UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

ANALIZA MOŽNOSTI ZAVAROVANJA KIBERNETSKIH TVEGANJ

Ljubljana, september 2016 DEJAN CAJHEN

IZJAVA O AVTORSTVU

Podpisani Dejan Cajhen, študent Ekonomske fakultete Univerze v Ljubljani, avtor predloženega dela z naslovom Analiza možnosti zavarovanja kibernetskih tveganj, pripravljenega v sodelovanju s svetovalcem prof. dr. Petrom Trkmanom

IZJAVLJAM

1. da sem predloženo delo pripravil 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 poskrbel, 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 pridobil vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označil;

7. da sem pri pripravi predloženega dela ravnal v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobil 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 05.09.2016 Podpis študenta:_____

KAZALO

KAZALO TABEL

KAZALO SLIK

UVOD

Informacijske in komunikacijske tehnologije so v zadnjih desetletjih prinesle koristi za podjetja, posameznike in družbo kot celoto. Internet oz. širše kibernetski prostor je postal temelj za široko paleto storitev in dejavnosti, ki so nam danes samoumevne. Za ponovni zagon evropskega gospodarstva je Evropska komisija leta 2010 sprejela Digitalno agendo, ki poudarja pomen zaupanja in varnosti v digitalne tehnologije ter potrebo po boljši zaščiti pred kibernetskimi napadi. Z resolucijo Evropskega parlamenta iz leta 2013 o strategiji Evropske unije za kibernetsko varnost pa se spodbuja odprt, varen in zanesljiv kibernetski prostor, ki omogoča konkurenčnost gospodarstva Evropske unije (v nadaljevanju EU).

Ob vedno večji družbeni odvisnosti od sodobnih tehnologij pri poslovanju se izjemno povečuje obseg osebnih in poslovnih informacij v lasti tretjih oseb (Subashini, Kavitha, 2011). Informacije, ki jih podjetja hranijo v digitalni obliki, so izpostavljene kršitvam zaupnosti s strani naklepnih hekerjev in neprevidnih zaposlenih. Stroški, ki nastanejo ob takšnih kršitvah, so lahko zelo visoki (Pearson, 2014).

Pravzaprav je vseprisotnost kibernetskega prostora pripeljala družbo do točke, kjer se veliko število tveganj, ki smo jim bili tradicionalno izpostavljeni v fizičnem svetu, danes pojavlja v kibernetskem prostoru (Refsdal, Solhaug & Stølen, 2015). V publikaciji »The Global Risk Report 2016« je tveganje kibernetskega napada (angl. *cyberattack*) uvrščeno med šest največjih globalnih ekonomskih tveganj, ki ogrožajo poslovanje podjetij.

Kibernetski kriminal je v porastu. Po nekaterih ocenah (McAfee, 2014) znaša letni strošek, ki ga utrpi svetovna ekonomija zaradi kibernetskega kriminala, več kot 400 milijard ameriških dolarjev (v nadaljevanju USD). Na osnovi konzervativne ocene znašajo stroški 375 milijard USD, medtem ko je najvišje ocenjeni znesek 575 milijard USD. Vlade in podjetja podcenjujejo izpostavljenost in hitro rast kibernetskega kriminala (McAfee, 2014).

Če so managerji tveganj, izvršni direktorji ali člani uprav v evropskih podjetjih v preteklosti še dvomili o rasti tveganja varovanja podatkov, se je njihova percepcija v zadnjem obdobju spremenila. Kršitve zaupnosti podatkov, ki so jih utrpele nekatere največje svetovne korporacije, in kibernetski napadi na državne institucije so postali stalnica. Kibernetski kriminal se stalno spreminja in izkorišča nove možnosti uporabe sodobnih tehnologij. Številna podjetja, ki so bila tarča kibernetskega napada, se ne sprašujejo »ali«, temveč »kakšna škoda je lahko povzročena«. Rezultat je povečan pomen managementa kibernetskih tveganj (angl. *cyber risk management*). V vedno več podjetjih se posvečajo managementu kibernetskih tveganj, pri čemer pridobiva pomen tudi prenos tveganj na zavarovalnice (Advisen, 2015). Povečuje se tudi zavedanje, da pri managementu tveganj ne gre le za zmanjševanje škode, ampak tudi za doseganje poslovne vrednosti (Trkman, Oliveira & McCormack, 2016).

Na osnovi globalne raziskave Ponemon Institute iz leta 2015 je povprečni strošek kršitve zaupnosti podatkov znašal 3,8 milijona USD. Ocenjena finančna škoda iz naslova 700 milijonov kompromitiranih podatkov, ki je znašala 400 milijonov USD, kaže na pomembnost ohranjanja zaupnosti podatkov, ene od kategorij kibernetskih tveganj.

Kljub temu je stopnja zavedanja poslovodstev o možnosti zavarovanja pred kibernetskimi tveganji še vedno na zelo nizki ravni. Na podlagi raziskave med družbami v Veliki Britaniji (Marsh, 2015), kjer je zavarovalni trg nadpovprečno razvit, lahko ugotovimo velik razkorak v percepciji stopnje zavarovaljivosti kibernetskega zavarovanja, saj večina v raziskavo vključenih predsednikov uprav družb meni, da imajo sklenjeno ustrezno zavarovanje, medtem ko je delež družb s kibernetskim zavarovanjem v resnici okoli 10-odstoten. Ocenjujem, da je največja prepreka za ustrezno umestitev kibernetskega tveganja v model managementa tveganj nezavedanje poslovodstev o spremembah globalnega okolja. Zato management kibernetskih tveganj ni ustrezno umeščen v organizacijsko strukturo podjetij in se običajno prenaša na nižje nivoje v strukturi managementa, največkrat na predstavnike oddelkov za informatiko.

Zavarovalnice so se ob pojavu novega tveganja odzvale s ponudbo kibernetskega zavarovanja (angl. *cyber insurance*), ki zagotavlja kritje škode oz. stroškov iz naslova kršitve zaupnosti podatkov (angl. *data breach*) in drugih posledic napadov hekerjev. Pri tem obstaja pomislek o vrednosti kibernetskega zavarovanja. V kolikor v podjetjih ne upoštevajo, na primer, osnovnih varnostnih standardov pri managementu kibernetskih tveganj, zavarovanje morda ne bo učinkovito pri managementu tveganj. Čeprav ima lahko kibernetsko zavarovanje koristno vlogo v strategiji managementa tveganj v podjetju, to ni zamenjava za osnovne preventivne ukrepe.

Po dolgoletnih pogajanjih so na nivoju EU decembra 2015 dosegli politični dogovor o reformi evropskega zakonodajnega okvira za varstvo osebnih podatkov. Aprila 2016 sta Evropski parlament in Svet EU potrdila zakonodajni sveženj, ki določa nov pravni okvir varstva osebnih podatkov v EU. Uredba o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov bo stopila v veljavo 2 leti po sprejemu, torej leta 2018. Ključne spremembe z vidika dodatnih obveznosti za podjetja so višje globe za hujše kršitve v višini do 20 milijonov evrov (v nadaljevanju EUR) oziroma 4 % svetovnega letnega prometa družbe ter postopki obveščanja nadzorne institucije in oškodovancev z novo teritorialno razsežnostjo (Uredba EU št. 679/2016 Evropskega parlamenta in Sveta EU). To daje dodatno težo kibernetskemu zavarovanju kot orodju za management tveganj, saj podjetja ob neuspelih preventivnih ukrepih preprečevanja kršitev zaupnosti podatkov zaradi kibernetskih napadov finančno breme postopkov in morebitnih kazni in glob nadzornih institucij ter odškodninskih zahtevkov oškodovancev lahko prenesejo na zavarovalnice.

Poleg novih zakonskih obveznosti bo na pomen ustreznega managementa kibernetskih tveganj v podjetjih vplival tudi hiter razvoj novih tehnologij (brezpilotna letala,

samovozeča vozila idr.) in družbenih omrežij ter fenomen Interneta stvari (angl. *internet of things*). Ocenjujejo, da bo število naprav v Internetu stvari z 1,2 milijarde v letu 2014 narastlo na 5,4 milijarde v letu 2020 (Verizon, 2015). Nekateri od pomembnih poslovnih trendov, kot so razmah analitike podatkov, digitalizacija poslovnih funkcij in prepletenost ponudbe storitev po različnih panogah, so razširile uporabo tehnologij in podatkov, kar ustvarja več tveganja kot kadar koli.

Namen magistrskega dela je s pomočjo predvsem tuje strokovne literature opredeliti vlogo zavarovanja v okviru managementa kibernetskih tveganj in ugotoviti, ali slovenska podjetja ustrezno umeščajo kibernetska tveganja v proces managementa tveganj, njihovo percepcijo o kibernetskih tveganjih in stopnjo zavedanja o možnosti prenosa dela tveganj na zavarovalnice v primerjavi z drugimi državami. Predvsem pa želim ugotoviti, ali se slovenska podjetja zavedajo kibernetskih tveganj, in spodbuditi deležnike (lastnike, regulatorje, interesna združenja in širšo javnost) k večjemu zavedanju in razumevanju tveganja izgube ugleda podjetja, ki je lahko ena izmed hujših posledic kibernetskega incidenta.

S pomočjo pregleda literature in globinskih intervjujev bom zato poskusil potrditi ali ovreči hipotezo, da predstavlja zavarovanje ustrezno orodje za management kibernetskih tveganj. Pri tem izhajam iz osnovne predpostavke, da prenos kibernetskih tveganj na zavarovalnice ni alternativa ostalim metodam managementa tveganj, temveč njihova dopolnitev. Hkrati želim raziskati, ali imajo obravnavana podjetja ustrezno umeščeno funkcijo managementa tveganj, ki bi primerno naslavljala ključna tveganja. Ker trenutno empiričnih spoznanj s področja managementa kibernetskih tveganj z uporabo zavarovanja kljub vedno večji relevantnosti za poslovanje v Sloveniji ni, pa je dodatni cilj dela tudi okvirna identifikacija stanja na področju managementa kibernetskih tveganj v izbranih slovenskih podjetjih.

Magistrsko delo v prvem delu temelji na poglobljenem teoretično-analitičnem pregledu strokovne literature, znanstvenih razpravah in raziskavah, empiričnih spoznanjih, aplikativne zakonodaje ter člankov, predvsem tujih strokovnjakov, s področja obravnavane teme. Poleg kritične analize strokovno teoretičnih dognanj so zaradi lažjega razumevanja za ilustracijo navedeni tudi praktični primeri iz strokovne literature in člankov.

Ta del magistrskega dela je analiziran s pomočjo opisne metode, interpretacije primarnih ter sekundarnih virov in metode kompilacije, s katero so združena spoznanja številnih avtorjev in organizacij predvsem s področja managementa kibernetskih tveganj in kibernetskega zavarovanja v svetu, zlasti pa iz Združenih držav Amerike (v nadaljevanju ZDA) in EU, saj je korporativno upravljanje in zavarovalništvo tam najbolj razvito.

Zadnji del magistrskega dela je namenjen raziskavi managementa kibernetskih tveganj v Sloveniji z uporabo globinskih intervjujev. Intervjuji so bili opravljeni s predstavniki izbranih slovenskih podjetij, ki so zadolženi za management kibernetskih tveganj ali

odgovorni za varstvo osebnih oz. poslovnih podatkov. Glede na nadpovprečno izpostavljenost finančnih institucij in trgovskih družb pred kibernetskimi tveganji so v raziskavo vključene banke, zavarovalnice in trgovska podjetja.

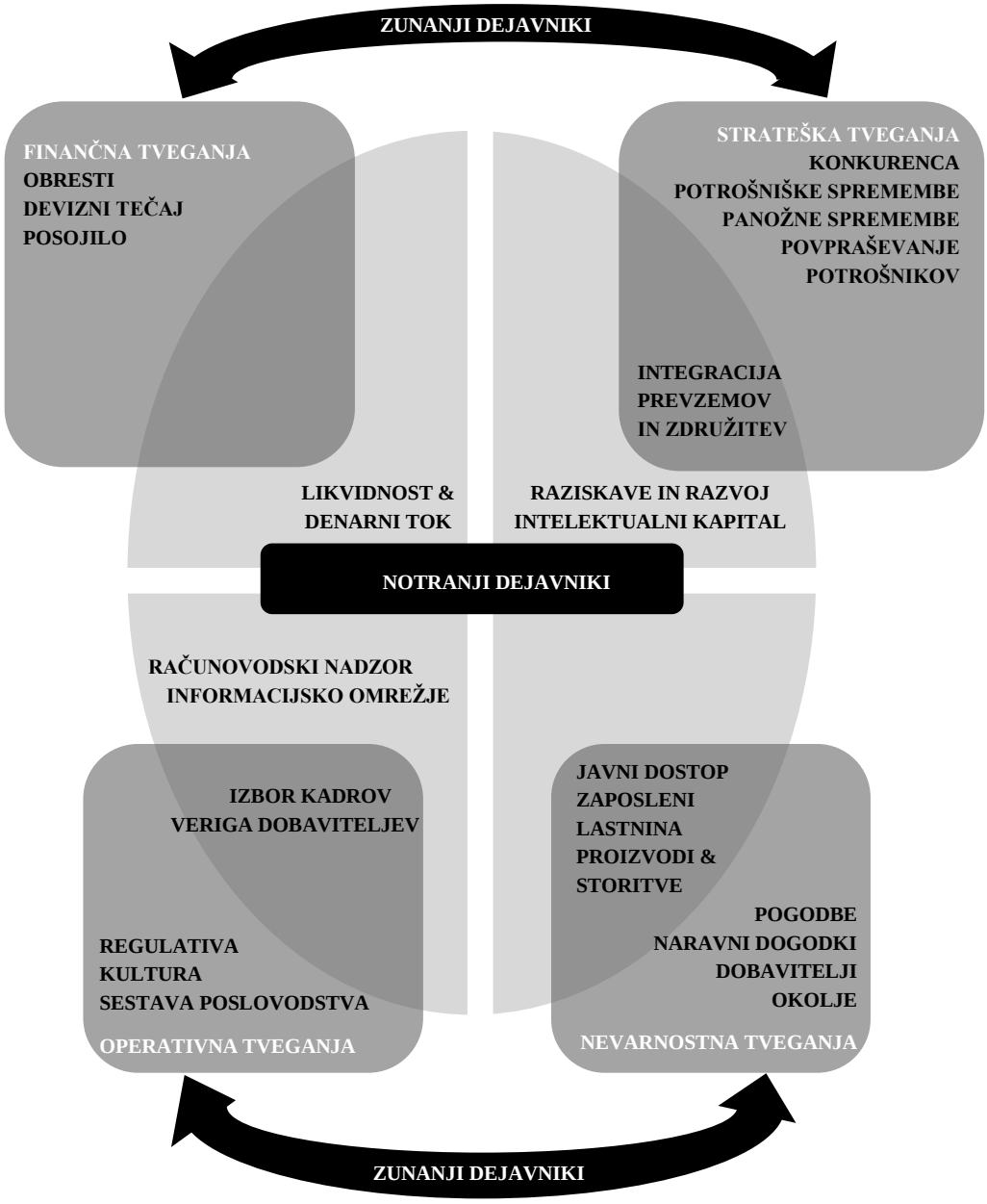
Magistrsko delo je sestavljeno iz štirih poglavij. V uvodu je predstavljena obravnavana problematika in navedeni razlogi za povečana kibernetska tveganja, s katerimi se soočajo podjetja. V prvem poglavju so predstavljeni nekateri temeljni pojmi in model managementa tveganj, saj brez poznavanja teoretičnih modelov managementa ne moremo razumeti modela managementa kibernetskih tveganj, ki vključuje tudi prenos tveganj na zavarovalnice. V drugem poglavju magistrskega dela so opredeljena kibernetska tveganja in predstavljen model managementa kibernetskih tveganj. Posebni podpoglavji sta namenjeni pregledu stanja managementa kibernetskih tveganj v praksi in poskusu napovedi razvoja managementa kibernetskih tveganj. V tretjem poglavju je zapisana vloga kibernetskega zavarovanja v procesu managementa tveganj, opredelitev kibernetskega zavarovanja, pregled stanja na zavarovalnem trgu in predstavljeni izzivi v prihodnje. Četrto poglavje je namenjeno raziskavi managementa kibernetskih tveganj v izbranih slovenskih podjetjih. Predstavljeni so rezultati globinskih intervjujev, ki nazorno prikazujejo, kakšni so pristopi k managementu kibernetskih tveganj in kakšen dostop imajo podjetja do zavarovalnega trga. V tem delu je opisano okolje za uvedbo prenosa tveganja na zavarovalni trg, tako z vidika razvitosti slovenskega zavarovalništva kot tudi z vidika veljavnih pravnih norm.

1 OPREDELITEV MANAGEMENTA TVEGANJ

Tveganje lahko opredelimo kot kombinacijo verjetnosti dogodka in njegovih posledic. V vseh oblikah podjetij obstaja možnost dogodkov in posledic, ki predstavljajo priložnosti za koristi ali nevarnosti za uspeh. Na področju varnosti je splošno sprejeto, da so lahko posledice le negativne. Zato je management varnostnih tveganj osredotočen na preprečevanje in ublažitev škode (FERMA, 2003, str. 3).

Management tveganj je osrednji del katerega koli strateškega managementa organizacije. Gre za proces, kjer podjetje premišljeno naslovi tveganja, ki se nanašajo na njihove dejavnosti, z namenom doseganja vzdržne koristi znotraj vsake dejavnosti in v okviru portfelja vseh dejavnosti. Osrednje vodilo dobrega managementa tveganj je identifikacija in obravnava predmetnih tveganj. Cilj je največja trajna dodana vrednost vseh dejavnosti podjetja. Management tveganj mora biti stalen in razvijajoč proces, ki se odvija preko strategije podjetja in njene implementacije. Ključna je vpetost v kulturo podjetja z učinkovito politiko in vodenjem programa s strani najvišjega poslovodstva. Zagotovljen mora biti prenos strategije v taktične in operativne cilje, določanje odgovornosti skozi celotno podjetje z odgovornim poslovodstvom in zaposlenimi, ki so zadolženi za management tveganj v okviru opisa njihovih delovnih nalog (IRM, 2002, str. 2).

Slika 1: Primeri ključnih tveganj



Vir: FERMA, A Risk Management Standard, 2003, str. 4.

Podjetja in njihovo poslovanje so izpostavljena tveganjem, ki so lahko posledica zunanjih in notranjih dejavnikov. Nadalje lahko opredelimo vrste tveganj kot strateške, finančne, operativne in nevarnostne (IRM, 2002, str. 2). Na Sliki 1 so povzeti primeri ključnih tveganj po vrsti tveganja. Iz prikaza je razvidno, da so določena tveganja lahko posledica skupnega delovanja zunanjih in notranjih dejavnikov in zato prekrivajo obe področji.

V Sloveniji management tveganj v podjetjih opredeljuje Zakon o gospodarskih družbah (Ur. l. RS, št. 42/2006, v nadaljevanju ZGD-1). ZGD-1 zahteva, da mora podjetje v poslovnem poročilu navesti najpomembnejša tveganja, s poudarkom na opisu bistvenih

finančnih tveganj, ki jim je podjetje izpostavljeno. V odvisnosti od presoje premoženja in obveznosti podjetja je potrebno prikazati cilje in ukrepe upravljanja tveganj družbe. Poleg tega je v okviru letnih poročil potrebno tudi razkritje tveganj, v kolikor je to nujno za oceno finančnega stanja družbe. Nadalje je med nalogami revizijske komisije navedeno tudi spremljanje sistemov za management tveganj.

Harrington in Niehaus (2003, str. 4) opredelita management poslovnih tveganj kot skrb za obvladovanje možnega znižanja poslovne vrednosti podjetja zaradi katerega koli vzroka. Poslovna vrednost za lastnike podjetja, ki se lahko odraža v tržni kapitalizaciji podjetja, je v osnovi odvisna od pričakovane velikosti, trenutka in spremenljivosti tveganj, povezanih s prihodnjimi neto denarnimi tokovi podjetja. Nepričakovane spremembe v pričakovanih prihodnjih neto denarnih tokovih so glavni razlog za nihanje poslovne vrednosti. Glavna poslovna tveganja, ki povečujejo spremenljivost denarnih tokov in poslovne vrednosti, so cenovno tveganje (angl. *price risk*), kreditno tveganje (angl. *credit risk*) in čisto tveganje (angl. *pure risk*).

1.1 Model managementa tveganj

Ne glede na vrsto obravnavanega tveganja proces managementa tveganj vključuje sledeče ključne korake (Harrington & Niehaus, 2003, str. 8–9):

1. identifikacija vseh ključnih tveganj,
2. ocena možne škodne pogostosti in višine škode,
3. razvoj in izbira metod managementa tveganj,
4. izvedba izbranih metod managementa tveganj,
5. stalni nadzor učinkovitosti in ustreznosti metod managementa tveganj in strategij.

V Tabeli 1 so povzete glavne metode managementa tveganj, ki se medsebojno ne izključujejo in jih lahko razvrstimo kot (1) omejevanje škod, (2) financiranje škod in (3) interno zmanjševanje tveganj. Omejevanje škod in interno zmanjševanje tveganj običajno vključujeta odločitve o investicijah v sredstva, ki zmanjšujejo pričakovane škode. Odločitve o financiranju škod pa se nanašajo na vprašanje, kako finančno nadomestiti posledice škode.

Tabela 1: Metode managementa tveganj

Omejevanje škod	**Financiranje škod**	**Interno zmanjševanje tveganj**
Znižan nivo tveganih aktivnosti	Lastni delež	Diverzifikacija
Povečanje previdnosti	Zavarovanje	Investicije v informacije
	Pogodbeno zniževanje tveganja	
	Drugi pogodbeni prenosi tveganja	

Vir: E. S. Harrington & R. G. Niehaus, Risk Management and Insurance, 2003, str. 9.

Dejanja, ki znižujejo pričakovane stroške škod z znižanjem frekvence škod in/ali obsega škod opredelimo kot **omejevanje škod**. Dejanja, ki primarno vplivajo na škodno pogostost se običajno imenujejo metode škodne prevencije, medtem ko dejanja, ki primarno vplivajo na višino škode, imenujemo metode zniževanja škod. Večina načinov omejevanja škod vpliva tako na škodno pogostost kot tudi na višino škod.

Gledano z drugega zornega kota obstajata dva splošna pristopa omejevanja škod, in sicer znižanje nivoja tveganih aktivnosti in povečanje previdnosti za preprečitev škode. Omejevanje tveganih aktivnosti primarno učinkuje na škodno pogostost. V skrajnem primeru se z opustitvijo dejavnosti škodna izpostavljenost lahko popolnoma odpravi. Takšno strategijo imenujemo izogibanje tveganjem. Drugi glavni pristop k omejevanju škod je povečanje nivoja previdnosti za določen nivo tveganih dejavnosti. Cilj je zagotoviti varnejšo dejavnost in tako zmanjšati škodno pogostost in višino škode (Harrington & Niehaus, 2003, str. 10).

