. J., & Young, L. R. (2010). A Taxonomy of Operational Cyber Security Risks, Technical Note CMU/SEI-2010-TN-028. Najdeno 2. maja 2016 na spletnem naslovu http://www.sei.cmu.edu/reports/10tn028.pdf
19. CEIOPS. (2009). CEIOPS' Advice for Level 2 Implementing Measures on Solvency II: SCR Standard Formula – Article 111 (f): Operational Risk. CEIOPS-DOC-45/09, Najdeno 2. maja 2016 na spletnem naslovu https://eiopa.europa.eu/CEIOPS-Archive/Documents/Advices/CEIOPS-L2-Final-Advice-on-Standard-Formula-operational-risk.pdf
20. CRO Forum. (2014, december). Cyber resilience, The cyber risk challenge and the role of insurance. Najdeno 2. maja 2016 na spletnem naslovu http://www.thecroforum.org/cyber-resilience-cyber-risk-challenge-role-insurance/
21. Cybernetics. (b.l.) V *Oxford Dictionaries.* Najdeno 2. maja 2016 na spletnem naslovu http://www.oxford dictionaries.com
22. Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal Information Security, 4*(2), 92–100. Najdeno 20. maja 2016 na spletnem naslovu http://www.scirp.org/journal/PaperInformation.aspx?paperID=30059
23. Eling, M., & Wirfs, J. H. (2016). *Cyber Risk: Too Big to Insure? Risk Transfer Options for a Mercurial Risk Class*. St. Gallen: Institute of Insurance Economics I.VW-HSG, University of St. Gallen.
24. European Commission. (2012). Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Najdeno 2. maja 2016 na spletnem naslovu http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
25. European Network and Information Security Agency. (2016, januar). ENISA Threat Landscape 2015. Najdeno 2. maja 2016 na spletnem naslovu https://www.enisa.europa.eu/publications/etl2015
26. Finkle, J., & Skariachan, D. (2013). Target cyber breach hits 40 million payment cards at holiday peak. Najdeno 2. maja 2016 na spletnem naslovu http://www.reuters.com/article/us-target-breach-idUSBRE9BH1GX20131219
27. Financial Services Sector Coordinating Council. (2016). Najdeno 2. maja 2016 na spletnem naslovu http://www.aba.com/Training/Conferences/Documents/NCCB16_Mon_Ins%20and%20Outs%20of%20Cyber%20Insurance_buyers%20guide.pdf

28. Fort, S. (2016, marec). Osiguranje cyber rizika. Prezentacija na konferenci *Cyber Risk*, Zagreb, Hrvaška.
29. Guy Carpenter. (2016). Cyber Insurance Solutions (interno gradivo). London: Guy Carpenter.
30. ISO standards. (b.l.). Najdeno 6. maja 2016 na spletnem naslovu http://www.iso.org/iso/ home/standards/management-standards/iso27001.htm
31. ISO Survey Report. (2014). Najdeno 6. maja 2016 na spletnem naslovu http://www.iso.org/iso/iso-survey
32. Labonte, M. (2010). The Size and Role of Government – Economic Issues, Congressional Research Service. Najdeno 2. maja 2016 na spletnem naslovu http://digitalcommons.ilr.cornell.edu/key_workplace/635/
33. Lloyd's. (2015). Business Blackout – The insurance implications of a cyber attack on the US power grid. Najdeno 2. maja 2016 na spletnem naslovu http://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf
34. Majuca, R. P., Yurcik, W., & Kesan, J. P. (2006). The evolution of cyberinsurance, working paper. Najdeno 2. maja 2016 na spletnem naslovu https://arxiv.org/ftp/cs/papers/0601/0601020.pdf
35. Marsh. (2014). Historical Development of Cyber (Re)Insurance. Najdeno 2. maja 2016 na spletnem naslovu http://www.gccapitalideas.com/2014/10 /23/