Za zagotovitev sredstev za plačilo ali nadomestilo nastalih škod se uporabljajo metode **financiranja škod**, navedene v Tabeli 1. Pri lastnem deležu podjetje zadrži del ali celotno obveznost plačila škode. Ob obstoju formaliziranega načrta financiranja škod se lastni delež imenuje samozavarovanje.

Druga metoda financiranja škod je sklenitev zavarovanja. Običajna zavarovalna pogodba vsebuje obveznost zavarovalnice za zagotovitev sredstev za plačilo škode v primeru nastanka zavarovalnega primera v zameno za plačilo zavarovalne premije ob sklenitvi pogodbe. Z zavarovalno pogodbo se zniža tveganje zavarovanca s prenosom dela tveganja nastanka škode na zavarovatelja. Zavarovatelj na drugi strani zniža tveganje preko diverzifikacije.

Tretja metoda je pogodbeno varovanje pred tveganjem (angl. *hedging*). Finančni derivativi, kot so terminske pogodbe (angl. *forwards*), standardizirane terminske pogodbe (angl. *futures*), opcije (angl. *options*) in zamenjave (angl. *swaps*), se uporabljajo za management

različnih vrst tveganj, predvsem cenovnega tveganja. Nekateri derivati so se začeli uporabljati tudi pri managementu čistega tveganja.

Četrta metoda je uporaba ene ali več različic drugih pogodbenih prenosov tveganj, ki podjetjem omogoča prenos tveganja na drugo osebo. Največkrat se uporabljajo pogodbena določila o dogovoru o povrnitvi škode oz. prenosu odgovornosti (angl. *hold harmless*) in dogovoru o varovanju pred zahtevki tretjih oseb (angl. *indemnity agreements*), ki od izvajalca zahtevajo zaščito naročnika pred izgubo finančnih sredstev zaradi tožbe, ki izvira iz dejanj izvajalca.

Poleg metod, ki omogočajo zmanjševanje tveganj s prenosom na drugo osebo, lahko podjetja tudi **interno zmanjšujejo tveganja**. Prva metoda je diverzifikacija aktivnosti podjetja po znanem načelu: »ne nosi vseh jajc v eni košari«. Druga metoda je investiranje v informacije za zagotovitev boljše napovedi pričakovanih škod. Takšne investicije lahko zagotovijo natančnejše ocene ali napovedi prihodnjih denarnih tokov in s tem znižajo spremenljivost denarnih tokov glede na pričakovano vrednost (Harrington & Niehaus, 2003, str. 11).

Zveza evropskih združenj za management tveganj (FERMA, 2003) svojim članom priporoča upoštevanje standarda managementa tveganj, ki predstavlja najboljšo prakso s tega področja. V okviru standarda je definiran postopek managementa tveganj, ki vključuje oblikovanje in prilagoditev:

- strateških ciljev podjetja,
- ocene tveganja,
- poročanja o tveganjih,
- odločanja,
- obravnavo tveganj,
- poročanja o preostalem tveganju,
- nadzora.

V okviru ocene tveganja so predvideni postopki analize tveganj in ovrednotenja tveganj. Analiza tveganj vključuje:

- Identifikacijo tveganja, ki je namenjena prepoznavanju izpostavljenosti podjetja negotovosti. To zahteva temeljito poznavanje podjetja, trga, na katerem deluje, pravno, socialno, politično in kulturno okolje, v katerem obstaja, kot tudi razvoj razumevanja strateških in operativnih ciljev podjetja.
- Opis tveganja, katerega namen je prikaz identificiranih tveganj v strukturirani obliki, z uporabo tabele.
- Ovrednotenje tveganja, ki je lahko kvantitativno, polkvantitativno ali kvalitativno v smislu verjetnosti nastanka dogodka in možnih posledic (FERMA, 2003).

2 KIBERNETSKA TVEGANJA

World Economic Forum v svojem zadnjem poročilu o globalnih tveganjih »The Global Risks Report 2016« izpostavlja kibernetski kriminal, ki globalni ekonomiji povzroči za 445 milijard USD škode (letno). Iz poročila (World Economic Forum, 2016, str. 77) je razvidno, da je kibernetski napad zaznan kot najbolj zaskrbljujoče tveganje v nekaterih vodilnih svetovnih gospodarstvih: na Japonskem, v Nemčiji, na Nizozemskem, v Singapurju, Švici in ZDA. Raziskava je bila opravljena na osnovi mnenja več kot 13.000 managerjev v 140 državah.

Večja podjetja, vlade in javno-storitvene organizacije so že bili tarča kibernetskih kriminalcev ali pa tako imenovanih hektivistov (angl. *hacktivists*). Od leta 2005 je bilo prijavljenih 5.029 incidentov kršitve zaupnosti podatkov v ZDA, kjer so organizacije zavezane k poročanju regulatorjem, vključujoč ocenjenih 675 milijonov podatkov. Statistični podatki za države izven ZDA so pomanjkljivi, vendarle je bilo po nekaterih ocenah od leta 2005 v Evropi vsaj 200 kršitev, ki zajemajo 227 milijonov podatkov (Allianz, 2015).

Povečanje zavedanja kibernetskega tveganja je razvidno iz poročila zavarovalnice Allianz, ki v letošnji letni globalni raziskavi Allianz Risk Barometer izpostavlja kibernetsko tveganje z največjim skokom na lestvici največjih poslovnih tveganj. Kibernetsko tveganje je od leta 2013, ko je s 6 % med vsemi zbranimi možnimi odgovori za največja poslovna tveganja zasedlo šele 15. mesto, v treh letih napredovalo na 3. mesto, z 28-odstotno potrditvijo v raziskavi sodelujočih podjetij. Hkrati so podjetja umestila kibernetska tveganja na prvo mesto med tveganji prihodnosti. Na podlagi odgovorov je izguba ugleda, ki je posledica kibernetskega incidenta (69 %), glavni vzrok za ekonomsko škodo, sledi obratovalni zastoj (60 %) in zahtevki iz naslova odgovornosti zaradi kršitve zaupnosti podatkov (52 %). Pomanjkanje razumevanja kompleksnosti obravnavanega tveganja (48 %) je navedeno kot glavni razlog, ki ovira podjetja pri boljši pripravljenosti za obrambo pred kibernetskimi nevarnostmi. Sledita neobstoj ocene stroškov, povezanih s predmetnim tveganjem (46 %), in omejenost sredstev (39 %) (Allianz, 2016, str. 10).

Podjetja morajo poleg navedenih nevarnosti, ki so jim izpostavljena, upoštevati tudi vpliv posledic kibernetskih incidentov pri svojih ključnih dobaviteljih. Povečuje se tudi uporaba zunanjih izvajalcev storitev ali ponudnikov infrastrukture v oblaku (angl. *cloud services*). Uporaba tovrstnih storitev sama po sebi niti ne poveča niti ne zmanjša stopnje tveganja. Potrebno je zagotoviti enako učinkovito nadzorovano okolje, tudi v primeru prenosa »v oblak« (Williams, 2014, str. 11).

Kibernetsko tveganje je po raziskavi Allianz Risk Barometer (Allianz, 2015) najbolj podcenjeno tveganje s strani podjetij, saj so na tovrstna tveganja najmanj pripravljena. Podjetja se ne zavedajo posledic kibernetskega napada ali incidenta. Ta ima lahko vpliv na njihovo oskrbovalno verigo, lahko so odgovorni v primeru nedobave svojih izdelkov v

predvidenem roku ali če izgubijo podatke strank, povečane stroške odvetnikov, strokovnjakov informacijske tehnologije (v nadaljevanju IT) in odnosov z javnostmi (v nadaljevanju PR). Še vedno obstaja napačna predstava, da so velika podjetja večkrat tarča kibernetskih napadov zaradi potencialno večje finančne nagrade za napadalce. Vendar so kibernetski napadi postali vsakodnevni dogodek, ki zadeva majhna, srednja in velika podjetja.

2.1 Opredelitev kibernetskega tveganja

Na področju terminološke opredelitve pojmov, povezanih s kibernetskim tveganjem, ni enotnega pristopa. Različni avtorji uporabljajo različne definicije. Biener, Eling in Wirfs (2015) izraz kibernetski (angl. *cyber*) opredelijo kot okrajšavo za besedo kibernetski prostor (angl. *cyberspace*), ki se na splošno pojmuje kot medsebojno povezano področje, ki je sestavljeno iz vseh digitalnih omrežij za shranjevanje, obdelavo in prenos informacij. Vključuje vsa informacijska omrežja za podporo poslovanja, infrastrukture in storitev.

Williams (2014, str. 10) s kibernetskim tveganjem opredeli možnost kakršne koli finančne izgube, motnje ali padec ugleda organizacije oziroma podjetja zaradi odpovedi informacijskega sistema. Takšno tveganje se lahko pojavi zaradi:

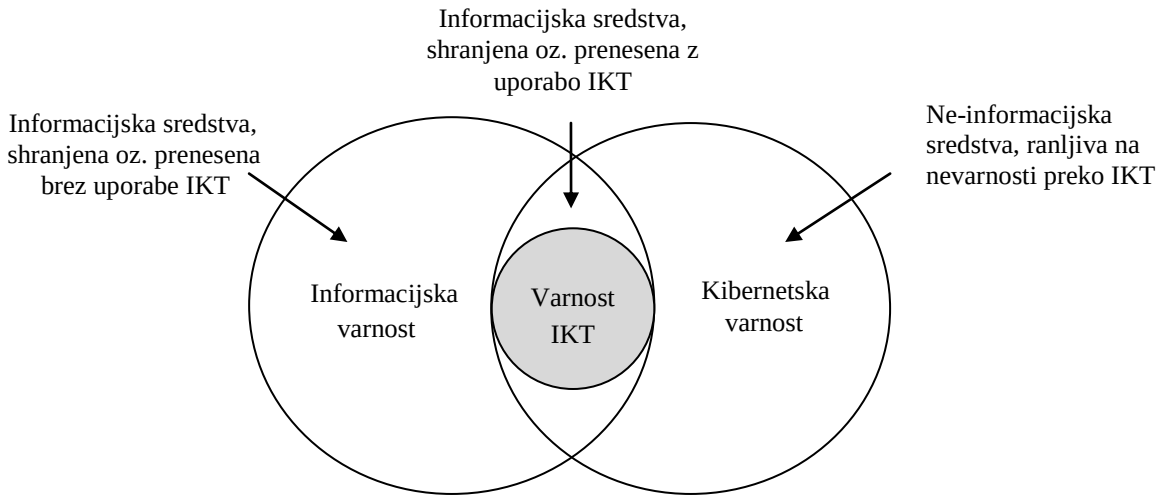
- namerne in nepooblaščene kršitve varnosti dostopa do informacijskih sistemov, z namenom vohunjenja, izsiljevanja in osramotitve,
- nenamerne ali naključne kršitve varnosti, ki vseeno lahko predstavlja izpostavljenost,
- operativnega IT-tveganja, posledice nezadostne sistemske celovitosti.

Izraz kibernetsko tveganje se nanaša na množico različnih virov tveganj, ki vplivajo na informacijska in tehnološka sredstva v podjetju. Kibernetska tveganja med drugimi vključujejo krajo identitete, razkritje občutljivih informacij in obratovalni zastoj. Nekatere definicije podajajo ozko opredelitev kibernetskega tveganja, in sicer kot tveganje, povezano z zlonamernimi elektronskimi dogodki, ki povzročajo prekinitev poslovanja in monetarno izgubo. Ob širšem pogledu lahko kibernetsko tveganje definiramo kot tveganje informacijske varnosti oziroma tveganje, ki izvira iz nedelovanja informacijskega omrežja (Biener, Eling & Wirfs, 2015).

Informacijska varnost (angl. *information security*) je zaščita zaupnosti, celovitosti in razpoložljivosti informacij, ki so lahko v kakršni koli pojavni obliki (elektronski, fizični ali kot znanje zaposlenih). Na drugi strani kibernetska varnost (angl. *cybersecurity*) predstavlja zaščito pred nevarnostmi v kibernetskem prostoru. Vendar kibernetska varnost ni omejena samo na informacijska sredstva, temveč vključuje tudi infrastrukturo in sredstva kot so življenje, zdravje, ugled in drugo (Refsdal, Solhaug & Stølen, 2015). Podobno razmejitev med informacijsko varnostjo in kibernetsko varnostjo opredelita tudi Von Solms in Van Niekerk (2013), ki dodatno umestita z grafičnim prikazom, kot razvidno iz Slike 2, še pojem varnosti informacijsko-komunikacijske tehnologije (v nadaljevanju

IKT). Varnost IKT zagotavlja zaščito dejanskega tehnološkega omrežja, na katerem so običajno shranjene in prenesene informacije.

Slika 2: Razmerja med varnostjo IKT, informacijske varnosti in kibernetske varnosti



Vir: R. Von Solms & J. Van Niekerk, From Information Security to Cyber Security, 2013, str. 101, slika 4.

V najširši obliki se kibernetsko tveganje povezuje s tveganjem informacijske tehnologije (angl. *information technology*). To pomeni povezavo poslovnih tveganj z uporabo, lastništvom, delovanjem, vpletenostjo, vplivom in sprejemanjem IT znotraj podjetja. Takšna široka definicija je smiselna, saj podoben razplet lahko nastane pri IT-dogodku, ne glede na to, ali je vzrok zlonameren ali ne in ali se je pojavil preko interneta ali izvira iz internih sistemov (Marsh, 2015, str. 8). S to definicijo se tudi najbolj približamo vsebini zavarovalnega kritja, ki ga zajema kibernetsko zavarovanje.

Cebula in Young (2010) sta definicijo kibernetskega tveganja povzela po kategorizaciji nadzornikov zavarovalnih in finančnih trgov in jo smatrata kot široko. Kibernetska tveganja opredelita kot **operativna tveganja**. Nadalje se omejita na operativna tveganja, ki so bistvena za informacijska in tehnološka sredstva. Zato kibernetsko tveganje opredelita kot operativno tveganje za informacijska in tehnološka sredstva, ki kot posledica vplivajo na zaupnost, razpoložljivost ali celovitost informacije oz. informacijskih sistemov. Skladno z okvirjem operativnih tveganj, zapisanih v dokumentih Basel II in Solventnost II, sta kibernetska tveganja kategorizirala v štiri skupine:

- dejanja ljudi,
- odpoved sistemov in tehnologije,
- neustrezni notranji procesi,
- zunanji dogodki.

Harrington in Niehaus (2003, str. 5) med glavna poslovna tveganja uvrstita tudi čisto

tveganje. V okviru glavnih vrst čistih tveganj (angl. *pure risk*) navajata med drugim tveganje znižanja vrednosti poslovnih sredstev zaradi fizične škode, kraje in prisvojitve ter tveganje pravne odgovornosti za škodo, ki jo utrpijo kupci, dobavitelji, lastniki in drugi.

Skupne značilnosti čistih tveganj, ki jih večinoma lahko pripišemo tudi kibernetskim tveganjem, vključujejo naslednje (Harrington & Niehaus, 2003, str. 6–7):

- Škode iz naslova uničenja premoženja, pravne odgovornosti in drugih nevarnosti imajo pogosto potencial, da so zelo velike glede na razpoložljiva sredstva in celo ogrozijo obstoj podjetja.
- Osnovni vzroki škod, povezani s čistimi tveganji, so pogosto zelo značilni za posamezno podjetje in so odvisni od dejanj podjetja. Zato lahko podjetja z dejanji, ki spremenijo vzroke za nastanek škode, znatno zmanjšajo škodno pogostost in višino škode. Pri drugih vrstah poslovnih tveganj podjetja večinoma ne morejo omejiti osnovnih vzrokov škod.
- Podjetja zmanjšajo negotovost in financirajo škode, povezane s čistimi tveganji, s sklenitvijo zavarovalne pogodbe z zavarovalnico, ki je specializirana za oceno in prevzem čistih tveganj.
- Za razliko od drugih vrst tveganj povzročijo škode iz naslova čistih škod znižanje skupnega družbenega premoženja.

Refsdal, Solhaug in Stølen (2015) definirajo kibernetsko tveganje kot tveganje, ki je posledica kibernetske nevarnosti. Z vidika zavarovanja so pomembne tri značilnost kibernetskih tveganj, ki jih posamično sicer lahko zasledimo pri različnih tveganji, vendar jih kibernetska tveganja združujejo na svojstven način (Lloyd's, 2015, str. 3):

- Sistemska izpostavljenost – digitalna omrežja in skupne tehnologije tvorijo povezave, ki jih kibernetski napadalci lahko izkoristijo in povzročijo obsežne posledice.
- Neopredmetena nevarnost – na podlagi raziskav je razvidno, da žrtve kibernetskih napadov spoznajo, da so bile tarča napada šele nekaj mesecev ali celo let po dogodku. Največkrat se nikoli ne ugotovi izvorne lokacije kibernetskega incidenta.
- Dinamična narava grožnje – kibernetski napadi se pogosto smatrajo kot problem tehnologije, vendar so posledica človekovih dejanj z namenom onemogočanja varnostnih mehanizmov.

2.1.1 Kategorije kibernetskih nevarnosti

Ruffle, Coburn, Ralph in Bowman (2013, str. 6) kibernetske nevarnosti razvrstijo zelo na splošno, na dejanja vojskovanja, terorizma in kriminala ali kot nezlonamerna.

Tabela 2: Kategorije kibernetskih nevarnosti

Kategorija	**Podkategorija**	**Primer**
Zaupnost	Vohunjenje	Podjetja, ki iščejo informacije o konkurentih. Vladne službe, vpletene v aktivnosti vohunjenja proti tujim državam in posameznikom.
	Kraja osebnih podatkov	Napad z zvabljanjem (angl. *phishing attack*) s ciljem zavesti uporabnike v razkritje osebnih podatkov, kot so številka bančnega računa; računalniški virusi, ki zapišejo in naložijo takšne informacije z uporabnikove naprave.
	Kraja identitete	Trojanski konji in drugo, uporabno za krajo identitete, ki je potem uporabljena pri izvršitvi kaznivih dejanj.
	Podatkovno rudarjenje	Tehnike odprte kode, uporabne za odkrivanje npr. osebnih informacij iz javno dostopnih podatkov.
	Prevara	Največkrat dostavljena preko nezaželene pošte, kot tudi poskusi prepričevanja prejemnikov za nakup lažnih izdelkov ali storitev.
Celovitost	Propaganda/ Dezinformacija	Sprememba ali manipulacija podatkov ali predstavitev nasprotujočih podatkov z namenom vpliva političnega ali poslovnega izida ali destabilizacije tujega režima.
	Ustrahovanje	Napad na spletne strani z namenom prisile njihovih lastnikov v brisanje ali spreminjanje vsebine ali zasledovanje drugih ciljev.
	Uničenje	Trajno uničenje podatkov z namenom škodovanja konkurentom ali napada tujih oblasti, kar lahko vodi do širšega konflikta.
Razpoložljivost	Zunanje informacije	Napad v obliki zavrnitve storitve na vladne ali zasebne storitve, ki so dostopne javnosti, npr. mediji, vladne strani za obveščanje.
	Notranje informacije	Napadi na zasebne ali vladne intranetne strani, npr. storitve nujne pomoči, energetsko in transportno nadzorno infrastrukturo, e-bančne strani, elektronsko pošto, sisteme za vodenje in nadzor.

Vir: D. Canham, Governance of Cyber Threat, 2014, str. 47.

Pri oceni kibernetskega okolja je koristno upoštevati kategorije kibernetskih nevarnosti: zaupnost, celovitost in razpoložljivost (angl. *confidentiality, integrity and availability*). Tabela 2 omogoča vpogled v možne vrste napadov in utemeljuje, za razliko od uveljavljenega pogleda na kibernetske nevarnosti, da niso vsi napadi motivirani za pridobitev protipravne premoženjske koristi.

2.1.2 Viri kibernetskih tveganj

Organizacije vseh velikosti, tako v javnem kot privatnem sektorju, so vedno bolj odvisne od informacijskih in tehnoloških sredstev, ki s pomočjo ljudi in obratnih sredstev izvršujejo poslovne procese za zagotavljanje storitev. Odpoved delovanja teh sredstev ima neposredni negativni vpliv na poslovne procese, ki jih omogočajo. To lahko vodi v

nezmožnost zagotavljanja storitev, kar nazadnje vpliva na poslanstvo organizacije. Ob upoštevanju teh povezav je management tveganj v povezavi s temi sredstvi ključni dejavnik za uspešnost poslovanja (Cebula & Young, 2010). V Tabeli 3 so kibernetska tveganja, sistematično razvrščena v štiri vrste virov tveganj: (1) dejanja ljudi, (2) odpoved sistemov in tehnologije, (3) nedelovanje internih postopkov in (4) zunanji dogodki.

Tabela 3: Viri kibernetskih tveganj po Cebula in Young

Vrsta	**Opis**	**Elementi**
Dejanja ljudi		
1.1 Nenamerno/Slučajno	Nenamerno delovanje brez zlonamernega ali škodljivega namena.	Napake, napačna ravnanja in opustitve.
1.2 Namerno	Namerno delovanje z namenom škodovanja.	Prevara, sabotaža, kraja in vandalizem.
1.3 Neodzivnost	Nedelovanje ali odpoved odziva v določeni situaciji.	Pomanjkanje ustreznih veščin, znanja, navodil in razpoložljivost osebja za odziv.
Odpoved sistemov in tehnologije		
2.1 Strojna oprema	Tveganja, ki so posledica napak v strojni opremi.	Odpoved zaradi kapacitete, zmogljivosti, vzdrževanja in zastarelosti.
2.2 Programska oprema	Tveganja, ki izvirajo iz vseh vrst sredstev programske opreme, vključno s programi, aplikacijami in operacijskimi sistemi.	Kompatibilnost, upravljanje konfiguracije, sprememba nadzora, varnostne nastavitve, praksa kodiranja in testiranje.
2.3 Sistemi/Omrežje	Nedelovanje povezanih sistemov, kot je bilo pričakovano.	Načrtovanje, specifikacije, integracija in kompleksnost.
Nedelovanje internih postopkov		
3.1 Načrtovanje procesov ali izvedba	Nedelovanje procesov za doseganje želenih rezultatov zaradi slabega načrtovanja procesov ali izvedbe.	Prenos postopka, dokumentacija postopka, vloge in zadolžitve, obvestila in opozorila, prenos informacij, izpostavljanje težav, dogovor o ravni storitev in prenos zadolžitev.
3.2 Nadzorni postopki	Neustrezen nadzor delovanja procesa.	Nadzor stanja, meritve, obdobno preverjanje in lastništvo procesa.
3.3 Podporni postopki	Odpoved organizacijske podpore procesov za zagotavljanje ustreznih virov.	Kadrovanje, računovodstvo, usposabljanje in razvoj ter nabava.

se nadaljuje

Tabela 3: Viri kibernetskih tveganj po Cebula in Young (nad.)

Vrsta	Opis	Elementi
Zunanji dogodki		
4.1 Katastrofe	Dogodki, naravnega in človeškega izvora, na katere organizacija ne more vplivati in ki se lahko zgodijo brez opozorila.	Vremenski pojav, požar, poplava, potres, nemiri.
4.2 Pravna vprašanja	Tveganja, ki izhajajo iz pravnih vprašanj.	Skladnost z zakonodajo, zakonodaja in pravdni spori.
4.3 Poslovne težave	Tveganja, ki izhajajo iz sprememb poslovnega okolja organizacije.	Zatajitev dobaviteljev, tržne in ekonomske razmere.
4.4 Odvisnost od storitev	Tveganja, ki izhajajo iz odvisnosti organizacije od zunanjih izvajalcev.	Dobavitelji energetskih in infrastrukturnih storitev, nujne storitve, gorivo in transport.

Vir: J. J. Cebula & L. R. Young, A Taxonomy of Operational Cyber Security Risks, 2010, str. 3, tabela 1.

Na podlagi analize podatkov o incidentih iz naslova kibernetskih tveganj, v obdobju od leta 1971 do 2014, sta Eling in Wirfs (2015) ugotovila, da so kibernetska tveganja iz aktuarskega vidika zelo različna od ostalih operativnih tveganj. Pri analizi podatkov sta razdelila škode v dve skupini, in sicer škode iz naslova kibernetskih tveganj in škode iz naslova ostalih operativnih tveganj. Vsi opisni statistični podatki (število dogodkov, povprečna vrednost, maksimalna vrednost) za kibernetska tveganja so značilno nižji kot pri ostalih operativnih tveganjih. Maksimalna škoda je pri kibernetskih tveganjih skoraj šestkrat nižja kot pri drugih operativnih tveganjih.

Rezultati raziskave so pokazali, da so glavni vir kibernetskih tveganj dejanja ljudi, medtem ko so ostali viri kibernetskih tveganj, kot na primer zunanji dogodki, zelo redki. V kategoriji »dejanja ljudi« so vključeni napadi hekerjev, fizične kraje informacij, človeške napake in vsi incidenti, kjer zaposleni namerno ali nenamerno prirejajo podatke. Rezultati so pomembni za vsakega predstavnika podjetja s področja managementa tveganj za boljše razumevanje kibernetskih tveganj in njihovih posledic. Za dejavnost finančnih institucij so še posebej pomembni, ker nadzorniki bank in zavarovalnic zahtevajo oblikovanje tveganega kapitala za operativna tveganja, ki so lahko posledica kibernetskih tveganj (Eling & Wirfs, 2015).

2.1.3 Posledice kibernetskih tveganj

Z večanjem kibernetskih tveganj se finančne posledice zaradi kibernetskih škod povečujejo še hitreje. V medijih največkrat zasledimo, da so podjetja plačala globe regulatorjev zaradi kršitve zaupnosti podatkov njihovih strank. Vendar so potencialne finančne posledice lahko mnogo večje od prisojenih glob (Hillyer, 2014, str. 31), kot je razvidno iz študije o nastalih stroških ob kršitvi zaupnosti podatkov Ponemon (2015, str. 7).

Hillyer (2014, str. 31) razdeli škode iz naslova kibernetskih tveganj na zavarovaljive in nezavarovaljive. Med nezavarovaljive posledice kibernetskih tveganj lahko štejemo globe, oškodovanje ugleda, izgubo strank, odhod zaposlenih in padec vrednosti delnic. Med posledice kibernetskih tveganj, ki jih je možno zavarovati in so opredeljene v 3. poglavju, lahko uvrstimo stroške kriznega managementa, forenzikov, preiskave, obveščanja kupcev in obratovalnega zastoja.

Vpliv posledic oškodovanja oziroma padca ugleda je običajno težko izmeriti. V okviru nekaterih kibernetskih zavarovanj je zagotovljeno kritje za omejitev padca ugleda podjetja, vendar morajo podjetja vseeno spremljati in ocenjevati vpliv na njihovo znamko in ugled. Izguba strank je verjetna posledica znatne kibernetske škode. Razlog je lahko v prekinitvi pogodbe zaradi kršitve pogodbenih določil ali v negativni medijski pozornosti, nastali ob incidentu. Dolgotrajne posledice škode lahko bistveno vplivajo tudi na pridobivanje novih strank. Negativno medijsko poročanje lahko vpliva tudi na zaznavanje omejene možnosti napredovanja ali celo ohranitve delovnega mesta pri zaposlenih kot tudi na padec vrednosti delnice. Vendar nekateri raziskovalci ugotavljajo, da je težko dokazati dolgoročni vpliv na vrednost podjetja zaradi kibernetskega incidenta. Kljub temu lahko sklepamo, da večji padec lojalnosti strank ali visoke globe regulatorjev negativno vplivajo na vrednost delnice podjetja (Hillyer, 2014, str. 32).

Potencialno škodo, ki izvira iz kibernetskih tveganj, lahko razvrstimo tudi na drugačen način, kot je prikazano v Tabeli 4.

Tabela 4: Kategorije izgub iz naslova kibernetskih napadov in nezlonamerne odpovedi delovanja IT

	Kategorija izgube	**Opis**
A	Kraja intelektualne lastnine	Izguba vrednosti sredstev intelektualne lastnine, izražena v izgubi prihodkov zaradi zmanjšanega tržnega deleža.
B	Obratovalni zastoj	Izgubljeni dobiček oz. dodatni stroški, nastali zaradi nedostopnosti IT-sistema ali podatkov kot posledica kibernetskega napada.
C	Izguba podatkov in programske opreme	Strošek ponovne vzpostavitve podatkov ali programske opreme, ki je bila izbrisana ali poškodovana.
D	Kibernetsko izsiljevanje	Strošek izvedencev, ki obravnavajo kibernetsko izsiljevanje, v kombinaciji z zneskom plačila odkupnine

se nadaljuje

Tabela 4: Kategorije izgub iz naslova kibernetskih napadov in ne-zlonamerne odpovedi delovanja IT (nad.)

	Kategorija izgube	**Opis**
E	Kibernetski kriminal/prevara	Neposredna finančna škoda, ki jo je utrpela organizacija izvirajoč iz uporabe računalnikov za storitev prevare ali kraje denarja, vrednostnih papirjev ali drugega premoženja.
F	Kršitev zasebnosti/zaupnosti podatkov	Stroški preiskave in odziva na kršitev zasebnosti, vključno z IT-forenziki in obveščanjem oškodovanih lastnikov podatkov. Zahtevki tretjih oseb iz naslova odgovornosti, ki izvirajo iz istega dogodka. Kazni s strani regulatorjev in interesnih združenj.
G	Odgovornost iz naslova napake v delovanju omrežja	Odgovornost do tretjih oseb iz naslova določenih varnostnih dogodkov, ki se zgodijo znotraj IT-omrežja organizacije ali potekajo preko omrežja z namenom napada na tretjo osebo.
H	Vpliv na ugled	Izguba prihodkov zaradi povečanega upada strank ali zmanjšanega obsega poslovanja, ki ga lahko neposredno pripišemo objavi dogodka kršitve varnosti.
I	Fizična poškodba sredstev	Lastna škoda zaradi uničenja fizičnega premoženja, ki izvira iz kibernetskega napada.
J	Smrt in telesna poškodba	Odgovornost do tretjih oseb za smrt in telesne poškodbe zaradi kibernetskega napada.
K	Preiskava incidenta in stroški odziva	Neposredni stroški, nastali ob preiskavi in zaključku incidenta ter zniževanje izgube po incidentu. Nanaša se na vse ostale kategorije/dogodke.

Vir: Marsh, UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk. 2015, str. 11, tabela 3.

Za velika podjetja predstavlja kraja intelektualne lastnine tveganje, ki ima lahko največje posledice. Zaradi zapletenega vrednotenja sredstev intelektualne lastnine ali občutljivih poslovnih podatkov in načina uporabe ukradenih informacij s strani hekerjev je ocena ekonomske škode, povzročene zaradi izgube intelektualne lastnine, sicer zahtevna. Poleg tega v primerjavi z drugimi kategorijami izgub za tovrstne dogodke ni na voljo veliko razpoložljivih informacij, saj je incidente težje zaznati oziroma jih podjetja zaradi zaupnosti ne želijo deliti z drugimi. Drugi dve ključni kategoriji izgub sta kršitev zaupnosti podatkov in obratovalni zastoj zaradi nedelovanja omrežja (Marsh, 2015, str. 12).

Siegel, Sagalow in Serritella (2002, str. 36) kategorizirajo finančne posledice kibernetskih incidentov v tri splošna področja tveganj:

- tveganje lastne finančne škode oz. lastna varnostna tveganja: neposredna finančna škoda, ki ne izvira s strani odškodninskega zahtevka tretje osebe,
- tveganje s strani tretje osebe: odškodninska odgovornost do drugih,
- tveganje ugleda: težje merljive izgube, ki izvirajo iz izgube ugleda in identitete blagovne znamke.

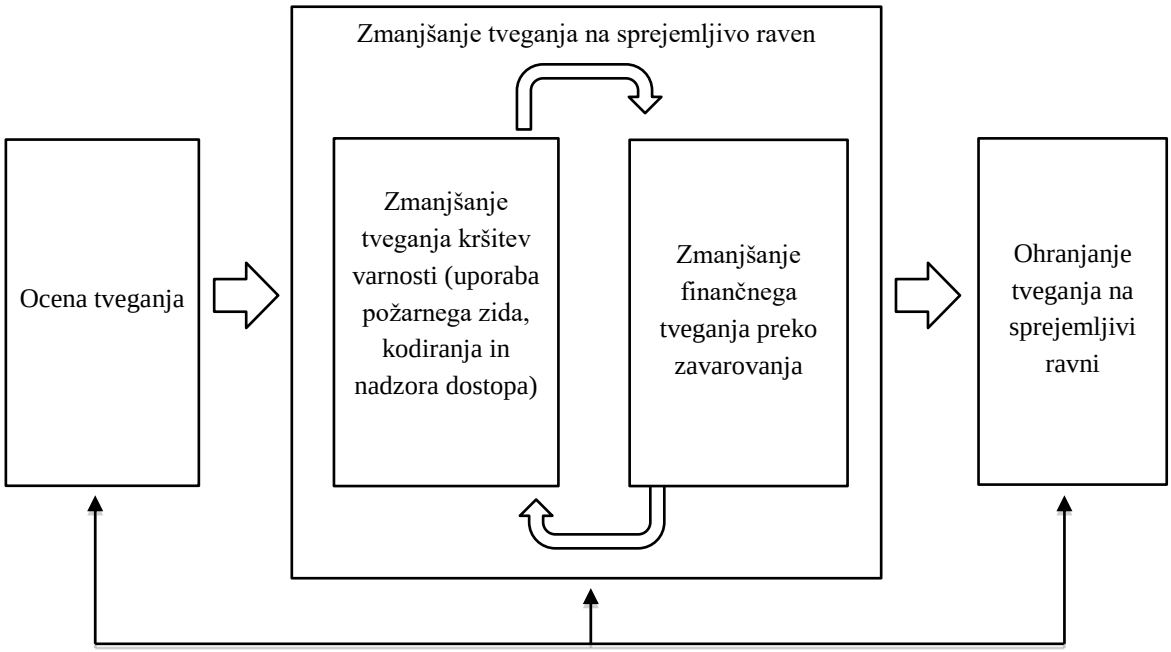
Lastna varnostna tveganja vključujejo finančno škodo, nastalo zaradi škode, uničenja ali poškodovanja informacijskih sredstev podjetja (t. j. podatkov). Informacijska sredstva so lahko v obliki seznama strank ali zaupnih informacij, poslovne strategije, informacij o konkurentih, sestavinah proizvodov ali drugih ključnih poslovnih skrivnostih. Njihova ustrezna zaščita in ovrednotenje je ključ uspešnih podjetij. Druga vrsta lastne škode je tveganje izgube prihodkov, posledica uspešnega kibernetskega napada z uporabo metode porazdeljene ohromitve storitve (angl. *DDoS* oz. *distributed denial-of-service*).

Varnostna tveganja s strani tretjih oseb se lahko manifestirajo v številnih vrstah zahtevkov iz naslova splošne pravne odgovornosti vloženih proti podjetju, poslovodstvu ali zaposlenim. Primeri tovrstnih tveganj izvirajo iz prisotnosti podjetja na spletu, zagotavljanja poklicnih storitev, prenosa zlonamerne kode ali povzročitve napada s porazdeljeno ohromitvijo storitve. Morda najtežje in še najpomembnejše tveganje za razumevanje je neopredmeteno tveganje oškodovanja ugleda.

2.2 Model managementa kibernetskih tveganj

Z vidika managementa kibernetskih tveganj je prva možnost izogibanje izpostavljenosti kibernetskim tveganjem z neodvisnostjo od računalnikov, mrežnih postaj in kakršne koli internetne povezave. Za nekatere organizacije je to izvedljivo, vendar za večino podjetij to ni ekonomsko uresničljivo. Naslednja možnost je prevzem tveganja, ob zavestni odločitvi o interni izravnavi katere koli škode oziroma ob finančni nezmožnosti uporabe drugih metod managementa tveganj. Tretja možnost je zmanjševanje tveganj z uporabo managerskih in tehničnih postopkov, kar vključuje investiranje v zaposlene in naprave za identifikacijo nevarnosti in pripravo protiukrepov s stalno izboljšavo varnostnih postopkov. Četrta možnost je prenos tveganja na tretjo osebo, zavarovalnico, za nadomestilo. Običajno podjetja sočasno uporabljajo kombinacijo vseh naštetih možnosti managementa tveganj. Prevzamejo del tveganja, zmanjšajo del tveganja in zavarujejo preostanek tveganja (Majuca, Yurcik & Kesan, 2006, str. 2–3).

Slika 3: Model managementa kibernetskih tveganj



Vir: A. L. Gordon et al., A Framework for Using Insurance for Cyber-Risk Management 2003, str. 84.

Kot razvidno iz Slike 3, Gordon, Loeb in Sohail (2003) opredelijo management kibernetskih tveganj kot proces ocenjevanja tveganja, ukrepov za zmanjševanje tveganja na sprejemljivo raven in ohranjanje ravni tveganja. Tako morajo podjetja najprej začeti z oceno nevarnosti in ranljivosti v povezavi z njihovim informacijskim sistemom. V tej fazi je pomembno upoštevati tudi vrednost informacij, ki so izpostavljene nevarnostim. Pri tem je lahko v pomoč matrika vrednosti-izpostavljenosti, s katero podjetja lahko prepoznajo, katerim informacijam morajo nameniti sredstva za varovanje. Z matriko se informacije razvrsti z vidika izpostavljenosti in vrednosti, od visoke do nizke, kot je prikazano v Tabeli 5. Z namenom učinkovite uporabe omejenih sredstev za informacijsko varnost se največ finančnih sredstev nameni informacijam, razvrščenim v poljih od 1, 2, 4 in 5.

Tabela 5: Matrika vrednosti-izpostavljenosti

	Izpostavljenost			
Vrednost		Visoka	Srednja	Nizka
	Visoka	1	2	3
	Srednja	4	5	6
	Nizka	7	8	9

Vir: A. L. Gordon et al., A Framework for Using Insurance for Cyber-Risk Management, 2013, str. 83, slika 1.

V naslednjem koraku podjetja znižajo tveganje informacijske varnosti na sprejemljivo raven, najprej z investiranjem v zaščito pred nastankom kršitve varnosti in nato s

sklenitvijo kibernetskega zavarovanja. Pri razporeditvi sredstev za znižanje celotne izpostavljenosti tveganju na sprejemljivo raven je potreben kompromis med sredstvi, ki jih podjetje nameni za znižanje verjetnosti kršitve varnosti in sredstvi za znižanje finančnega tveganja preko kibernetskega zavarovanja z vidika stroškov in koristi. To vpliva na raven preostalega tveganja, ki se smatra kot sprejemljiva raven. Ko je sprejemljiva raven preostalega tveganja določena, jo je potrebno vzdrževati.

2.3 Načini managementa kibernetskih tveganj

Učinkovit način managementa kibernetskih tveganj se začne s strategijo in osnovami, ki temeljijo na tveganjih. Na podlagi raziskave PwC (2015b), ki je zajela več kot 10.000 predstavnikov podjetij iz 127 držav, je velika večina podjetij (91 %) sprejela okvir kibernetske varnosti. Največkrat implementirane smernice so ISO 27001 in NIST (angl. *National Institute of Standards and Technology*). Smernice omogočajo podjetjem identifikacijo in postavljanje prioritet, meritev zastarelosti praks kibernetske varnosti in izboljšanje notranje in zunanje komunikacije.

Z namenom doseganja ustrezne ravni zaščite pred nevarnostmi in zagotavljanja vseh potrebnih mehanizmov za zaščito sredstev in znanja v podjetju je bilo v preteklosti razvitih veliko različnih pristopov in metod managementa kibernetske varnosti. Na osnovi ovrednotenja obstoječih metodologij managementa tveganja informacijske varnosti sta Fenz in Heurix (2014) ugotovila, da obstajajo med njimi majhne razlike. Vsaka metodologija zahteva predhodni popis in varnostno razvrstitev relevantnih elementov infrastrukture in identifikacijo misije in ciljev podjetja. Na splošno naslednje stopnje v postopku managementa tveganj vedno zahtevajo identifikacijo nevarnosti in pripadajoče ranljivosti za ugotavljanje verjetnosti, ki so potrebni, za ugotavljanje dejanskega tveganja.

Avtorja sta na tej osnovi ustvarila generično metodologijo managementa tveganj informacijske varnosti, ki predvideva sledeče stopnje:

- **Opis omrežja**. Definicija omejitev omrežja in sredstev, ki jih omrežje uporablja, zahteva sistematični popis opredmetenih (npr. oseb ali materialnih sredstev) in neopredmetenih (npr. podatki ali programska oprema) sredstev in določitev sprejemljive ravni tveganja za vsako popisano sredstvo.
- **Ocena nevarnosti in ranljivosti**. Ta stopnja zahteva določitev potencialnih nevarnosti, pripadajoče izvore nevarnosti in ranljivosti. Predvideno je preverjanje varnostnih zahtev, ki se lahko uporabijo za oceno skladnosti obstoječega in načrtovanega nadzora v naslednji stopnji.
- **Opredelitev tveganj**. Med drugim se oceni verjetnost, da nevarnost izkoristi določeno ranljivost v omrežju. Sledi analiza vpliva na zmožnost izvajanja misije podjetja, v kolikor nevarnost uspešno izkoristi ranljivost. Z združevanjem verjetnosti nevarnosti z obsegom posledic podjetje določi stopnjo tveganja in posledično načrtuje potrebne ukrepe.

- **Identifikacija nadzora**. Ta stopnja ob upoštevanju že uvedenega nadzora natančno razloži dodatno izvedbo nadzora, ki lahko ublaži ali zmanjša tveganje na sprejemljivo raven.
- **Ovrednotenje nadzora in implementacija.** Ta stopnja ovrednoti identificirane izvedbe nadzora ali kombinacije le-teh z vidika razmerja med stroški in koristmi. Tiste različice izvedbe nadzora, ki so ustrezne za ublažitev tveganja na sprejemljivo raven ob najnižjih možnih stroških, se vključi v načrt implementacije nadzora.

2.3.1 Umestitev v organizacijsko strukturo

Na splošno pogled višjega poslovodstva podjetij na potrebo po obsegu in pomembnosti managementa tveganj ter možnost administrativne učinkovitosti določa umestitev funkcije managementa tveganj v organizacijsko strukturo in natančne dolžnosti organizacijskih enot, zadolženih za management tveganj. Večina večjih podjetij ima posebne oddelke, zadolžene za management čistih tveganj, ki so vodeni s strani vodje za management tveganj (angl. *risk manager* oz. *chief risk officer*). Glede na to, da škode lahko nastanejo iz različnih razlogov, se celovit proces managementa tveganj vseeno idealno odraža v koordiniranih aktivnostih ključnih oddelkov in poslovnih enot v podjetju, vključno s proizvodnjo, trženjem, financami in kadrovsko funkcijo (Harrington in Niehaus, 2003, str. 12).

Podjetja danes v pretežni meri že delujejo v kibernetskem prostoru, kjer se znanje, ugled in mnenje potrošnikov lahko deli z drugimi ali izgubi v trenutku. Canham (2014, str. 46) na osnovi raziskave informacijske varnosti navaja, da podjetja še zdaleč niso dosegla učinkovite ravni managementa kibernetskih tveganj. Respondenti v raziskavi so bili nejasni, kdo v upravi podjetja je odgovoren za kibernetska tveganja. Raziskava je razkrila tudi slabo spremljanje programov izobraževanja in zavedanja o kibernetskih tveganjih.

Večina managerjev v podjetjih se zaveda naraščajočega kibernetskega tveganja, kar je razvidno iz rezultatov raziskave Advisen (2015, str. 4). Po največjih kršitvah zaupnosti podatkov, ki so se zgodile v letu 2014, so v raziskavi inštituta Ponemon (2015b) pri preverjanju zaskrbljenosti managementa podjetij glede izpostavljenosti pred kibernetskimi napadi ugotovili, da se je raven zavedanja managementa znatno zvišala.

Kljub temu se strategije managementa kibernetskih tveganj ne izvajajo v smislu ustrezne umestitve zmogljivosti kibernetske varnosti v podjetjih. Bailey, Kaplan in Rezek (2014) navajajo več razlogov za počasnejšo uveljavitev potrebnih strategij managementa kibernetskih tveganj. Najprej velja izpostaviti pritisk imperativa konkurenčnosti. Poslovodstvo je pod pritiskom ohranitve konkurenčnega položaja na trgu primorano sprejemati kompromise med tveganjem in uvajanjem inovativnih poslovnih rešitev. Posledice kibernetske varnosti zadevajo vse poslovne funkcije v podjetju. In samo to dejstvo ovira sprejem in implementacijo strategije managementa in omejevanja kibernetskih tveganj. Kot primer lahko navedemo odločitve o razvoju proizvoda ali

storitve, ki pogosto povečujejo količino zbranih občutljivih informacij o strankah. Naslednji razlog je otežena kvantifikacija kibernetskega tveganja. Izostanek merila za vrednotenje izpostavljenosti pred kibernetskimi tveganji otežuje komunikacijo o nujnosti vključitve najvišjega poslovodstva v sprejemanje potrebnih odločitev. In najtežje je spremeniti navade uporabnikov. Za veliko podjetij največjo ranljivost ne predstavlja delovanje znotraj podjetja, temveč neprevidne aktivnosti ali odločitve njihovih strank.