36. Marsh. (2016). Benchmarking Trends: Operational Risks Drive Cyber Insurance Purchases. Najdeno 2. maja 2016 na spletni strani https://www.marsh.com/us/insights/research/cyber-benchmarking-trends-2016.html
37. McAfee, & CSIS. (2013). The economic impact of cybercrime and cyber espionage. Najdeno 2. maja 2016 na spletnem naslovu http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf
38. McAfee, & CSIS. (2014). Net Losses: Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II. Najdeno 1. maja 2016 na spletnem naslovu http://www.mcafee.com/us/resources/reports/rp-
39. Olsen, T. (2013). Insurance Cyber risks. Najdeno 2. maja na spletnem naslovu http://www.pwc.dk/da/arrangementer/assets/cyber-tineolsen.pdf
40. Pace, G., Shapella, A., & Vernaci, G. (2015). Achieving Cyber Resilience. *The Geneva Risk Management Newsletter*. Najdeno 2. maja 2016 na spletnem naslovu https://www.genevaassociation.org/media/916146/ga2015-rm55.pdf
41. Ponemon Institute. (2015). 2015 Cost of Data Breach Study: Global Analysis. Najdeno 5. maja 2016 na spletnem naslovu http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03053wwen/SEW03053WWEN.PDF
42. PricewaterhouseCoopers. (2015). Insurance 2020 and beyond: Reaping the dividents of cyber resilience. Najdeno 2. maja 2016 na spletnem naslovu http://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf
43. Schlayer, A. (2015). Cyber insurance – a new product to ensure paremium growth? *Dnevi zavarovalništva v Sloveniji* (str. 5). Ljubljana: Slovensko zavarovalno združenje.

44. SI-CERT. (2012). Poročilo o omrežni varnosti za leto 2012. Najdeno 2. maja na spletnem naslovu https://www.cert.si/porocilo-o-omrezni-varnosti-za-leto-2012/
45. SI-CERT. (2014). Poročilo o omrežni varnosti za leto 2014. Najdeno 2. maja na spletnem naslovu https://www.cert.si/porocilo-o-omrezni-varnosti-za-leto-2014/
46. SI-CERT. (2015). Poročilo o omrežni varnosti za leto 2015. Najdeno 30. maja 2016 na spletnem naslovu https://www.cert.si/wp-content/uploads/2016/06/SI-CERT_LP_2015.pdf
47. Swiss Re. (2014). Gearing up for Cyber risk. Najdeno 2. maja 2016 na spletnem naslovu http://www.swissre.com/library/
48. Swiss Re. (2016). Cyber Liability: Features of a data breach. Najdeno 2. maja 2016 na spletnem naslovu http://www.swissre.com/library/
49. Verizon. (2014). Data breach investigation report. Najdeno 2. maja 2016 na spletnem naslovu http://www.nu.nl/files/Verizon.pdf#page=1&zoom=auto,-274,848
50. Verizon. (2015). Data breach investigation report. Najdeno 2. maja 2016 na spletnem naslovu https://msisac.cisecurity.org/whitepaper/documents/1.pdf
51. Verizon. (2016). Data breach investigation report. Najdeno 2. maja 2016 na spletnem naslovu http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/
52. Vlada Republike Slovenije (2016, februar). Strategija kibernetske varnosti. Najdeno 2. maja 2016 na spletni strani http://www.mizs.gov.si/fileadmin/mizs.gov.si/pageuploads/Informacijska_druzba/pdf/DSI2020_Strategija_Kibernetske_Varnosti.pdf
53. World economic forum. (2014). The Global Risk Report. Najdeno 2. maja 2016 na spletnem naslovu http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf
54. World economic forum. (2015). The Global Risk Report. Najdeno 2. maja 2016 na spletnem naslovu http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report 15. pdf
55. World economic forum. (2016). The Global Risk Report. Najdeno 2. maja 2016 na spletnem naslovu http://www3.weforum.org/docs/GRR/WEF_GRR16.pdf