Kibernetska varnost je vprašanje sprejemanja odločitev na nivoju najvišjega poslovodstva v podjetju. Na osnovi raziskave avtorjev Bailey et al. (2014) na temo kibernetske varnosti, ki so jo opravili z managementom več kot 200 največjih podjetij na svetu, je vključitev in časovna razpoložljivost najvišjega poslovodstvo prepoznana kot najpomembnejši dejavnik pri stopnji naprednosti managementa kibernetskih tveganj. Bolj pomemben kot velikost, dejavnost in razpoložljiva sredstva podjetja. Pri podjetjih, ki so najuspešnejša pri razvoju kibernetske odpornosti, so v raziskavi zaznali sledeče aktivnosti višjega poslovodstva:

- aktivno vključevanje pri sprejemanju strateških odločitev,
- vključevanje vseh poslovnih funkcij v obravnavo posledic kibernetske varnosti,
- spodbujanje spremembe uporabniških navad z lastnim zgledom,
- zagotovitev učinkovitega upravljanja in poročanja o izvajanju programa kibernetske varnosti.

Ključno v procesu managementa kibernetskih tveganj je torej postavitev odgovornosti za kibernetsko varnost na raven upravnega odbora podjetja. Vendar to ne pomeni, da člani poslovodstva potrebujejo poglobljeno tehnično znanje, temveč da kibernetska tveganja z vidika pomembnosti obravnavajo na enak način kot finančna in poslovna tveganja (IRM, 2014, str. 234).

V ZDA je združenje direktorjev podjetij (angl. *National Association of Corporate Directors*) za svoje člane izdalo priporočilo za ustrezno umestitev kibernetskih tveganj v strategijo managementa tveganj, ki vključuje sledeče (Chertoff & Pflaging, 2015):

- obravnava kibernetskega tveganja kot tveganja na ravni podjetja,
- razumevanje pravnih posledic kibernetskih tveganj,
- razprava o kibernetskih tveganjih na sejah poslovodnega odbora, pri čemer se kibernetskemu tveganju nameni enako pozornost kot ostalim tveganjem,
- zahteva, da ima management merljiv načrt kibernetske varnosti,
- na nivoju uprave podjetja pripravljen razvoj načrta managementa kibernetskega tveganja, vključno z usmeritvijo, katerim tveganjem se izogiba, se jih sprejme, zmanjša ali prenese na zavarovalnice.

2.4 Management kibernetskih tveganj v praksi

Kibernetski napadi se stopnjujejo v pogostosti, resnosti in vplivu. Metode preprečevanja in odkrivanja so se večinoma izkazale za neučinkovite proti vedno spretnejšim napadom. Veliko podjetij ne ve, kaj narediti, ali pa nimajo sredstev za borbo proti visoko usposobljenim in agresivnim kibernetskim kriminalcem. Tehnološke spremembe zahtevajo pogoste spremembe poslovnega modela (DaSilva et al., 2013), zato otežujejo dolgoročno ustvarjanje tržnega položaja in dodane vrednosti podjetij. Nekateri od pomembnejših poslovnih trendov, kot so podatkovna analitika, digitalizacija poslovnih funkcij in medpanožno mešanje ponudbe storitev, so razširili uporabo tehnologij in podatkov, kar ustvarja več tveganja kot kadar koli (PwC, 2015b).

Na osnovi raziskave Eurostat (2015) o varnosti IKT v podjetjih, v katero je bilo vključenih 148.800 evropskih podjetij z več kot 10 in več zaposlenimi, je razvidno, da ima 32 % podjetij formalno definirano politiko varnosti IKT. Obstoj politike varnosti IKT pomeni, da se v podjetju zavedajo pomembnosti svojega IKT-sistema in bistvenih potencialnih tveganj. Hkrati se s tem nakazuje obstoj strategije podjetja za zaščito podatkov in IKT-sistemov kot tudi obvezna dolžnost za vse zaposlene.

V okviru formalno definirane politike varnosti IKT podjetja naslavljajo tri vrste tveganj, ki ustrezajo definiciji varnosti IKT, t. j. celovitost, zaupnost in razpoložljivost podatkov in sistemov. V politiki varnosti IKT podjetij je največkrat zapisano tveganje uničenja ali zlorabe podatkov zaradi napada ali drugega nepričakovanega incidenta (Eurostat, 2015).

Ocenjujejo, da bi približno 80 % kibernetskih napadov lahko preprečili ali zmanjšali njihov vpliv z osnovnim managementom tveganj (Allianz, 2015). Giblin (2015) navaja preventivne ukrepe, ki zmanjšujejo verjetnost odškodninskih tožb:

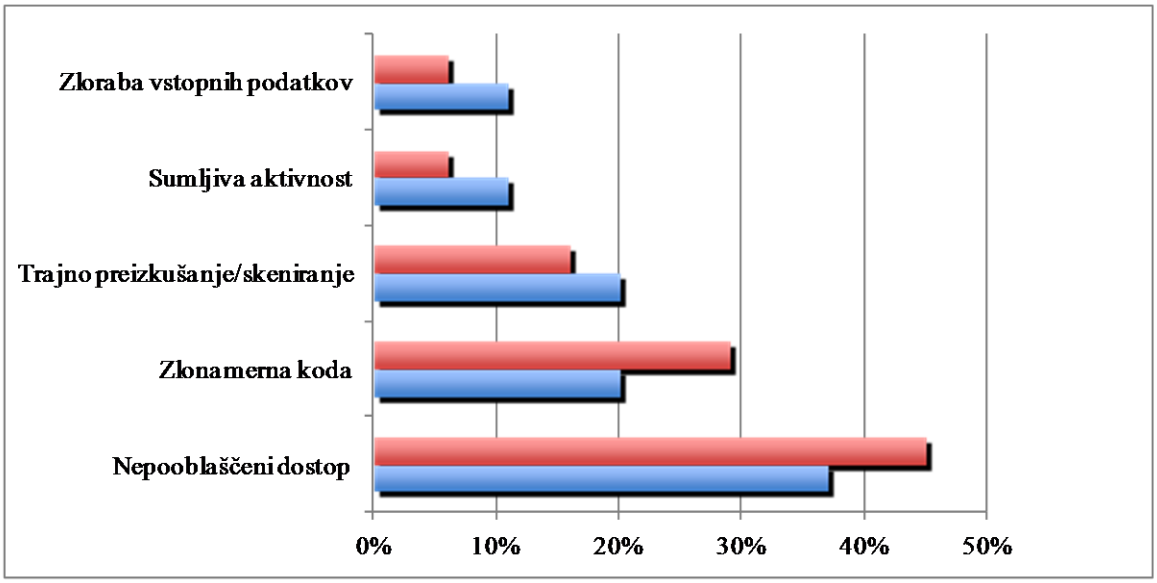
- oblikovanje in posodabljanje varnostne politike,
- izobraževanje zaposlenih o varnostni politiki in kibernetskih tveganjih,
- oblikovanje celovitega odzivnega načrta ob incidentu,
- izvedba poskusnega vdora v sistem,
- šifriranje mobilnih naprav,
- izvedba vaje s simulacijo kibernetskega napada ali kršitve.

2.4.1 Kategorije in viri kibernetskih incidentov

Na osnovi medijskega poročanja o kibernetskih incidentih lahko razumno sklepamo, da so za večino kibernetskih incidentov odgovorni zlonamerni hekerji, z željo po doseganju političnih, verskih ali drugih ciljev oziroma protipravne materialne koristi. Vendar na osnovi raziskave kibernetske varnosti, ki jo je IBM objavil v letu 2016, lahko ugotovimo, da je bilo v letu 2015 največ, 60 % vseh kibernetskih napadov izvršenih s strani zaposlenih, bodisi zlonamernih (44,5 %) bodisi nepazljivih (15,5 %) zaposlenih v podjetju.

Z drugimi besedami, napadi so bili izvršeni največkrat s strani tistih, ki se jim najbolj zaupa. V primerjavi s podatki iz leta 2014 je zaznan zmanjšan delež zunanjih kibernetskih napadalcev, ki se je v letu 2015 spustil s 45 % na 40 %.

Slika 4: Kategorije kibernetskih incidentov



Vir: IBM, IBM 2016 Cyber Security Intelligence Index, 2016.

V okviru poročila Cyber Security Intelligence Index (IBM, 2016) so navedene tudi kategorije kibernetskih incidentov med petimi največkrat kibernetsko napadenimi dejavnostmi. Iz Slike 4 je razvidno, da je najpogostejša kategorija kibernetskega incidenta nepooblaščeni dostop do uporabe informacijskih sistemov oz. podatkov, ki predstavlja skoraj polovico vseh obravnavanih dogodkov.

Kibernetski kriminal ustvarja visoke donose ob majhnem tveganju in relativno nizkih stroških za hekerje. Najpogosteje uporabljeni tehniki izkoriščanja, ki sta presenetljivo poceni, sta socialni inženiring (angl. *social engineering*), kjer kibernetski kriminal prevara uporabnika z namenom omogočanja dostopa, in izkoriščanje ranljivosti (angl. *vulnerability exploitation*), kjer kibernetski kriminal izkorišča napake v programiranju ali pri implementaciji vstopnih dovoljenj. Nasprotno velja za branilce, podjetja ali posameznike. Odziv na kibernetski kriminal je poslovna odločitev. Glede na to, kako lahko upravljajo s potencialno škodo iz naslova kibernetskega kriminala, podjetja in posamezniki sprejemajo odločitve o obsegu tveganja, ki so ga pripravljeni sprejeti, in o višini sredstev za zmanjšanje tveganja. Težava je v tem, da v kolikor se podjetje ne zaveda možne višine škode ali podcenjuje svojo ranljivost, bodo tveganja podcenjena (McAfee, 2014).

Opredelitev zlonamernih nevarnostnih virov, motiv in namen posameznikov ter njihova zmožnost in sredstva, ki jih uporabljajo pri kibernetskem kriminalu, je predstavljena v Tabeli 6.

Tabela 6: Viri zlonamernih nevarnosti

Nevarnostni vir	**Motiv in namen**	**Zmožnost in sredstva**
Hekerski malčki (angl. *script kiddie*)	Doseči status znotraj skupine in dokazati sposobnost povzročitve škode. Redko so vztrajni, če se soočijo s težavami in začetnim neuspehom.	Relativno neusposobljeni, nezmožni izvedbe zahtevnih napadov. Napade običajno izvedejo z uporabo orodij, ki so jih razvili drugi. Imajo omejen dostop do tehničnih in denarnih sredstev.
Kibernetski teroristi (angl. *cyber-terrorist*)	Povzročajo motnje v družbi z izvajanjem kibernetskih napadov, najraje usmerjenih na ključno infrastrukturo. Močni politični, ideološki ali verski motivi in pripravljenost na ekstremna dejanja.	Lahko posedujejo znatna sredstva in veščine ter so v nekaterih primerih podprti s strani držav. Zmožnost dolgoročnega načrtovanja, priprav in izvedbe napadov.
Vdiralci (angl. *Black hat hacker*)	Motivirani za pridobitev osebne koristi, npr. z nedovoljenim poseganjem v podatke ali izsiljevanjem.	Raven usposobljenosti vdiralcev se lahko zelo razlikuje, vendar so najboljši vodilni strokovnjaki na svetu za kibernetsko varnost. Če so del večje kriminalne združbe, lahko upravljajo tudi z znatnimi sredstvi.
Hektivisti (angl. *hacktivist*)	Podobno kot kibernetski teroristi so motivirani s političnim, ideološkim ali verskim programom in uporabljajo kibernetske napade za dosego svojih ciljev. Čeprav je razmejitev med kibernetskimi teroristi in hektivisti zabrisana, predpostavljamo, da so hektivisti manj podvrženi ekstremnim dejanjem. Njihov cilj je bolj škodovanje izbranim skupinam, politikom ali drugim posameznikom kot pa družbi na splošno.	Raven usposobljenosti se lahko zelo razlikuje. Večina hektivistov deluje samostojno ali v majhnih ali slabo organiziranih skupinah. Toda, v kolikor so dobro organizirani imajo lahko dostop do znatnih računalniških sredstev.
Notranja oseba (angl. *insider*)	Nelojalni zaposlen ali svetovalec v podjetju, ki je običajno motiviran bodisi za pridobitev osebne koristi bodisi z željo, da bi škodoval delodajalcu zaradi konflikta in nezadovoljstva.	Ima omogočen dostop do vseh sistemov in poseduje podrobne informacije in znanje o arhitekturi, funkcionalnosti in varnostnih lastnostih sistema.
Škodljiva programska oprema (angl. *malware*)	Razvita z namenom poškodovanja računalniških sistemov.	Razvijalci zlonamerne programske opreme so največkrat zelo usposobljeni. Zato lahko povzročijo znatno škodo na sistemih, ki temeljijo na standardnih operacijskih sistemih ali drugi programski opremi.

Vir: A. Refsdal, B. Solhaug & K. Stølen, Cyber-Risk Management, 2015 str. 67, tabela 7.2.

2.4.2 Izpostavljenost po dejavnostih in največji primeri kibernetskih incidentov

Podjetja iz najširšega nabora dejavnosti so izpostavljena potencialno enormnim fizičnim škodam kot tudi odgovornostim in stroškom, ki so posledica kibernetskih napadov in kršitve zaupnosti podatkov.

Na podlagi raziskave kršitve zaupnosti podatkov (Verizon, 2015, str. 3) lahko ugotovimo, da so glede na število varnostnih incidentov najbolj izpostavljene dejavnosti javnih inštitucij, informacijskih podjetij, finančnih inštitucij in trgovcev. Medtem ko je po številu potrjenih primerov izgube podatkov, poleg prej omenjenih dejavnosti, potrebno izpostaviti še dejavnost hotelirjev, izvajalcev zdravstvenih in drugih poklicnih storitev.

Zanesljive podatke o posamičnih škodnih dogodkih v podjetjih, ki so bila predmet kibernetskega napada, je težko pridobiti. Podjetja največkrat skrbi škoda iz naslova izgube ugleda, v kolikor bi javno objavili podatke o škodi iz naslova kibernetskega napada. Kot je razvidno iz najnovejših raziskav s področja kibernetskih tveganj, škode iz naslova kibernetske varnosti in kibernetskega kriminala povečujejo pozornost podjetij.

Eling in Wirfs (2015) sta v raziskavi podatkov 994 incidentov iz naslova kibernetskih tveganj ugotovila, da so severnoameriška podjetja v obdobju od leta 1971 do 2014 doživela več kot dvakrat več incidentov (51,9 %) kot podjetja iz Evrope (23,2 %) in veliko več kot dvakrat več kot podjetja z vseh drugih kontinentov. Pri višini škode imajo podjetja iz Severne Amerike med najnižjimi povprečnimi škodami iz naslova kibernetskih tveganj, medtem ko imajo podjetja iz Evrope in Azije veliko višje povprečne škode. Avtorja navajata verjetnost večje zmožnosti in pripravljenosti severnoameriških podjetij za investicije v ukrepe za zmanjševanje tveganj pred večjimi škodami, kar izvira iz daljše tradicije prepoznavanja in managementa kibernetskih tveganj v primerjavi z Evropo in Azijo.

Največji delež, 78,6 % vseh kibernetskih incidentov, se je zgodil v finančni panogi, kar ni presenetljivo, glede na to, da banke in zavarovalnice hranijo precejšnjo količino občutljivih osebnih podatkov. Vendar je povprečna škoda iz naslova kibernetskih tveganj za podjetja iz nefinančnih dejavnosti približno dvakrat večja kot pri podjetjih, ki nudijo finančne storitve. Ta ugotovitev se lahko pojasni z večjim zavedanjem finančnih podjetij o občutljivosti podatkov in boljšo zaščito pred kibernetskimi tveganji (Eling & Wirfs, 2015, str. 6).

Dinamično naravo kibernetskih tveganj lahko razberemo iz najnovejše raziskave IBM (2016). Iz primerjave podatkov za leti 2015 in 2014 je namreč razvidno, da se je dejavnost zdravstvenih storitev v letu 2015 povzpela na prvo mesto med najbolj izpostavljenimi dejavnostmi pred kibernetskimi napadi in prehitela proizvodnjo in dejavnost izvajalcev finančnih storitev. Slednja je v letu 2014 veljala za dejavnost z največjim številom kibernetskih napadov.

V nadaljevanju so predstavljeni nekateri večji primeri kibernetskih napadov, ki so imeli za posledico kršitev zaupnosti podatkov (World's Biggest Data Breaches, 2016):

- **J.P. Morgan Chase & Co**. Poleti 2014 so hekerji napadli banko iz ZDA, J.P. Morgan Chase. Z uporabo škodljive programske opreme so prevzeli oddaljen nadzor nad omrežjem banke. Izkoristili so varnostne luknje, katerih se banka do takrat ni zavedala, znane kot 0-dan ranljivost (angl. *zero day vulnerability*). Napad je banka odkrila dva meseca kasneje. Pri tem je bilo odtujenih več kot 76 milijonov osebnih in 7 milijonov poslovnih podatkov. Podatki so vključevali imena, naslove, telefonske številke in naslove elektronske pošte, kot tudi notranje informacije o strankah.
- **Target Corporation**. V primeru hekerskega napada na trgovca iz ZDA, v letu 2013, naj bi bilo odtujenih približno 40 milijonov podatkov o kreditnih in plačilnih karticah in 70 milijonov enot osebnih podatkov. Skupni ocenjeni stroški napada znašajo 300 milijonov USD (Ferrillo, 2015, str. 38). Primer kršitve zaupnosti podatkov pri trgovcu Target iz ZDA je razkril, kako hude so lahko posledice v primeru nepripravljenosti poslovodstva podjetja za management večjega kibernetskega incidenta. Kljub temu da je bil kibernetski napad dobro izpeljan, preko zunanjega izvajalca ogrevalnih in prezračevalnih naprav z dostopom do vstopnih podatkov v sisteme trgovca, je bila ključna napaka poslovodstva, ki ni zagotovilo ustrezne zaščite podatkov in stabilnega odzivnega načrta, kjer bi bili tudi sami vključeni v potrebne aktivnosti v primeru varnostnega incidenta.
- **eBay**. Kibernetski napadalci so pridobili vstopne podatke nekaj zaposlenih in jih uporabili za dostop do baze podatkov, ki je vsebovala šifrirana gesla strank in druge nefinančne podatke. Podjetje je pozvalo vseh svojih 145 milijonov uporabnikov storitev, naj preventivno zamenjajo gesla, in zagotovilo, da niso opazili povečanih goljufivih aktivnosti (Economist, 2014).
- **Home Depot**. Zlonamerna programska oprema, ki so jo hekerji namestili na blagajne ameriškega trgovca z opremo in izdelki za dom, je izpostavila 56 milijonov podatkov o kreditnih karticah kupcev. Podjetje ni aktiviralo protivirusne zaščite, ki so jo kupili zaradi predhodnega napada na trgovca Target.
- **Anthem**. V drugi največji zdravstveni zavarovalnici v ZDA so februarja 2015 potrdili vdor hekerjev v njihove računalniške strežnike, ki so pri tem ukradli do 80 milijonov osebnih podatkov zavarovancev (imena, rojstni podatki, naslovi, elektronski naslovi, osebni dohodki). Zdravstveni in finančni podatki po zagotovilih zavarovalnice niso bili ogroženi.
- **Experian / Court Ventures**. Z okoli 200 milijoni podatkov, ki so bili izpostavljeni kršitvi zaupnosti se primer podjetja Court Ventures, kasneje prevzeto strani podjetja Experian iz ZDA, uvršča na prvo mesto po številu kompromitiranih podatkov do zdaj. Podjetje Court Ventures se je ukvarjalo z zbiranjem in prodajo osebnih informacij za vodenje postopkov na sodiščih. Podjetje je v letu 2012 prodalo del podatkovne zbirke podjetju iz Vietnama, ki je podatke preprodalo svojim uporabnikov. Ti podatki so bili kasneje uporabljeni v številnih primerih prevar.

2.4.3 Pregled stroškov v primeru kibernetskega incidenta

Trenutno večina podjetij ne želi javne objave informacij o kibernetskem napadu zaradi možnosti padca ugleda podjetja. Celo znotraj podjetij predstavniki IT-oddelkov lahko nadrejenim prikrivajo podrobnosti o kibernetskih kršitvah varnosti. To se bo spremenilo s trendom zahtev regulatorjev po razkritju kibernetskih kršitev, kot je to primer Komisije za vrednostne papirje in borzo v ZDA in nove EU Uredbe o varstvu podatkov (ENISA, 2012, str. 5–6).

V zadnjih letih so imela podjetja vseh dejavnosti po vsem svetu izpostavljene svoje podatke tveganju kibernetskega napada. Prej omenjeni največji primeri kršitev zaupnosti podatkov so poleg padca ugleda povzročili podjetjem milijonske škode. Kot posledica kršitve zaupnosti podatkov je trgovska družba Target iz ZDA pristala na zunajsodno poravnavo odškodninskega zahtevka iz naslova vložene skupinske tožbe njenih strank, v višini 10 milijonov USD. Po nekaterih ocenah (McAfee, 2014, str. 18) so skupni stroški posledic kibernetskega napada, ki zajemajo povračilo škode strank, stroške ponovne izdaje plačilnih kartic, odvetniških stroškov in nadzora porabe na bančnih računih strank, znašali do 420 milijonov USD. Na osnovi študije, katere rezultate je leta 2015 objavil inštitut Ponemon, je razvidno, da so se povprečni skupni stroški, nastali ob kršitvi zaupnosti podatkov pri 350 podjetjih, vključenih v raziskavo, zvišali s 3,52 milijona USD v letu 2014 na 3,79 milijona USD. Raziskava kaže tudi na zvišanje povprečnega stroška vsakega izgubljenega ali ukradenega zapisa občutljivih ali zaupnih informacij s 145 USD v letu 2014 na 154 USD v letu 2015.

Tabela 7: Povprečni strošek kršitve zaupnosti podatkov v letu 2015 po državah (v USD)

	Povprečni strošek kršitve zaupnosti podatkov (v milijonih)	**Povprečni strošek na ukradeni zapis**
ZDA	6,53	217
Nemčija	4,89	211
Francija	4,34	186
Velika Britanija	3,72	163
Italija	2,75	146

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

Ob vedno večjem tveganju varnosti podatkov je tudi verjetnost kršitve zaupnosti podatkov večja kot kadar koli prej. V raziskavi inštituta Ponemon (2015b) je omenjenih nekaj spremenljivk, kot so država, dejavnost, vključenost managementa v ukrepe varovanja, ki vplivajo na strošek kršitve zaupnosti podatkov. Kot razvidno iz Tabele 7 so stroški v ZDA višji kot v kateri koli drugi državi, vključeni v raziskavo. Strošek na ukradeno enoto je najvišji pri reguliranih dejavnostih, kot so zdravstvo in izobraževanje, in najnižji pri transportni dejavnosti in javnem sektorju. Največjo rast povprečnega stroška na ukraden

zapis so zabeležili v trgovini na drobno, kjer se je strošek povišal s 105 USD v 2014 na 165 USD v letu 2015.

Potrebno je upoštevati tudi povečanje celotnega stroška kršitve zaupnosti podatkov zaradi izgube strank. Podjetja v nekaterih državah, na primer v Franciji, Italiji, Veliki Britaniji in na Japonskem imajo večje težave pri ohranjanju lojalnosti strank po dogodku kršitve zaupnosti podatkov. Z vidika dejavnosti pa imajo večjo izpostavljenost pred izgubo obstoječih strank dejavnosti zdravstvenih storitev, farmacije in finančnih storitev. V primeru aktivne vloge managementa podjetja pri razvoju varnostnih ukrepov so stroški kršitve zaupnosti podatkov nižji. Kibernetsko zavarovanje, izobraževanje zaposlenih, skupine za odziv v primeru varnostnega incidenta in splošna uporaba šifriranja podatkov lahko znižajo strošek kršitve zaupnosti podatkov. Dodatno se znižajo stroški, v kolikor ima podjetje vzpostavljen sistem zagotavljanja neprekinjenega poslovanja (Ponemon, 2015b).

Z vidika vpliva na globalno gospodarstvo in kot pokazatelj resnosti problema je pomenljiv podatek o strošku kibernetskega kriminala v razmerju do BDP. Iz Tabele 8 je razvidno, da ocenjeni globalni stroški kibernetskega kriminala predstavljajo podobno breme za globalno ekonomijo kot druge uveljavljene oblike kaznivih dejavnosti.

Tabela 8: Strošek kaznivih dejavnosti v BDP

Dejavnost	**Strošek v % BDP**
Pomorsko piratstvo	0,02 (globalno)
Meddržavni kriminal	1,2 (globalno)
Ponarejanje/Nedovoljeno razmnoževanje	0,89 (globalno)
Tatvine	1,5 (ZDA)
Avtomobilske prometne nesreče	1,0 (ZDA)
Prodaja drog	0,9 (globalno)
Kibernetski kriminal	0,8 (globalno)

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

Možen pogled na strošek kibernetskega kriminala je z vidika predpostavke, da družba vzame v zakup breme stroškov kriminala in povzročeno škodo kot kompromis za udobnost in učinkovitost. Podjetja in posamezniki so vzeli v zakup, da pozitivni učinki uporabe avtomobilov in čezatlantskih tovornih ladij odtehtajo potencialne stroške. Težava s takšno analogijo je v tem, da se veliko podjetij ne zaveda velikosti škode iz naslova kibernetskega kriminala, kar posledično vodi v napačne odločitve o sprejemljivi škodi. Obenem je vprašanje, ali je neposredna, merljiva škoda pravšnje merilo. Obstajajo neopredmeteni stroški, kot je omajano zaupanje poslovnih partnerjev in kupcev (McAfee, 2014).

2.5 Prihodnost managementa kibernetskih tveganj

Podjetja delujejo znotraj vedno bolj povezanega in medsebojno odvisnega okolja, kjer niso v nevarnosti samo njihovi sistemi in podatki, temveč tudi sistemi in podatki dobaviteljev, kupcev in strateških partnerjev. Internet stvari je še povečal povezljivost in dodatno poglobil ranljivost. Zaskrbljujoča je tudi nevarnost napadov na infrastrukturo, od katere so odvisni (PwC, 2015a).

Zavedanje o kibernetskih tveganjih je največje v ZDA, kjer stroga zakonodaja s področja varstva podatkov podjetjem nalaga obvezno obveščanje posameznikov o kršitvi zaupnosti podatkov. V drugih državah je varstvo podatkov različno urejeno, vendar je povsod trend v smeri strožje zakonodaje, z namenom povečanja kibernetske varnosti. V EU je bil aprila 2016 sprejet zakonodajni sveženj, ki določa pravni okvir varstva osebnih podatkov in vzpostavlja obvezno poročanje o kršitvah varstva osebnih podatkov tako pristojno nadzorno institucijo kot tudi posameznika, lastnika informacije. Posledično lahko pričakujemo večje finančno breme za podjetja iz naslova prisojenih kazni s strani nadzornikov kot tudi tožbenih zahtevkov potrošnikov (Allianz, 2015).

Ob povečani selitvi poslovnih dejavnosti v spletno okolje in ob vedno večjem številu potrošnikov z dostopom do interneta ter povezljivosti avtonomnih naprav (Internet stvari) se povečujejo tudi priložnosti za kibernetski kriminal. Lahko pričakujemo tudi povečanje škod iz naslova kraje intelektualne lastnine zaradi povečane zmožnosti držav, uporabnic ukradene tehnologije in znanja, za proizvodnjo konkurenčnih izdelkov (McAfee, 2014, str. 18).

2.5.1 Vpliv razvoja tehnologije

Smo v zlati dobi inovacij, ki jo zaznamujejo tehnologije storitev v oblaku, mobilnosti, velikih podatkov (angl. *big data*), družbenih medijev, odprtokodne programske opreme, virtualizacije in Interneta stvari. Te spremembe omogočajo posameznikom, oblastem in podjetjem inovacije in ponovno odkritje načina vzajemnega delovanja. Toda z razširjeno uporabo sodobnih tehnologij so se pojavila nova tveganja, pri čemer so v ospredju kibernetska tveganja.

Preobrazba globalne ekonomije v smeri digitalizacije poslovanja zadeva vse industrijske in storitvene sektorje. Vendar obstoječe zakonodajne omejitve pri spletnem poslovanju ne omogočajo polne uporabe sodobnih tehnologij. Evropska komisija je v Strategiji za enotni digitalni trg zapisala sklop ukrepov za digitalizacijo industrije in povezanih storitev v vseh sektorjih, z namenom spodbuditi naložbe, ki bodo zagotavljale gospodarsko rast in konkurenčnost evropskega gospodarstva. Tako z izboljševanjem ocenjevanja in upravljanja kibernetskega tveganja kot z zagotavljanjem trdnejše informacijske infrastrukture gospodarstvu v EU na splošno, ki bo podpirala inovacije in rast, kar bo ustvarilo nove priložnosti za podjetja, da bodo postala produktivnejša. Predstavljen je predlog ukrepov za

oblikovanje skupnih standardov na prednostnih področjih, kot so komunikacijska omrežja 5G, kibernetska varnost in modernizacija javnih storitev (Evropska komisija, 2016).

Ob predpostavki, da je prihodnost v digitalizaciji, lahko pričakujemo še večji obseg zbranih podatkov, ki bodo analizirani in potencialno ogroženi. Podjetja bodo generirala in delila vedno več informacij o ljudeh in procesih, Internet stvari bo sprožil val informacij na relaciji naprava-naprava. Upravičeno lahko pričakujemo, da bodo prihodnji nevarnostni dejavniki uporabljali še bolj napredna orodja in taktike. Na ta način se ustvarja vedno več tveganj, ki se jim managerji poskušajo izogniti in izboljšati rezultate poslovanja. Najpogostejša skupna točka pri novih tehnologijah so storitve v oblaku, ki imajo osrednjo vlogo v med seboj povezanem digitalnem ekosistemu posameznikov, podjetij in oblasti (PwC, 2015b).

Naprave, ki sestavljajo **Internet stvari**, imajo običajno svoj IP-naslov, vgrajen računalniški sistem, napravo za zaznavanje okolice in večinoma brezžično omrežno povezljivost. Naprave Interneta stvari so lahko aparati za vsakdanjo uporabo, prevozna sredstva ali pa stroji v proizvodnji, ki jih upravlja programska oprema. Takšne naprave avtomatizirajo veliko običajnih aktivnosti in strojem omogočajo sprejemanje odločitev brez poseganja človeka. Avtonomne naprave bodo nadzirale stanje zalog, potrjevale poslovne transakcije preko interneta in urejale prevoz in dostavo brez posega človeka (Lewis, 2016, str. 2). Z vidika kibernetskih tveganj naprave Interneta stvari največkrat zaradi pomanjkljivih osnovnih varnostnih zaščit potencialno omogočajo nevarnostnim akterjem vstop v omrežja podjetij ter posledično zlorabo podatkov, prekinitev poslovanja in ogrožanje integritete proizvodov in storitev (PwC, 2015b).

Na eni strani **storitve v oblaku** zagotavljajo pomembne priložnosti pri poslovanju podjetij, vendar se ob pomanjkljivem nadzoru nad sredstvi, ki temeljijo na storitvah v oblaku, poraja dvom o varnosti in učinkovitosti (Roberts, 2014, str. 102).

Namesto vzpostavitve lastne IT-infrastrukture, ki vključuje strojno opremo ter razvoj in vzdrževanje programske opreme, lahko podjetja uporabljajo informacijske storitve v oblaku. Dostop do storitev v oblaku je možen le preko interneta. V letu 2014 je 19 % podjetij iz držav članic EU uporabljalo informacijske storitve v oblaku, večinoma za gostovanje sistemov za elektronsko pošto in elektronsko hrambo dokumentov. Od teh jih je 46 % uporabljalo napredne storitve v oblaku, ki so vezane na uporabniške programe za finance in računovodstvo. Štiri od desetih podjetij (39 %), ki so uporabljala storitve v oblaku omenjajo tveganje kršitve varnosti kot glavni omejujoči dejavnik pri uporabi storitev v oblaku. Podoben delež podjetij (42 %), ki ne uporabljajo storitev v oblaku navaja nezadostno poznavanje informacijskih storitev v oblaku kot ključni razlog za neuporabo. Največji delež uporabnikov storitev v oblaku je pričakovano v informacijsko-komunikacijski dejavnosti (45 %). Nadpovprečen delež uporabe (27 %) je še v dejavnosti poklicnih, znanstvenih in tehničnih storitev, medtem ko je pri večini drugih dejavnosti delež med 14 % in 20 % (Eurostat, 2014).

Uporaba **mobilnih naprav** zaposlenih za poslovne namene je čedalje bolj priljubljena pri zaposlenih in dovoljena s strani delodajalcev. Takšne naprave, ki niso preverjene s strani podjetja, imajo dostop do korporativnih informacij v lasti podjetja in pogosto povečujejo izpostavljenost podjetja tveganjem. Visok delež podjetij (75 %), ki imajo zapisano politiko uporabe privatnih naprav v službene namene, kaže na zavedanje podjetij o tveganjih, povezanih s takšno prakso. Večina podjetij ima poleg tega urejeno tudi uporabo službenih mobilnih naprav, tudi za čas izven delovnika. V raziskavi obstoja varnostne politike za uporabo mobilnih naprav se je izkazalo, da ima 83 % večjih evropskih podjetij sprejeta ustrezna interna navodila o uporabi službenih mobilnih naprav, medtem ko je delež pri manjših podjetjih 63 % (Advisen, 2015, str. 8).

2.5.2 Vpliv družbenih medijev

Družbeni mediji podjetjem zagotavljajo koristi, kot so povečana prepoznavnost znamke, možnost oglaševanja in neposredna komunikacija s ciljno publiko, na stroškovno učinkovit način. Podjetja so s svojo znamko lahko prisotna na oddaljenih trgih, kamor brez sodobne tehnologije ne bi imele enostavnega dostopa. Družbeni mediji omogočajo podjetjem tudi administracijo in organizacijo na bolj povezan in neposreden način in tako zagotavljajo pravočasen in učinkovit način delovanja. Na drugi strani pa so družbeni mediji neraziskano in stalno spreminjajoče se okolje, ki ga je včasih težko uporabljati varno in produktivno. Managerji tveganj in poslovodstvo podjetij morajo zagotoviti vzpostavitev ustreznih ukrepov za varovanje podatkov podjetja, varne povezave in zaščito pred vedno pogostejšimi zlonamernimi napadi preko družbenih omrežij (Chatzilia, 2014, str. 156).

Podjetja so izpostavljena predvsem tveganjem morebitne izgube ugleda, zagotavljanja zasebnosti, kršenja intelektualne lastnine drugih in kršitve zaupnosti podatkov. Iz raziskave o uporabi družbenih medijev v podjetjih je razvidno, da se ta zavedajo tovrstnih tveganj, saj ima 75 % podjetij sprejeto politiko uporabe družbenih medijev v povezavi s poslovanjem podjetja (Advisen, 2015, str. 8).

Družbeni mediji so povezani s posamezniki, vključenimi v podjetje, kot tudi z informacijami in tehnologijo, ki jih podjetja uporabljajo ob izvajanju poslovanja za doseganje poslovnih ciljev. Na osnovi tega lahko tveganja iz naslova družbenih medijev razvrstimo v tri kategorije (Chatzilia, 2014, str. 144):

- tveganja, povezana z ljudmi,
- tveganja, povezana s tehnologijo,
- tveganja, povezana z informacijami.

Tveganja, povezana z ljudmi, vključujejo napade, ki so povezani s socialnim inženiringom. Takšni napadi se zgodijo, ko so na družbenih medijih objavljene zaupne, občutljive ali drugače uporabne informacije in jih tretja oseba kasneje zlonamerno uporabi. Izrazito šibka točka z vidika tveganj v podjetju je kraja uporabniškega računa oz. identitete.

Zaposleni namreč pri potrjevanju identitete ob uporabi korporativnih IT-omrežij ali uporabniških programov uporabljajo podatke, ki jih pogosto objavljajo na zasebnih socialnih omrežjih. Za ugled podjetja je škodljivo neprimerno obnašanje in nepremišljeno objavljanje informacij in podatkov o podjetju, njegovih zaposlenih ali strankah. Zaradi množične in prekomerne uporabe družbenih omrežij poskušajo podjetja, predvsem z namenom ohranjanja produktivnosti in poklicnih standardov, na različne načine omejevati uporabo družbenih medijev s strani svojih zaposlenih.

Ob uporabi tehnološke opreme, ki ima dostop do spletnih strani družbenih medijev, se povečuje tveganje izpostavljenosti napadom virusov ali zlonamerne programske opreme. Eno največjih tveganj v povezavi z družbenimi mediji je dejstvo, da podjetja ne morejo nadzorovati vsebino objav na spletu. Nezmožnost ustreznega odziva ali celo umik vsebine lahko hitro škoduje ugledu in znamki podjetja. Zaradi vedno večje uporabe družbenih medijev pri poslovnih interakcijah so posledice napada zoper spletne strani družbenih omrežij resna težava pri zagotavljanju neprekinjenega poslovanja.

Verjetno so podjetja ob kibernetskem incidentu v okviru družbenih medijev najbolj izpostavljena tveganju izgube ugleda podjetja. Zaposleni, stranke, dobavitelji in prodajalci so lahko največji ambasadorji podjetja, hkrati pa lahko oslabijo njegovo blagovno znamko in javno podobo. Istočasno lahko uporabniki družbenih medijev objavijo obrekljive komentarje o izdelkih ali storitvah podjetij. Nadzor ali spremembo zapisov na spletnih portalih pa je zelo težko doseči. V kolikor so neprimerne vsebine objavljene v družbenih medijih, ki jih upravlja podjetje, obstaja pravno in regulatorno tveganje. Z vidika tveganj, ki so tudi povezana z informacijami je zaradi množice podatkov, ki jih podjetja prejemajo, ustvarjajo, urejajo, delijo in shranjujejo, kritično razkritje informacij. Na spletnih družbenih medijih se celo objavljajo zaupni dokumenti, interne komunikacije, poslovne skrivnosti in intelektualna lastnina. V takih primerih škode ni mogoče preprečiti zgolj z brisanjem objavljenih dokumentov. V kolikor konkurenčna prednost podjetja temelji na osnovi razkritih informacij je lahko celo ogrožena strategija podjetja in posledično finančni rezultat. Poleg tega razkritje informacij o kupcih lahko povzroči izgubo njihovega zaupanja ali celo prekinitev poslovnega sodelovanja (Chatzilia, 2014, str. 149).

3 KIBERNETSKO ZAVAROVANJE KOT ORODJE MANAGEMENTA TVEGANJ

Management kibernetskih tveganj običajno vključuje metode zmanjševanja tveganj in resnosti posledic. Te metode (požarni zid, zaznavanje vdorov, itd.) znižajo tveganja, vendar jih ne odpravijo, zato ostaja vprašanje, kako ravnati s preostankom tveganja. Eden od preostalih načinov je uporaba zavarovanja.

Postaja vedno bolj jasno, da prvi modeli kibernetske varnosti, ki so se osredotočali izključno na odpravo tveganj, niso zadostni v zapletenem svetu interneta. Ne obstaja čudežna rešitev za kibernetsko varnost. Vendar zavarovanje ne more prevzeti samostojne

vloge za znižanje tveganja. Prva obrambna linija mora biti vedno celovit varnostni program in implementacija varnostnih orodij in proizvodov. Samo preko vzvoda obeh pristopov podjetja lahko dosežejo največjo stopnjo zmanjšanja tveganja in nadzor. Optimalni model zahteva program razumevanja, zmanjševanja in prenosa tveganja preko uporabe povezane tehnologije, procesov in zavarovanja – pristop k managementu tveganj (Siegel, Sagalow & Serritella, 2002, str. 33).

Pristop k managementu tveganj, ki je v večini gospodarskih panog splošno sprejet, opredeljuje zaščito kot relativno. Zato se tveganja obravnava v odvisnosti od preferenc vključenih strank in kompromisov zaradi posebnosti okolja. Nasprotno je v IT-panogi prevladoval pristop, kjer je zaščita edini način managementa tveganj, v kolikor se tveganjem ni mogoče izogniti. Računalniški strokovnjaki so razvijali tehnologije, ki bodo rešile varnostne težave interneta. Ob ugotovitvi, da popolna varnost ni možna in da so stroški previsoki, se miselnost počasi spreminja v smeri doseganja zadovoljive varnosti. Preostanek tveganja, ki ga ni moč omejiti, pa se lahko prenese na zavarovalnice (Majuca, Yurcik & Kesan, 2006, str. 3).

Gordon et al. (2003) predlagajo, da podjetja najprej investirajo v zaščito pred tveganjem nastanka kršitve varnosti, kar vključuje namestitev požarnega zidu, šifriranje podatkov in tehnike nadzora dostopa. Vendar je kljub najboljši zaščiti, odkrivanju in sistemom za popravke verjetnost nastanka škode zaradi kršitve varnosti velika. Zato je priporočljiv naslednji korak, sklenitev kibernetskega zavarovanja. Obstaja kompromis med obsegom sredstev, ki jih podjetje nameni za zaščito pred varnostnimi kršitvami, in sredstvi za kibernetsko zavarovanje. Za določen nivo informacijske vrednosti oz. ranljivosti je ob višjem nivoju varnostne zaščite potreben manjši obseg kibernetskega zavarovanja in obratno.

Kibernetsko zavarovanje je trenutno ena izmed najhitreje rastočih zavarovalnih vrst na zavarovalnem trgu. Letna globalna premija kibernetskih zavarovanj se bo z današnjih 2,5 milijarde USD predvidoma povečala na 7,5 milijarde USD v letu 2020 (PwC, 2015b).

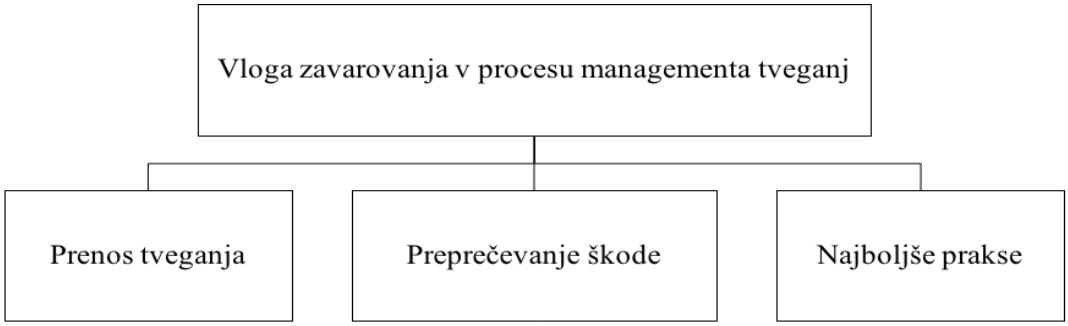
3.1 Vloga zavarovanja v procesu managementa tveganj

Zavarovanje je tradicionalno opredeljeno kot orodje managementa tveganj, kjer ena stranka (zavarovanec) ob plačilu premije prenese del ali celotno tveganje na drugo stranko (zavarovalnico), s sklenitvijo zakonsko obvezujoče pogodbe. Zavarovalnica v zameno zagotovi obljubo za izpolnitev svojih obveznosti v primeru nastanka dogodka, ki je opredeljen kot škoda ali zahtevek. Obljubo zavarovalnice lahko opišemo kot pogojni kapital, ki je zagotovljen zavarovancu za prihodnje dogodke, skladno s pogoji zavarovanja. Dogovor o prenosu tveganja zavarovancu zagotavlja manjšo nestabilnost denarnih tokov in ohranitev premoženja. Odločitev o izbiri zavarovanja kot orodja za materializacijo cilja ohranitve ali povečanja vrednosti podjetja je odvisna od številnih dejavnikov. Ti med drugim vključujejo stroškovno učinkovitost zavarovanja kot metode financiranja tveganj v

primerjavi z drugimi metodami, zaznano vrednost dodatnih storitev zavarovalnice, kapaciteto zavarovalnega trga, zakonsko in davčno regulativo zavarovalnih storitev, zavarovančevo nagnjenost k tveganju in v primeru podjetja njegovo organizacijsko strukturo (Kwon, 2003, str. 36).

Vlogo zavarovanja v procesu managementa tveganj lahko razumemo tudi kot funkcijo prenosa tveganja, preprečevanja škode in najboljših praks, kot prikazano na Sliki 5. V postopku prenosa tveganja se odločitve sprejemajo na osnovi stopnje izpostavljenosti pred kibernetskimi tveganji. Učinkovit način izračuna kibernetskih tveganj vodi do boljšega finančnega managementa tveganj. Z vidika preprečevanja škode so pomembne spodbude zavarovalnic za znižanje zavarovalne premije, ki podjetja usmerjajo k ukrepom za zmanjševanje tveganj. Zavarovalnice lahko s svojimi izkušnjami pri obravnavi škodnih primerov in vpogledom v škodno zgodovino svojih zavarovancev pomagajo podjetjem pri ukrepih za preprečitev nastanka škodnega primera ali pri znižanju posledic v primeru nastanka zavarovalnega dogodka. Z implementacijo uveljavljenih standardov s področja managementa kibernetskih tveganj, priznanih s strani zavarovalnic se izboljša raven kibernetskega varovanja. Upoštevanje smernic zavarovalnic, ki jih podjetja nato privzamejo, pripomore k vzpostavitvi odpornosti proti kibernetskim tveganjem.

Slika 5: Vloga zavarovanja v procesu managementa tveganj



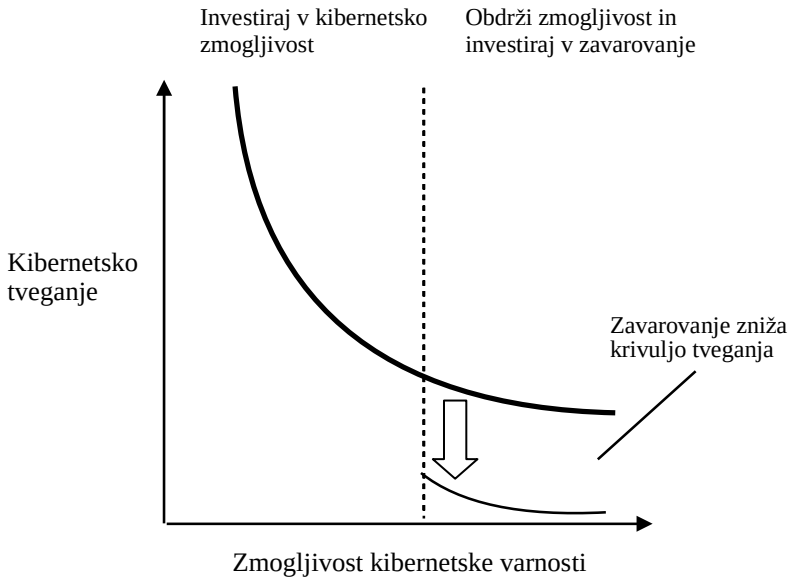
Vir: Timetric, Insight Report: The Future of Cyber Risk Insurance, 2015, str. 21, slika 10.

Vrsto let so se podjetja pri managementu kibernetskih tveganj osredotočala na nakup varnostno-tehnoloških rešitev z namenom odstranitve tveganj. Ključno pri oceni optimalnega obsega sredstev, ki jih podjetje nameni za kibernetsko varnost, je možnost znižanja preprečitve kibernetskega napada. Ti so vendarle neizogibni, zato so podjetja odvisna od finančnih sredstev za premostitev posledic kibernetskega dogodka. Tu ima zavarovalni trg pomembno vlogo, ne samo kot ponudnik finančne gotovosti, temveč tudi kot panoga, ki zagotavlja vpogled in podatke za preudarno investiranje v kibernetsko varnost.

Optimiranje investicij v zniževanje kibernetske izpostavljenosti lahko ponazorimo s Sliko 6, kjer je orisano razmerje med kibernetskim tveganjem in zmogljivostjo kibernetske

varnosti. Podjetja, ki imajo minimalno zmožnost zagotavljanja kibernetske varnosti, so soočena z največjo stopnjo tveganja. Za takšna podjetja pomeni investicija v osnovne mehanizme kibernetske varnosti velik pomik po krivulji kibernetskega tveganja navzdol. Podjetja na skrajni levi strani krivulje bodo na zavarovalnem trgu soočena z visokimi premijami ali kritja sploh ne bodo mogla dobiti, kar je signal, da mora podjetje okrepiti kibernetsko varnost preko uveljavljenih metod omejevanja kibernetskega tveganja. Vendar na določeni točki krivulja postane položna in vsaka dodatna enota sredstev, vložena v kibernetsko zmogljivost, ne prinaša sorazmernega znižanja tveganja. Od te točke naprej je za podjetja smotrno prenesti preostanek kibernetskega tveganja na zavarovalnice.

Slika 6: Krivulja kibernetskega tveganja in zmogljivost kibernetske varnosti



Vir: S. Kannry & D. White, Optimizing Investment to Minimaze Cyber Exposure, 2015, str. 285.

Za razliko od običajih metod omejevanja tveganja zavarovanje zniža ali odpravi stroške v povezavi s kibernetskim dogodkom in tako premakne celotno krivuljo kibernetskega tveganja navzdol.

3.2 Opredelitev kibernetskega zavarovanja

Kibernetsko zavarovanje lahko opredelimo kot prenos finančnega tveganja v povezavi z omrežnimi in informacijsko tehnološkimi incidenti na tretjo osebo (Böhme & Schwartz, 2010, str. 1).

Kibernetsko zavarovanje je vrsta zavarovanja, zasnovana za zaščito uporabnikov tehnoloških storitev ali proizvodov. Natančneje je namen zavarovanja kritje odgovornostnih in premoženjskih škod, ki izvirajo iz uporabe raznih elektronskih dejavnosti, kot so prodaja preko spleta ali zbiranje podatkov v okviru internih elektronskih

omrežij. Posebnost v primerjavi z ostalimi zavarovanji je kritje izgube podatkov in drugih neopredmetenih sredstev ter posledične škode.

Kibernetsko zavarovanje zagotavlja predvsem, ne pa izključno, kritje za odgovornost podjetja za primer kršitve zaupnosti podatkov, pri čemer so s strani hekerjev ali drugih kriminalcev razkrite ali ukradene osebne informacije strank podjetja, kot so na primer številke kreditnih kartic ali zdravstvenega zavarovanja. Zavarovanje krije različne stroške, povezane s kršitvijo zaupnosti podatkov, vključno s stroški obveščanja, spremljanja porabe, obrambe zahtevkov regulatorjev, kazni in glob in škode iz naslova kraje identitete. Dodatno je krita odgovornost, ki izhaja iz spletnih medijskih vsebin, kot tudi premoženjska izpostavljenost iz naslova obratovalnega zastoja, izgube ali uničenja podatkov, računalniške prevare, škoda iz naslova prenosa sredstev in kibernetskega izsiljevanja.

Prve različice današnjega kibernetskega zavarovanja so se pojavile konec 90. let prejšnjega stoletja, ko so zavarovalnice začele razvijati zavarovanja poklicnih odgovornosti z namenom pokritja nevarnosti, ki so se pojavile z novimi tehnologijami, predvsem internetom in elektronskim poslovanjem. Glavna spodbuda je bila negotovost z zanesljivostjo programske opreme ob prehodu v novo tisočletje, t. i. problem milenijskega hrošča (angl. *milleninum bug*) oz. »Y2K« (Allianz, 2015, str. 18). »Spletna« zavarovanja so odražala osnovni namen zavarovanja poklicne odgovornosti in so zagotavljala kritje le za odškodninsko odgovornost iz naslova varnostnih napak v zavarovančevem informacijskem sistemu. Stroški, povezani z omejevanjem škode, nastali na strani zavarovanca, niso bili pokriti. Poleg tega podatki v materialni obliki niso bili predmet zavarovanja.

V nekaj letih so zavarovalnice kritje prilagodile zahtevam zavarovancev in v kritje vključile tudi kršitev zaupnosti podatkov, tako v elektronski kot fizični obliki, postopke nadzornih institucij in prisojene kazni zaradi kršitev zakonodaje ter odgovornost za kršitev pogodbenih obveznosti. Povečano povpraševanje je bilo predvsem posledica novih predpisov s področja varstva osebnih podatkov v ZDA in razmaha organiziranega kriminala, ki je zaznal donosnost iz naslova ukradenih informacij. V zadnjih letih so zavarovalnice v okviru zavarovalnega kritja razvile ponudbo storitev, ki jih zagotavljajo zunanji specializirani svetovalci, za preprečevanje oz. omejitev stroškov zavarovanca (Jones, 2015).

Za razliko od ostalih zavarovanj pri kibernetskem zavarovanju ne obstajajo standardizirani pogoji zavarovanja na zavarovalnem trgu. Kibernetsko zavarovanje sledi razvoju tehnologije. Obseg zavarovalnega kritja pa se v praksi vsako leto spreminja tudi na osnovi izkušenj zavarovalnic s škodnimi primeri. Večina trenutno dostopnih kibernetskih zavarovanj na zavarovalnem trgu zagotavlja kombinacijo kritja zahtevkov tretjih oseb (angl. *third party coverage*), ki jih običajno zagotavljajo tradicionalna odgovornostna zavarovanja, in kritje lastne škode (angl. *first party coverage*).

Kot posebnost kibernetskih zavarovanj velja izpostaviti zagotavljanje svetovalnih storitev zunanjih izvajalcev s področja informacijske varnosti, pravnega svetovanja in odnosov z javnostmi, ki jih v okviru zavarovalnega kritja zagotavljajo nekateri ponudniki kibernetskih zavarovanj.

3.2.1 Zavarovane in nezavarovane nevarnosti

Na splošno zavarovalnice ponujajo kibernetsko zavarovanje na modularni način. Zavarovancem omogočajo izbiro posameznih sklopov zavarovanja, ki so zanje relevantni. V Tabeli 9 je predstavljena vsebina tipične zavarovalne police za kibernetsko zavarovanje. Glavni sklopi kritja pri kibernetskem zavarovanju so:

- Obramba in kritje škode iz naslova zahtevka za očitano odgovornost, ki izvira iz kibernetskega incidenta ali kršitve zaupnosti podatkov (Odgovornost).
- Kritje preiskave in zmanjševanja kibernetskega incidenta ali kršitve zaupnosti podatkov (Odziv na dogodek).
- Kritje stroškov postopkov regulatorjev in prisojenih kazni oziroma glob (Postopki regulatorjev).
- Kritje obratovalnega zastoja zaradi kibernetskega incidenta (Obratovalni zastoj).
- Kritje za odziv na grožnjo povzročitve škode na omrežju ali objave zaupnih informacij (Kibernetsko izsiljevanje).

Pri tem je ključno razumevanje sprožilca (angl. *trigger*) zavarovalnega kritja. Značilnost kibernetskega incidenta je odpoved zavarovančevih informacijskih varnostnih sistemov, medtem ko je incident zaupnosti kakršna koli neuspešna zaščita zaupnih informacij (Jones, 2015, str. 29).

Tabela 9: Tipična zavarovalna polica za kibernetsko zavarovanje

Kritje	**Vzrok kibernetske škode**	**Zavarovane škode**
Sklop A: Zahtevek s strani tretjih oseb		
Odgovornost iz naslova kršitve zasebnosti/zaupnosti informacij	• Razkritje zaupnih informacij zbranih ali upravljanih s strani zavarovanca (npr. zaradi malomarnosti, namernih dejanj, izgube ali kraje s strani zaposlenih)	• Odškodninska odgovornost (vključno s stroški obrambe in kazni regulatorjev) • Posredna odgovornost (v primeru zunanjih izvajalcev) • Nadzor v krizni situaciji, ki vključuje tudi storitve zunanjih svetovalcev (npr. stroški obveščanja deležnikov, varnostnih preiskav, forenzičnih preiskav in odnosov z javnostmi)

se nadaljuje

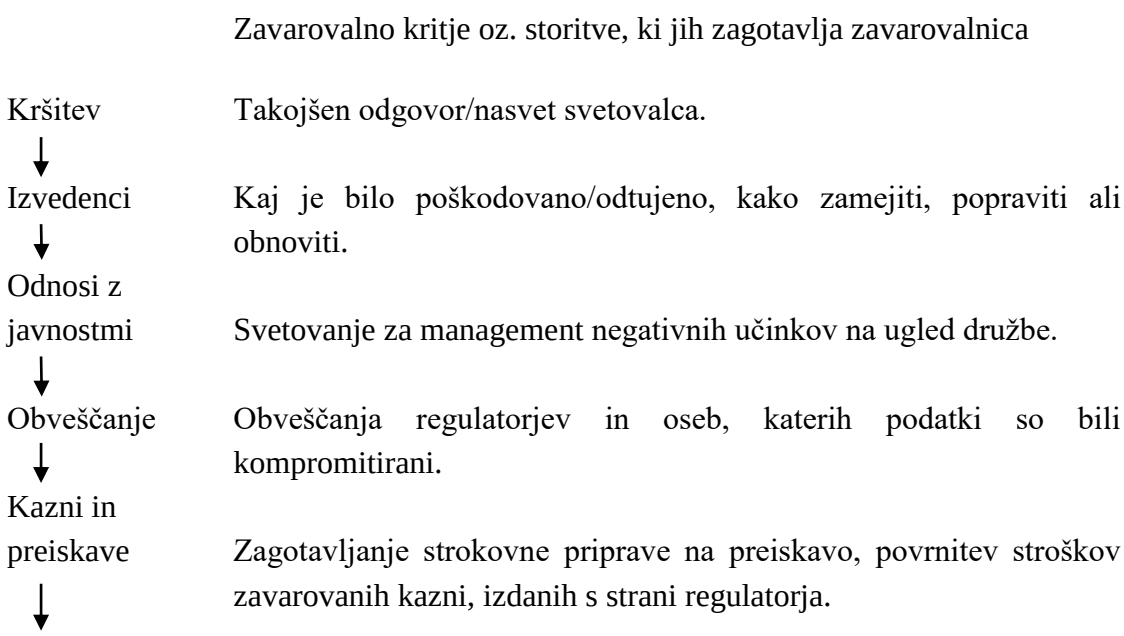
Tabela 9: Tipična zavarovalna polica za kibernetsko zavarovanje (nad.)

Kritje	**Vzrok kibernetske škode**	**Zavarovane škode**
Odgovornost iz naslova zaščite omrežja	• Povzročitev škode tretji osebi zaradi nenamernega posredovanja računalniških virusov • Škoda na sistemu tretje osebe zaradi nepooblaščenega dostopa zavarovanca • Moten dovoljeni dostop strank • Prisvojitev intelektualne lastnine	• Stroški ponovne vzpostavitve • Stroški pravdnih postopkov
Intelektualna lastnina in medijske kršitve	• Kršitev programske opreme, blagovne znamke in medijske izpostavljenosti (obrekovanje ipd.)	• Odškodninska odgovornost (vključno s stroški obrambe in kazni regulatorjev)
Sklop B: Lastna škoda		
Krizni management/ Odziv na dogodek	• Sovražni napad na informacijska in tehnološka sredstva	• Stroški specializiranih ponudnikov za povrnitev ugleda podjetja • Stroški obveščanja deležnikov in neprekinjeni monitoring (npr. uporaba kreditnih kartic)
Obratovalni zastoj	• Napad za zavrnitev storitve • Hekerski vdor	• Stroški ponovne vzpostavitve • Izguba dobička
Zaščita podatkovnih sredstev	• Sprememba, poškodovanje ali uničenje podatkovnih sredstev zaradi računalniškega napada • Poškodovanje ali uničenje drugih neopredmetenih sredstev (npr. programske aplikacije)	• Stroški ponovne vzpostavitve in zamenjava podatkov • Stroški ponovne vzpostavitve in nadomestitev intelektualne lastnine (npr. programske opreme)
Kibernetsko izsiljevanje	• Izsiljevanje za predajo oz. prenos informacij ali tehnoloških sredstev (npr. občutljivi podatki) • Izsiljevanje za zamenjavo, poškodovanje ali uničenje informacij ali tehnoloških sredstev • Izsiljevanje za motenje ali prekinitev storitev	• Stroški plačila izsiljevanja • Stroški izogibanja plačila izsiljevanja (stroški poizvedovanja)

Vir: C. Biener, M. Eling & J. H. Wirfs, Insurability of Cyber Risk: An Empirical Analysis, 2015, str. 136, tabela 2.

Slika 7 prikazuje delovanje kibernetskega zavarovanja in storitve, ki jih zavarovalnice zagotavljajo v okviru zavarovalnega kritja.

Slika 7: Kako deluje kibernetsko zavarovanje



Vir: Advisio, Cyber zavarovanje (interno gradivo), 2016.

Poleg sistemskih izključitev kritja, kot so na primer vojna, terorizem, naravne nevarnosti, radiacija, onesnaževanje, ki jih narekuje pozavarovalni trg, so ključne tri vrste izključitev:

- poškodovanje opredmetenih sredstev oz. premoženjska škoda,
- poškodovanje oseb oz. telesne poškodbe,
- izguba finančnih sredstev.

Kritje za premoženjske škode in telesne poškodbe je običajno podano v uveljavljenih premoženjskih in odgovornostnih zavarovanjih, medtem ko so odtujena finančna sredstva običajno zavarovana v okviru komercialnega zavarovanja kriminalnih dejanj (angl. *commercial crime insurance*). Velja omeniti tudi tveganje izgube intelektualne lastnine, ki je posledica protipravne odtujitve. Zavarovalnice trenutno v okviru kibernetskega zavarovanja tega kritja ne zagotavljajo, saj imajo težave z razumevanjem interne vrednosti škode ob škodnem dogodku.

Z napredkom tehnologije, kot so Internet stvari, računalniško vodeni medicinski pripomočki idr., se povečuje možnost kibernetskega incidenta, ki ima za posledico premoženjsko škodo in/ali telesnih poškodb. Zato nekateri zavarovatelji izključujejo rizike, povezane s kibernetskimi incidenti, iz kritja premoženjskih in odgovornostnih zavarovanj (Jones, 2015, str. 29).

Nekatere zavarovalnice se poslovno povezujejo s ponudniki storitev informacijske varnosti, ne samo za zagotavljanje ustreznega odziva v primeru kibernetskega incidenta, temveč zavarovancem pomagajo pri ocenjevanju in povečevanju informacijske varnosti in odpornosti proti kibernetskim napadom.

3.2.2 Umestitev kibernetskih tveganj v okviru drugih zavarovalnih vrst

Zavarovalnice zagovarjajo stališče, da so tveganja, povezana z varstvom podatkov, bistveno drugačna od običajnih tveganj, ki izvirajo iz opredmetenih sredstev. V večini primerov zavarovalnice v zavarovalnih pogojih premoženjskih in odgovornostnih zavarovanj iz kritja izključujejo škodo na neopredmetenih sredstvih (Glascott & Eisen, 2013, str. 215).

Tabela 10: Primeri tipičnih kibernetskih izključitev in vrzeli v kritju tradicionalnih zavarovanj

Vrsta zavarovanja	**Ključne vrste kritja**	**Potencialna vrzel v kritju kibernetskih nevarnosti**
Premoženjsko zavarovanje	Fizična poškodba sredstev (lastna škoda)	Izključitev kibernetskih napadov in izrecno kritje za fizične poškodbe sredstev. Ni kritja za škodo na programski opremi in podatkih (kar se smatra za neopredmeteno obliko premoženja).
Zavarovanje obratovalnega zastoja	Izgubljeni prihodki in dodatni nastali stroški (lastna škoda)	Tradicionalna zavarovanja niso aktivirana zaradi kibernetskih napadov, ki ne povzročijo fizične škode.
Zavarovanje splošne odgovornosti	Odgovornost do tretjih oseb zaradi fizičnega poškodovanja premoženja, telesnih poškodb in škode zaradi obveščanja (odgovornostni zahtevki, ki izvirajo iz objavljene vsebine, vključno s kršitvijo zasebnosti)	Izključitev nepooblaščenega razkritja osebnih informacij.
Zavarovanje poklicne odgovornosti	Odgovornost do tretjih oseb, ki izvirajo iz opravljanja poklicnih storitev.	Kritje je lahko omejeno samo na odgovornostne zahtevke s strani strank. Zato so zahtevki iz naslova razkritja podatkov zaposlenih pogosto izključeni. Navedene so številke izključitve (npr. prenos računalniških virusov).

Vir: Marsh, UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk. 2015, str. 18, tabela 8.

Zavarovatelji spoznavajo, da so kibernetska tveganja lahko povod za škode oz. zahtevke iz naslova zavarovalnih vrst, kjer kibernetske škode niso izrecno predmet zavarovalnega

kritja. V tem primeru govorimo o t. i. skriti kibernetski izpostavljenosti (angl. *silent cyber exposure*). Gre predvsem za primere zavarovanj, kjer so zavarovane vse nevarnosti, ki niso eksplicitno izključene, t.i. »All Risk« zavarovanja. Zavarovalnice se kljub temu morda ne zavedajo obsega njihove izpostavljenosti za novonastalo vrsto tveganja in ne upoštevajo ustreznega dodatka pri izračunu premije. Zavarovalnice imajo večjo kibernetsko izpostavljenost v okviru svojega portfelja drugih zavarovanj, kot si predstavljajo (Lloyd's, 2015, str. 25). Na podlagi teh ugotovitev je Lloyd's pripravil strategijo v primeru kibernetskih napadov in sindikatom (angl. *syndicates*), ki delujejo v okviru Lloyd'sa, posredoval smernice pri sklepanju zavarovanj. Pri tem je posebej izpostavljena možnost nepričakovane akumulacije zaradi skrite kibernetske izpostavljenosti. Implementacija strategije je predvidena do konca leta 2017 in vključuje sledeče (Lloyd's, 2016):

- podporo za nadaljnji razvoj (po)zavarovalnih rešitev za kibernetske napade, ki bodo v okviru tržišča na Lloyd'su ustrezno naslovljeni v fazi prevzema rizika in kapitalsko podprti,
- spodbudo za razvoj in uporabo ustreznih izključitev in/ali podlimitov za kibernetske napade,
- izoblikovano razumevanje akumulacije rizika kibernetskega napada, vključno z metodologijo za merjenje škodnega potenciala,
- vzpostavitev dobre prakse pri umestitvi tveganja kibernetskega napada v kapitalske modele sindikatov,
- zmanjšano možnost za akumulacijo iz naslova nepričakovanega oz. skritega kibernetskega tveganja.

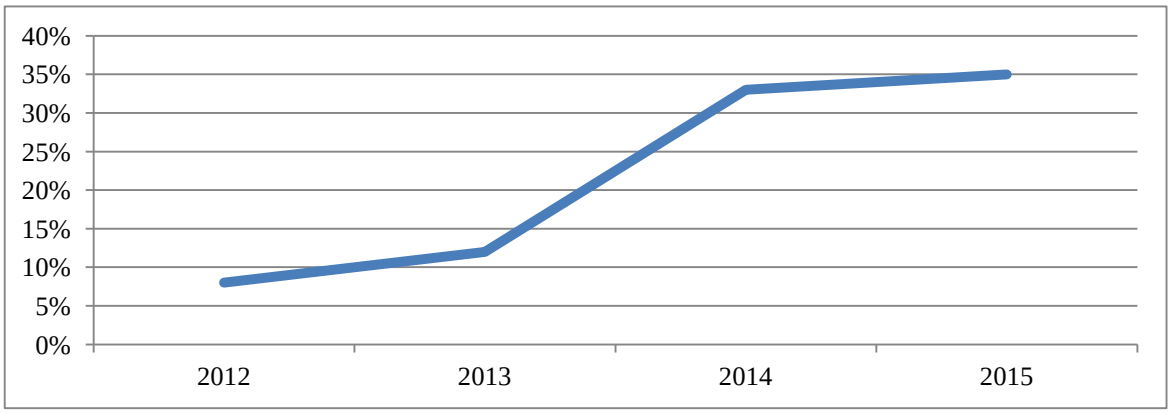
3.2.3 Pregled stanja na zavarovalnem trgu

Do nedavnega so redka podjetja načrtovala sklenitev kibernetskega zavarovanja in še manj jih je dejansko zavarovanje tudi sklenilo. Vendarle se zavarovalnemu trgu kibernetskih zavarovanj napoveduje rast. Zadnji trendi potrjujejo napovedi. Leto 2013 lahko identificiramo kot prelomno leto, ko so poleg velikih podjetij tudi manjša spoznala izpostavljenost pred kibernetskimi tveganji. To je odraz, da je zavarovanje privzeto kot del strategije managementa kibernetskih tveganj (Advisen, 2013).

Skladno s temi ugotovitvami lahko v poročilu raziskave inštituta Ponemon (2015a) razberemo zaskrbljenost managementa zaradi povečane možnosti vpliva kibernetskega kriminala na poslovanje podjetij v prihodnje.

V raziskavi trga kibernetskih zavarovanj (Advisen, 2014a, str. 4) je največ sodelujočih izpostavilo novice o škodah, povezanih s kibernetskimi incidenti, kot ključni razlog za rast povpraševanja. Kot naslednja pomembna dejavnika na strani povpraševanja sta bila izpostavljena povečano znanje in zavedanje o kibernetskem zavarovanju in zahteva tretjih oseb (npr. poslovnih partnerjev in strank) za predložitev dokazila o sklenjenem kibernetskem zavarovanju.

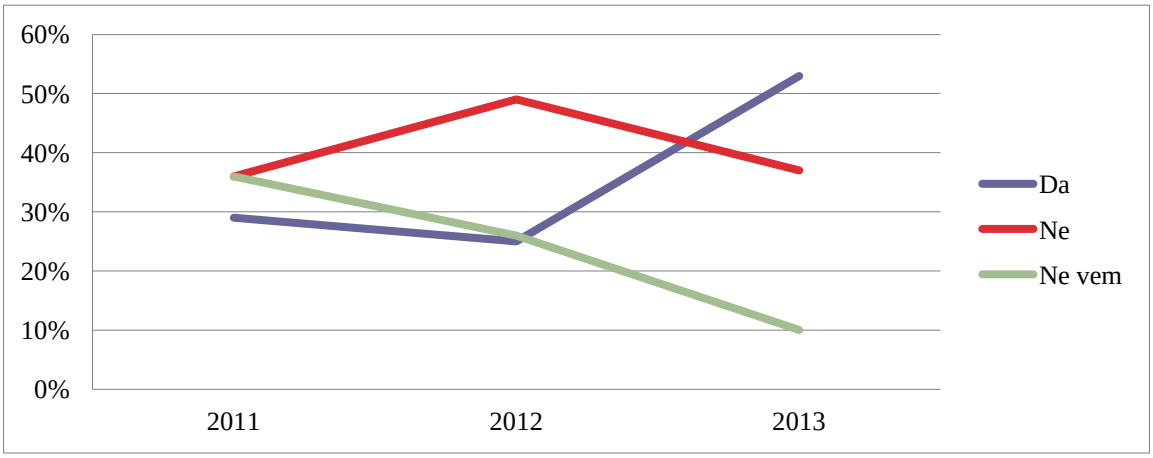
Slika 8: Delež evropskih podjetij s sklenjenim kibernetskim zavarovanjem



Vir: Advisen, 2015 Network Security & Cyber Risk Management, 2015, str. 9, slika 7.

Čeprav še vedno precej manj kot v ZDA se je delež evropskih podjetij, ki imajo sklenjeno kibernetsko zavarovanje, v nekaj letih zvišal na več kot tretjino, kot je razvidno iz Slike 8. Na podlagi tega lahko ocenimo, da je kibernetsko zavarovanje postalo del orodja managementa kibernetskih tveganj.

Slika 9: Ali načrtujete sklenitev kibernetskega zavarovanja v naslednjih letih?



Vir: Advisen, 2013 Information Security Cyber Liability & Risk Management, 2013, str. 8, slika 7.

Veliko podjetij načrtuje sklenitev kibernetskega zavarovanja v prihodnje, vendar jih ne bistveno manj ne namerava skleniti zavarovanja zaradi dodatnih stroškov in izključitev po polici, omejitev in nezavarovanih tveganj. Drugi razlogi za počasnejšo razširjenost kibernetskih zavarovanj so: 1) prepričanje, da so investicije v preventivo boljše kot zavarovanje, 2) omejen trg zavarovanj, 3) neznanje zavarovalnega posrednika in 4) pomanjkanje informacij za sprejem odločitev (Glascott in Aisen, 2013).

Premija iz naslova kibernetskih zavarovanj, ki so jo globalno zbrale zavarovalnice, je v letu 2014 znašala 2,5 milijarde USD. Večino zavarovanj, 90 %, sklenejo podjetja iz ZDA.

Glede na to, da so kibernetska tveganja splošno prisotna, brez geografskih omejitev, je možnost rasti na preostalih zavarovalnih trgih velika. Na primer v Veliki Britaniji ima samo 2 % podjetij sklenjeno samostojno kibernetsko zavarovanje. Tudi v ZDA, kjer so tovrstna zavarovanja bolj uveljavljena, ima samo tretjina podjetij sklenjeno kibernetsko zavarovanje. Obstajajo tudi razlike v razširjenosti zavarovanja po panogah. Če je stopnja zavarovalne gostote samo 5 % pri proizvodnih podjetjih, ima tovrstno zavarovanje sklenjenih približno 50 % podjetij v zdravstvu, trgovini in tehnologiji (PwC, 2015a).

Ob zavedanju kibernetskih tveganj, zahtevah po predložitvi dokazil o sklenjenem kibernetskem zavarovanju s strani poslovnih partnerjev in regulatorjev se bo obseg sklenjenih zavarovanj v prihodnje še povečeval. Ocenjena globalna premija iz naslova kibernetskih zavarovanj bo v letu 2025 znašala 18 milijard USD. Izrazito rast premije je v zadnjem obdobju zaznati pri Lloyd'su, kjer se je število zavarovalnih sindikatov, ki ponujajo kibernetsko zavarovanja, z 22 v letu 2013 povečalo na 63 v letu 2016. Letna premija na tržišču Lloyd's of London je v letu 2015 dosegla 322 milijonov britanskih funtov (v nadaljevanju GBP), medtem ko je leto prej znašala 206 milijonov GBP. V letu 2016 je pričakovana ohranitev rasti in letna premija v višini 500 milijonov GBP. Tudi pri Lloyd'su večina, 80 % premije, izvira iz naslova rizikov iz ZDA (Lloyd's, 2016).

Na splošno je s strani zavarovalnic zaznati interes po nadaljnji rasti trga kibernetskih zavarovanj, predvsem zaradi nadpovprečno visokih premijskih stopenj v primerjavi z ostalimi odgovornostnimi zavarovanji (PwC, 2015a).

3.2.4 Ponudba na zavarovalnem trgu

Na splošno obstajata dva glavna razloga za omejeno ponudbo na zavarovalnem trgu za kibernetska tveganja: nizka raven poznavanja nove oblike tveganja in pomanjkanje podatkov o škodnem dogajanju. Nekateri avtorji (Biener et al., 2015) izpostavljajo tudi omejeno ponudbo pozavarovalnic, ki podobno kot zavarovalnice brez zanesljivih aktuarskih podatkov ne morejo natančno oceniti škode, ki lahko nastane zaradi kibernetskih incidentov. V nadaljevanju so izpostavljeni glavni izzivi pri razvoju trga kibernetskih zavarovanj, ki vključujejo naključnost škodnega dogodka, asimetrijo informacij in določanje zavarovalne premije.

Na podlagi raziskave trga kibernetskih zavarovanj v ZDA, ki jo izvedel Advisen (2014a, str. 6), lahko ugotovimo, da je 73 % vprašanih kot glavno oviro pri sklepanju tovrstnih zavarovanj navedlo pomanjkanje razumevanja izpostavljenosti pred kibernetskimi tveganji. Med glavnimi razlogi so navedeni: nesprejemanje s strani IT-strokovnjakov, da so njihovi sistemi lahko ogroženi, in zanikanje zavarovancev o izpostavljenosti kibernetskim tveganjem. Skoraj polovica vključenih v raziskavo je kot naslednja najpomembnejša razloga za nesklenitev zavarovanja izpostavila pomanjkljive informacije o zavarovalnem produktu in znanje s strani zavarovalnih posrednikov ter strošek zavarovanja oz. natančneje izostanek planiranih sredstev za kibernetsko zavarovanje.

V večini razpoložljive literature na temo kibernetskih zavarovanj (npr. Gordon et al., 2003; Glascott & Aisen, 2013) se izpostavljajo značilnosti kibernetskih tveganj. Asimetrija informacij in s tem povezana negativna selekcija in moralni hazard ter visoka korelacija rizikov negativno vplivajo na ponudbo kibernetskih zavarovanj.

V idealni situaciji imajo pogodbene stranke popolne informacije, ki so pomembne za sprejemanje odločitev. Vendar ima lahko ena stranka nepopolno informacijo o vsebini proizvoda oz. storitve, ki je predmet pogodbe. V zavarovalništvu težava nastane, ko se zavarovatelji ne zavedajo, ali potencialni zavarovanec predstavlja visoko ali nizko tveganje z vidika ocene rizika. Ker zavarovanec ve ali je nizko ali visoko tveganje, medtem ko zavarovatelj tega ne ve, obstaja med njima asimetrija informacij, ki vodi do problema **negativne selekcije**. Ko nastane takšna situacija, teorija predvideva, da zavarovatelj ponudi dva tipa pogodbe: pogodbo z nizko premijo in ozkim kritjem za podjetja z nizkim tveganjem in pogodbo z visoko premijo in širokim kritjem za tiste z visokim tveganjem. V ravnovesju podjetja z visokim tveganjem izberejo ponudbo s polnim zavarovalnim kritjem, medtem ko tisti z nizkim tveganjem izberejo ponudbo z omejenim obsegom kritja. Na ta način so podjetja z nizkim tveganjem prikrajšana za ustrezno kritje (Majuca et al., 2006, str. 8).

Pri kibernetskem zavarovanju se problem negativne selekcije jasno pokaže na način verjetnosti kršitve varnosti. Podjetja, kjer je večja verjetnost kršitve informacijske varnosti, bodo bolj nagnjena k sklenitvi kibernetskega zavarovanja kot podjetja z majhno verjetnostjo takšne kršitve. Z namenom zaščite pred negativno selekcijo zavarovalnice pred sklenitvijo kibernetskega zavarovanja običajno zahtevajo pregled informacijske varnosti pri zavarovancu (Gordon et al., 2003, str. 82).

Druga večja težava, s katero se soočajo zavarovatelji pri razvoju kibernetskih zavarovanj, je problem **moralnega hazarda**. Ta nastane, ko podjetja s sklenjenim kibernetskim zavarovanjem namenoma povzročijo škodo ali ne izvajajo preventivnih ukrepov za preprečitev nastanka škode. Podjetja lahko po sklenjenem zavarovanju izvajajo ohlapnejšo varnostno politiko, tako ne investirajo v varnostno infrastrukturo ali nimajo spodbude za ohranitev ali nadgradnjo obstoječe ravni varnosti (Majuca et al., 2006, str. 11).

Medtem ko se negativna selekcija nanaša na zavarovančeve privatne informacije oz. skrite informacije (angl. *hidden information problem*) pred sklenitvijo zavarovalne pogodbe, se problem moralnega hazarda ukvarja s pomanjkanjem spodbude zavarovanca za dejanja (angl. *hidden action problem*), ki znižujejo verjetnost nastanka škode po sklenitvi zavarovanja. Zavarovalnice lahko problem moralnega hazarda omejijo z določitvijo samopridržaja zavarovanca oz. odbitne franšize v zavarovalni pogodbi. V primeru nastanka zavarovalnega primera bo zavarovanec finančno breme škode delno nosil sam. S tem samopridržaj deluje kot finančna spodbuda zavarovanca k dejanjem, ki znižujejo verjetnost nastanka škodnega dogodka. Drugi način za zmanjšanje problema moralnega

hazarda je znižanje zavarovalne premije, v kolikor zavarovanec z določenimi ukrepi oz. aktivnostmi zniža verjetnost nastanka škodnega dogodka (Gordon et al., 2003, str. 82; Majuca et al., 2006, str. 11).

Razlika med problemom moralnega hazarda in negativne selekcije je v stroških in njuni strukturi. Za obvladovanje problema negativne selekcije je potrebna investicija v postopek podpore odločanja, s katerim se določi klasifikacija tveganja potencialnega zavarovanca. Slednjega zavarovalnici ni potrebno pogosto preverjati. Za investicijo so značilni nepovratni stroški (angl. *sunk costs*). Nasprotno je za omejitev moralnega hazarda potrebna investicija v infrastrukturo za nadzor in spremljavo zavarovanca, ki jo je potrebno neprestano pregledovati (Majuca et al., 2006, str. 11).

Za ugotavljanje **možnosti prevzema rizikov** v zavarovanje se pri analizi zavarovalnega trga in zavarovalnih produktov največkrat presojajo kriteriji, ki jih je uvedel Berliner (1985, str. 325).

Tabela 11: Kriteriji možnosti prevzema rizikov v zavarovanje

Kriterij možnosti zavarovanja		**Zahteve**
Aktuarski	Naključnost škodnega dogodka	Neodvisnost in predvidljivost škodne izpostavljenosti
	Največja možna škoda	Obvladljiva
	Povprečna škoda po dogodku	Zmerna
	Škodna izpostavljenost	Mora biti velika
	Asimetrija informacij	Neizrazita prisotnost moralnega hazarda in negativna selekcija
Tržni	Zavarovalna premija	Povrnitev stroškov zavarovalnice in dostopnost
	Limit kritja	Sprejemljiv
Družbeni	Javna politika	Skladno z družbenimi vrednotami
	Pravne omejitve	Kritje je dovoljeno

Vir: B. Berliner, Large Risks and Limits of Insurability, 1985, str. 325.

Osnovni pogoj za zagotavljanje zavarovanja pred določenimi riziki je neodvisnost rizikov in predvidljivost škodne izpostavljenosti (Biener et al., 2015, str. 141). Hkrati je to tudi **aktuarski kriterij** možnosti zavarovanja skladno s Tabelo 11.

Drugače kot v fizičnem svetu, kjer so riziki geografsko razpršeni, v informacijskem svetu zlorabe omrežij računalniški črvi in virusi takšnih omejitev nimajo. Pri slednjih Böhme in Kataria (2006, str. 3) ugotavljata visoko interno kot tudi globalno **korelacijo rizikov**. Zaradi izrazite homogenosti in prisotne odvisnosti informacijskih sistemov ima njihova odpoved visoko korelacijo, kar vpliva na odločitev zavarovalnic pri določanju višje premije oz. omejeni ponudbi kibernetskih zavarovanj.

Na drugi strani Biener et al. (2015, str. 141) na osnovi empirične analize ugotavljajo, da so v 16,8 % primerov kibernetskih incidentov škode povezane s škodo v drugem podjetju. Z drugimi besedami, večina kibernetskih incidentov ni v korelaciji z drugimi primeri, pri čemer je pomembno upoštevati tudi dejstvo, da se v nekaterih kategorijah kibernetskih tveganj korelacija ne pojavi vedno, zato je potrebno naključnost gledati v kontekstu dejanskega incidenta (npr. fizična kraja podatkov). Poleg vprašanja korelacije je razpršitev rizikov omejena s trenutno relativno majhnim številom sklenjenih kibernetskih zavarovanj.

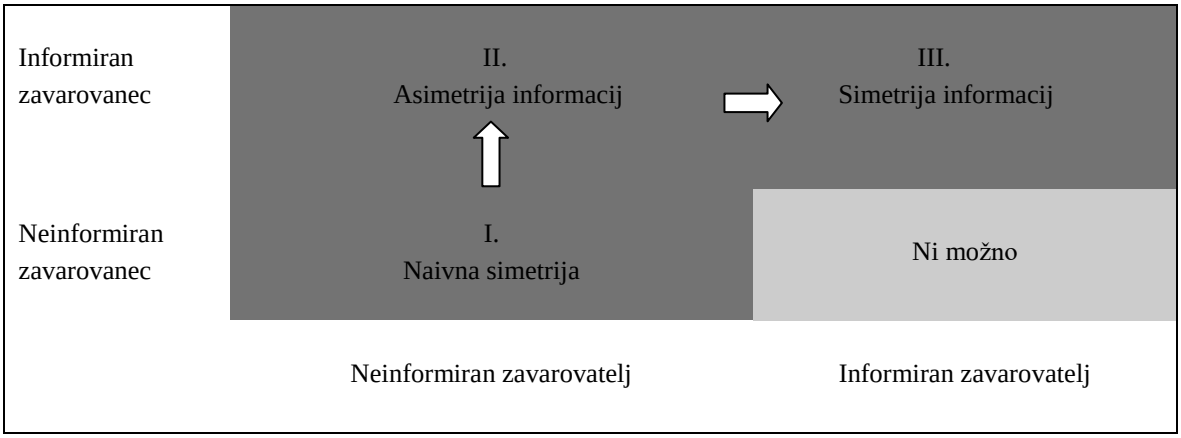
Na podlagi analize podatkovne baze operativnih škod, ki so jo izvedli Biener et al. (2015, str. 139), izhaja, da so največje pretekle škode iz naslova kibernetskih tveganj znatno nižje kot tiste pri splošnih operativnih tveganjih. S tega vidika se zdijo škode iz naslova kibernetskih tveganj obvladljive. Vendar je potrebno upoštevati tudi dinamiko razvoja tehnologije in posledično povečane izpostavljenosti katastrofalnim škodnim dogodkom, ki lahko v skrajnem primeru povzročijo zavarovateljevo insolventnost (Marsh, 2015, str. 23). Temu pritrjuje tudi raziskava PwC (2015a), iz katere je razviden naraščajoči finančni vpliv vedno večjega števila varnostnih incidentov. Teh so v letu 2014 zabeležili skoraj 43 milijonov, kar je ekvivalent 100.000 kibernetskih napadov na dan. Povprečna finančna škoda za velika podjetja je v letu 2014 znašala 5,9 milijona USD, medtem ko je za srednje velika podjetja, s prihodki med 100 milijoni in 1 milijardo USD, znašala 1,3 milijona USD. Zavarovalnice so tako lahko soočene s hitrim zaporedjem zelo velikih škod, ki jih je težje izravnati oz. zagotoviti zaščito bilance zavarovalnice.

Kot omenjeno, je za trg kibernetskih zavarovanj značilna **asimetrija informacij**, kar vodi v neoptimalni prenos kibernetskih tveganj. Pomanjkanje informacij o rizikih, ki jih ima morda zavarovanec na razpolago, lahko vodi do negativne selekcije rizikov. V vsakem primeru navedene situacije odražajo oportunistično obnašanje tako na strani povpraševanja kot na strani ponudbe (Glascott & Eisen, 2013, str. 213).

Na Sliki 10 so prikazani premiki na trgu kibernetskih zavarovanj preko možnih scenarijev asimetrije informacij. Prvotno je trg v stanju naivne simetrije (I. kvadrant), kjer niti zavarovanec niti zavarovatelj ne poznata obstoja, narave ali obsega sekundarne škode. V podjetju se ob izvajanju poslovnih procesov soočijo s posledicami neuporabe, zlorabe in neustrezne rabe informacijskih sredstev. Zavarovanec zazna možnost nastanka sekundarne škode in na tej osnovi optimizira strategijo prijave zahtevkov zavarovatelju, kar je v nasprotju s pogodbeno pričakovanim vedenjem. Trg se premakne iz območja naivne simetrije v II. kvadrant, asimetrijo informacij. V okviru informacijske asimetrije zavarovanec ne uspe ustrezno opozoriti na izvenpogodbeno vedenje oz. zavarovatelj ob pripravi zavarovalne pogodbe ne upošteva prejetih opozoril. Kakor koli, zavarovalni trg je v stanju informacijske asimetrije in zavarovanci posledično plačujejo višje premije zaradi tržne neučinkovitosti. V kolikor zavarovatelji pri določanju zavarovalne premije upoštevajo dejstvo, da zavarovanci selektivno upoštevajo pogoje zavarovanja, se vzpostavi

stanje, ko se kibernetska tveganja učinkoviteje prenašajo od zavarovanca k zavarovatelju (Bandyopadhyay et al., 2009).

Slika 10: Asimetrija informacij in tržne spremembe



Vir: T. Bandyopadhyay et al.,Why IT Managers Don't Go for Cyber - Insurance Products, 2009, str. 72, slika 8.

Kibernetsko zavarovanje se zdi zavarovancem cenovno nedostopno in z nepravično določeno zavarovalno premijo. Po mnenju Biener et al. (2015) obstajajo vsaj štirje razlogi za to, in sicer:

- novost zavarovanja in posledično manjši zajem tveganj,
- novost zavarovanja in posledično manjše število ponudnikov,
- novost zavarovanja in omejenost podatkov, kar je vzrok za visoke pribitke na zavarovalno premijo,
- precejšna asimetrija informacij, ki zahteva drago preverjanje stanja in vnaprejšnjo oceno tveganja.

Na podlagi študij, ki obravnavajo ustreznost višine zavarovalne premije, se te pri kibernetskih zavarovanjih lahko na splošno smatrajo za zmerne. Razen pri zavarovanjih za srednja in majhna podjetja, kjer so zavarovalne premije ocenjene kot previsoke (Biener et al., 2015).

Trenutno je na zavarovalnem trgu ustrezna dostopnost za zahtevani limit kritja za večino zavarovancev. Obstajajo pa omejitve kritja za določena tveganja, med katerimi je pomembno tveganje izgube ugleda podjetja. Tega tveganja zavarovalnice v okviru kibernetskega zavarovanja največkrat ne želijo v celoti pokriti (Biener et al., 2015). Zaradi velikega števila izključitev kritja in dinamične narave kibernetskih tveganj obstaja negotovost glede dejanskega kritja. Zapletenost zavarovalnih pogojev se tako izpostavlja kot eno večjih ovir za sklenitev zavarovanja na strani zavarovancev. Veliko podjetij tudi verjame, da njihova obstoječa premoženjska in odgovornostna zavarovanja nudijo zadostno kritje za kibernetska tveganja (ENISA, 2012). Pogosto se kot pogoj za veljavnost

kritja pojavlja obveznost zavarovanca, da zagotavlja šifriranje podatkov, in klavzula za zagotavljanje najnovejših posodobitev programske opreme, kar pa je podjetjem težko stalno zagotavljati (PwC, 2015a).

Z vidika družbenega kriterija velja omeniti ugotovitev Bolot in Lelarge (2009), ki v nasprotju z zgoraj navedenim mnenjem o zmanjšanju investicij v varnost zaradi zavarovanja ugotavljata da razširjena praksa sklepanja kibernetskih zavarovanj povečuje splošno internetno varnost in zagotavlja močno spodbudo za investicije v samozaščito. To predstavlja javno dobro, ki prinaša pozitivne eksternalije. Glede na to se zastavlja vprašanje posredovanja oblasti v imenu promocije trga kibernetskih zavarovanj. Zaradi pomanjkanja pozavarovalnih kapacitet za kibernetska tveganja se izpostavlja dodatna vloga vlade v funkciji zavarovatelja v skrajni sili, na podoben način kot so v nekaterih državah vzpostavljena državna jamstva za (po)zavarovalni trg v primeru terorizma (ENISA, 2012).

Ponekod zaradi pravnih omejitev nekaterih klavzul zavarovalnega kritja ni mogoče uporabiti. V nekaterih državah je na primer zakonsko prepovedano zavarovati kazni regulatorjev. Nova splošna uredba o varstvu podatkov v EU med drugim predvideva obvezno obveščanje oškodovancev. Za kršitelje zakonodaje so predvidene tudi visoke kazni, kar za zavarovalnice pomeni povečano tveganje. Po drugi strani pa sprememba zakonodaje lahko vodi v povečano povpraševanje po kibernetskih zavarovanjih.

Kljub temu da se kot glavni razlog za počasen razvoj trga kibernetskih zavarovanj največkrat omenja neizkušenost zavarovalnic in posledični konzervativni pristop k oblikovanju ponudbe, nekateri, kot so na primer Bandyopadhyay, Mookerjee in Rao (2009), izpostavljajo **omejitve na strani povpraševanja**. Ob predpostavki, da ne obstaja regulatorna zahteva za razkritje kršitve zaupnosti podatkov, so avtorji mnenja, da je premija, ponujena s strani zavarovalnic, previsoka zaradi nezmožnosti ocene zavarovalnic o višini sekundarne škode zavarovancev.

V primeru kibernetskega incidenta je podjetje najprej soočeno s primarno škodo, zaradi izgubljenih informacij ali podatkov in operativne izgube. Sekundarna škoda nastane, ko po javnem razkritju informacije o kibernetskem incidentu deležniki (investitorji in stranke), zaradi dvoma o varnosti informacijskega programa spremenijo svojo percepcijo o tveganjih podjetja in posledično znižajo vrednost podjetja. V primeru obstoja kibernetskega zavarovanja se ob kibernetskem incidentu pojavi povečan pretok informacij preko zunanjih izvajalcev zavarovanca, kar zelo zniža možnost ohranitve informacije o kršitvi zaupnosti podatkov v privatni domeni. Odločitev managementa o prijavi zavarovalnega primera zavarovalnici tako temelji na presoji možnosti povrnitve skupne, primarne in sekundarne, škode iz naslova izplačila zavarovalnice.

Dodatna omejitev na strani ponudbe kibernetskih zavarovanj je dinamična narava kibernetskih tveganj, ki se zaradi tehnološkega napredka in uporabe novih sistemov ter

naprav hitro in drastično spreminjajo. Analiza preteklih podatkov iz naslova kibernetskih tveganj je zato lahko zavajajoča, v kolikor se je narava obravnavanega tveganja bistveno spremenila (Biener et al., 2015, str. 142).

Čeprav se zdi ena izmed osnovnih funkcij pozavarovanja, zagotavljanje kritja zavarovalnicam v primeru izjemnih katastrofalnih dogodkov, uporabna tudi v primeru kibernetskih zavarovanj, so pozavarovalnice pri ponujanju svojih kapacitet previdne. Enako kot pri zavarovanju je tudi pozavarovanje bolj učinkovito, v kolikor se riziki lahko združujejo ob predpostavki obstoja velikega števila zavarovalnic z neodvisnim ali pa vsaj omejeno povezanim portfeljem rizikov. Pri prevladujočih zavarovalnih vrstah se to lahko doseže z regionalno ali mednarodno razpršitvijo rizikov, vendar je zaradi globalne homogenosti kibernetskih tveganj, ki jih lahko pogosto pripišemo homogenosti informacijskih sistemov, pozavarovalni trg za kibernetska tveganja zelo omejen (Böhme & Schwartz, 2010, str. 17).

Kljub zaznanim, morda teoretičnim omejitvam pri zavarovanju kibernetskih tveganj se trg kibernetskih zavarovanj razvija in raste. En razlog za hitro rast je uvedba strožje zakonodaje na področju varstva osebnih podatkov v ZDA in Evropi (Glascott & Eisen, 2013, str. 213). Poleg tega smo v letih 2013 in 2014 zabeležili večje število medijsko odmevnih primerov kibernetskih incidentov (Ponemone, 2015a, str. 1). Ne gre pa zanemariti tudi dejstva, da so kapitalski trgi v iskanju naložbenih priložnosti v obdobju nizkih donosov z vlaganjem finančnih sredstev v (po)zavarovalno panogo doprinesli k presežku (po)zavarovalnih kapacitet na mednarodnem trgu zavarovanj. Posledično se tudi na trgu kibernetskih zavarovanj pojavljajo novi ponudniki, tudi v Evropi.

3.2.5 Določanje zavarovalne premije pri kibernetskem zavarovanju

Na splošno se postopek zavarovalnice za oceno pričakovanih stroškov iz naslova škode, določanje ustrezne premijske stopnje in odločitev o pripravi ponudbe za zavarovanje imenuje prevzem rizika (angl. *underwriting*). Določanje premije po zavarovalni vrsti in s tem povezani standardi prevzema rizika se razlikujejo med zavarovatelji (Harrington & Niehaus, 2003, str. 141).

Pri določanju zavarovalne premije se zavarovatelji tradicionalno zanašajo na aktuarske izračune, ki temeljijo na veliki količini preteklih podatkov. Ob dejstvu, da internet ni dolgo v uporabi, ne obstaja dolga zgodovina elektronskih prevar in s tem povezanih škod. Zbirke podatkov o varnostnih kršitvah, ki obstajajo (npr. www.cert.org), ne vključujejo veliko preteklih let. Poleg tega so njihove vrednosti vprašljive, ker podjetja pogosto ne želijo razkriti podrobnosti o kršitvi varnosti (Gordon et al., 2003, str. 82).

Naloga prevzemnika rizika (angl. *insurance underwriter*) je ustrezna ocena izpostavljenosti zavarovancev in ugotovitev, v kakšnem obsegu so se kibernetska tveganja v procesu managementa tveganj zmanjšala. Ko je ocena narejena, lahko prevzemnik rizika

določi ustrezni obseg kritja in zavarovalno premijo oz. ceno zavarovanja. V procesu ocene in prevzema rizika se običajno poslužujejo zbiranja informacij s pomočjo izpolnjenih vprašalnikov zavarovancev, spletnih orodij za samooceno rizika ali tehnologije zunanjih ponudnikov. Zavarovalnice vedno bolj vztrajajo, da zavarovanci pred sklenitvijo zavarovanja opravijo ustrezne ukrepe za zmanjšanje tveganja (Advisen, 2014b, str. 5).

Med drugim prevzemnike rizika zanima, kako so zaščiteni podatki pred nepooblaščenim dostopom in malomarnim razkritjem. Zanima jih, ali so podatki shranjeni na lokalnem strežniku ali pri ponudniku oblačnih storitev, kakšni so sistemi požarne zaščite, šifriranja podatkov, možnost oddaljenega brisanja podatkov z ukradene naprave, kako hitro so odvzete uporabniške pravice bivšega zaposlenega, sposobnost zaznave vdora v sistem in skladnost z najnovejšimi standardi za transakcije s kreditnimi karticami. Nekateri ukrepi, kot je na primer zaznava vdora v sistem, se uporabljajo samo pri najbolj naprednih zavarovancih, kot so finančne institucije (Advisen, 2014b, str. 7).

Analiza določanja zavarovalne premije pri kibernetskem zavarovanju kaže, da je stopnja na linijo (angl. *rate on line*), osnova enota za merjenje višine premije in izračunana kot razmerje med zavarovalno premijo in limitom kritja, trikrat višja kot pri zavarovanju splošne odgovornosti in šestkrat višja kot pri premoženjskem zavarovanju. Na izračun premije vpliva več dejavnikov. V primeru kibernetskega zavarovanja lahko na premijo vpliva tudi negotovost glede tveganja v primerjavi s tradicionalnimi zavarovanji. To se odraža pri bistveno bolj ploskem premiranju kibernetskih zavarovanj kot pri drugih zavarovalnih vrstah. Razlika med tretjo in prvo četrtino višine zavarovalne premije znaša 1,7-kratnik pri kibernetskem zavarovanju, medtem ko znaša razlika pri zavarovanju splošne odgovornosti 9,1-kratnik in pri premoženjskem zavarovanju 2,6-kratnik. Kombinacija višje absolutne zavarovalne premije in nizke cenovne diferenciacije nakazuje zgodnjo fazo v razvoju kibernetskih zavarovanj ter konzervativnejši pristop prevzemnikov rizika. Taka razmerja pa ne spodbujajo zavarovancev k zmanjšanju kibernetskih tveganj in s tem prihranku pri zavarovalni premiji (Marsh, 2015, str. 22).

Negotovost glede tveganja še dodatno povečuje dejstvo, da kibernetske varnostne kršitve lahko ostanejo nezaznavne še nekaj mesecev ali celo let. Na ta način se poveča možnost akumulacije in povečanja škod. Delno je razlog za relativno visoke premije pri kibernetskem zavarovanju tudi omejeno število zavarovalnic, ki ponujajo takšno zavarovanje (PwC, 2015, str. 9).

Višino zavarovalne premije zavarovalnice določajo glede na dejavnost zavarovanca, merljive podatke, kot so število zapisov osebnih podatkov, število zaposlenih in prihodki, ter oceno naprednosti IT zavarovanca. Biener et al. (2015, str. 144) poleg majhnega povpraševanja in ponudbe ter pribitkov na zavarovalno premijo zaradi omejenih podatkov izpostavljajo še izrazito asimetrijo informacij, ki zahtevajo stroškovno izdatno preverjanje stanja in predhodne ocene rizika.

Kibernetsko zavarovanje je relativno nova zavarovalna vrsta z omejenim številom do zdaj izplačanih škod. Posledica so neskladni standardi ocene rizika in določanja primerne premije. Izostanek pravil pri prevzemu rizika onemogoča zavarovateljem določiti ustrezno premijo (angl. *fair premium*) brez znatnega skrbnega pregleda in presoje vsakega posredovanega povpraševanja. Pomembno je, da lahko izostanek ustreznih aktivnosti pri prevzemu rizika pripelje do premije, ki z vidika narave predmetnega rizika ni pravična niti za zavarovalnico niti za zavarovanca (Glascott & Aisen, 2013, str. 210). Harrington in Niehaus (2003, str. 134) opredelita ustrezno premijo kot premijo, ki bi jo zavarovalnice zaračunale na popolnoma konkurenčnem zavarovalnem trgu, pri čemer so upoštevane pričakovane škode, prihodki od naložb, administrativni stroški in ustrezni dodatek za dobiček zavarovalnice.

Osnovni problem pri določanju cene kibernetskega zavarovanja je v izostanku razpoložljivih podatkov. Ne glede na razvoj natančnosti in visoke stopnje naprednosti modeliranja kibernetskih tveganj je njihova uporabna vrednost brez ustreznih vhodnih podatkov majhna (Biener et al., 2015, str. 142). Zaradi pomanjkanja jasnosti o kibernetskih tveganjih so zavarovatelji pri določanju višine premije konzervativni (Bandyopadhyay et al., 2009).

3.3 Izzivi v prihodnje

Management kibernetskih tveganj se ne posveča dovolj seštevanju kibernetskih tveganj. Medsebojna povezanost družbe in interneta lahko v primeru majhne napake ali serije napak na enem mestu povzroči prekomerni vpliv drugje (Risk Nexus, 2014, str. 2).

Trenutno se v managementu kibernetskih tveganj poenostavljeno domneva, da so tveganja posamezne zasebne/javne dejavnosti ali države preprost seštevek lokalne tehnologije in postopkov v posamezni organizaciji. Odgovorni za management tveganj se osredotočajo večinoma na tisto, kar se dogaja znotraj njihovega podjetja. Glede na to, da kibernetska tveganja niso zaprta znotraj posameznih podjetij, morajo managerji razširiti svoja obzorja. Povezovanje v internet pomeni izpostavljenost množici tveganj iz naslova medomrežnih povezav z in v odvisnosti še od poslovnih partnerjev, zunanjih izvajalcev in pogodbenikov, verige dobaviteljev, moteče tehnologije, energetske infrastrukture in zunanjih šokov. V preteklosti so se motnje iz tega naslova že pojavljale, vendar je bila družba do nedavnega omejeno odvisna od interneta. Takšna sistemska kibernetska tveganja so bila največkrat prezrta. Na nek način je to zelo podobno neupoštevanju podobnega sistemskega tveganja v finančnem sektorju pred finančno krizo v letu 2008 (Risk Nexus, 2014, str. 5).

3.3.1 Trendi razvoja kibernetskega zavarovanja

V prihodnje lahko pričakujemo, da bo zaradi izostanka zanesljivih podatkov določanje višine premije še vedno bolj podvrženo neaktuarskim metodam. Pričakuje pa se boljši pregled nad ocenjeno največjo verjetno škodo, s katero bodo zavarovalnice lahko

uravnavale svojo nagnjenost k tveganju. Za boljšo oceno izpostavljenosti zavarovancev bodo zavarovalnice morale zaposliti strokovnjake s področja IT in varnostnih agencij, ki bodo dopolnili znanje aktuarjev in prevzemnikov rizikov. Trenutno zavarovatelji sklepajo zavarovanja brezpogojno. Učinkovitejši način je zagotavljanje kritja ob izpolnjevanju pogojev, ki se jih preverja s spremljanjem zavarovančevih ranljivosti in izpolnjevanja dogovorjenih zavez. Z upoštevanjem navodil in nasvetov v postopku ocenjevanja in preverjanja izpostavljenosti je omogočena večja cenovna prilagodljivost zavarovalnic in poglobljeno poslovno sodelovanje (PwC, 2015a, str. 12).

Zaradi možnosti padca ugleda podjetja ob razkritju primera kršitve zaupnosti podatkov podjetja ne želijo razkrivati informacij o kibernetskih incidentih. Hkrati zavarovalnice ne želijo deliti svojih informacij in izkušenj zaradi morebitne izgube konkurenčne prednosti pred konkurenti. Vzpostavitev podatkovnih baz o primerih kršitev zaupnosti, na osnovi zakonodaje o varstvu osebnih podatkov v ZDA in EU, lahko pripomore k povečani dostopnosti informacij in boljšemu ovrednotenju tveganj. Običajni 18-mesečni cikel razvoja pogojev zavarovanja se mora spremeniti v dinamično upravljanje z limiti kritja in izpostavljenostmi in v povezavi z izboljšano varnostjo programske opreme. Medtem ko je kibernetski pozavarovalni trg manj razvit kot direktni zavarovalni trg, lahko boljše razumevanje nevarnosti in razvoj modelov za oceno maksimalne izpostavljenosti pripomoreta k dodatnim pozavarovalnim kapacitetam (PwC, 2015a, str. 13).

3.3.2 Vpliv implementacije Splošne uredbe o varstvu podatkov v EU

Z namenom povečanja kibernetske varnosti oblasti v številnih državah zaostrujejo predpise s področja varovanja podatkov. To ima pomemben vpliv na podjetja, ker so kazni iz naslova neupoštevanja predpisov lahko drastično visoke. V ZDA stroga zakonodaja zahteva obvezno obveščanje posameznikov v primeru kršitve zaupnosti podatkov, s katerimi razpolaga podjetje. V zadnjem obdobju se krepi pozornost na odgovornost iz naslova kibernetskih incidentov na Bližnjem Vzhodu, v Singapurju in Avstraliji (Allianz, 2016).

Nezaupanje potrošnikov pri spletnih nakupih in uporabi novih storitev lahko vpliva na razvoj inovativne uporabe novih tehnologij, zato je za zagotovitev gospodarskega razvoja, ki temelji na zaupanju potrošnikov, v okviru Evropske digitalne agende in strategije Evropa 2000 osrednja vloga namenjena varstvu osebnih podatkov. Z namenom razvoja notranjega trga digitalnega gospodarstva ter posodobitve in prenovitve pravil o varstvu podatkov so evropske institucije v letu 2012 pripravile reformo varstva podatkov (Evropska komisija, 2012).

Evropski parlament in Svet EU sta po dolgih usklajevanjih o vsebini reforme 14.4.2016 potrdila zakonodajni sveženj, ki določa nov pravni okvir varstva osebnih podatkov v EU. Uredba Evropskega parlamenta in Sveta EU o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (Splošna uredba o varstvu podatkov), ki bo

stopila v veljavo čez 2 leti po objavi v Uradnem listu EU, nadomešča Direktivo 95/46/ES, iz leta 1995, ko je bila uporaba interneta v začetni fazi. Medtem ko je bil takrat osnovni namen zagotoviti temeljne pravice do varstva podatkov in omogočiti prost pretok osebnih podatkov med državami članicami, je nova regulativa namenjena krepitvi možnosti nadzora posameznika nad njegovimi osebni podatki v digitalnem svetu pametnih telefonov, družbenih medijih, spletnega bančništva in mednarodne trgovine.

Poleg Splošne uredbe o varstvu podatkov je Evropski parlament sprejel tudi Direktivo Evropskega parlamenta in Sveta EU o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov. Direktiva nadomešča Okvirni sklep Sveta o varstvu podatkov (2008/977/PNZ) iz leta 2008.

Ključne spremembe v novi splošni uredbi o varstvu podatkov:

- pravica do pozabe,
- jasnejša in trdnejša definicija posameznikovega soglasja k obdelavi osebnih podatkov,
- zagotovilo, da so pravila zaupnosti podatkov pojasnjena na razumljiv način,
- pravica prenosa osebnih podatkov k drugemu ponudniku storitev,
- pravica do obveščenosti o kršitvi varstva osebnih podatkov,
- pravila obravnave kršitev, ki presegajo meje ene države članice,
- strožji nadzor nad izvajanjem uredbe in uvedba vodilnega nadzornega organa na ravni celotne EU,
- v primeru neupoštevanja pravil so predvidene visoke globe za kršitelje,
- imenovanje odgovorne osebe za varstvo podatkov v javnem sektorju in zasebnih podjetjih.

Splošna uredba o varstvu podatkov ima namen izboljšati varstvo podatkov za posameznike in spodbuditi poslovne priložnosti, skladno z usmeritvijo Evropske komisije za spodbujanje digitalizacije poslovanja, vendar pomenijo zapisana pravila v zakonodajnem okviru varstva podatkov dodatne obveznosti za upravljavce z osebnimi podatki.

Določena je na primer obveznost upravljavcev, da posameznikom zagotavljajo pregledne in lahko dostopne informacije o obdelavi njihovih podatkov. Podrobno so opredeljene tudi splošne obveznosti upravljavcev in oseb, ki osebne podatke obdelujejo v njihovem imenu. Za potencialne kršitelje, podjetja, predstavlja obveznost uradnega obveščanja o kršitvah varstva osebnih podatkov lahko veliko finančno breme. V primeru kršitve varnosti osebnih podatkov, kjer je pričakovana povzročitev velike gospodarske izgube ali družbene škode, mora upravljavec nemudoma obvestiti nadzorni organ in oškodovance. Za hujše kršitve so predvidene globe v višini do 20 milijonov EUR oziroma 4 % svetovnega letnega prometa družbe. Poleg tega bodo morala velika podjetja in podjetja, katerih osrednja dejavnost je

obdelava določenih vrst podatkov, v določenih primerih imenovati odgovorno osebo za varstvo podatkov (Evropski parlament, 2016).

Pričakuje se, da se bo povpraševanje za sklenitev kibernetskega zavarovanja v Evropi znatno povečalo ob uveljavitvi Splošne uredbe o varstvu podatkov v letu 2018, predvsem zaradi obveznosti obveščanja o kršitvah varstva osebnih podatkov, ki za podjetja lahko pomeni veliko finančno breme, in predvidenih globah. Večino ponudnikov kibernetskega zavarovanja zagotavlja kritje tudi za takšne finančne izgube oz. posledice upoštevanja zakonskih obveznosti. Podobne zahteve so v številnih zveznih državah ZDA bistveno povečale stroške postopkov ob kršitvah zaupnosti podatkov (Allianz, 2016).

3.3.3 Management sistemskega tveganja

Kibernetsko zavarovanje je globalna zavarovalna vrsta. Zaradi nefizične narave kibernetskega tveganja so zavarovalnice lahko soočene s škodami s strani velikega števila zavarovancev z različnih koncev sveta zaradi enega samega dogodka. Zaradi tega so zavarovalnice in pozavarovalnice soočene z agregacijo rizikov, ki lahko ob katastrofalnih škodah povzroči nezmožnost izpolnitve pogodbenih obveznosti s strani zavarovalnic (Marsh, 2015, str. 23).

Kljub definiranim limitom kritja, pogojem zavarovanja in izključitvam, ki omejujejo potencialne škode zavarovalnic so nadzorniki zavarovalnih trgov zaskrbljeni zaradi morebitne akumulacije in koncentracije kibernetskih tveganj. Še posebno je bila izpostavljena reakcija nadzornih organov v Veliki Britaniji, kjer deluje največ prevzemnikov rizika za kibernetsko zavarovanje. Novembra 2014 je Lloyd's of London predstavil nove ukrepe za povečanje pregleda nad agregacijo rizikov in postopkov vodenja, s čimer bo zagotovljena možnost ciljnega posredovanja, v kolikor bo potrebno. Glavna skrb je možnost, da kibernetska tveganja niso ustrezno ocenjena s strani prevzemnikov rizika ali da je zaračunana zavarovalna premija prenizka. Izpostavljena je tudi materialna nevarnost akumulacije izpostavljenosti zaradi morebitnega neustreznega nadzora (Lloyd's, 2014).

Zavarovalnice so bile do sedaj soočene le z večjimi posamičnimi zavarovalnimi primeri, povezanimi s kibernetskimi napadi, medtem ko ni bilo nobenih katastrofalnih škodnih dogodkov, povzročenih s strani razširjenih kibernetskih napadov, ki bi večjemu številu podjetij hkrati povzročili resne posledice v poslovanju. Gre za dinamično tveganje, ki se odraža v hitri spremembi tehnoloških aplikacij, ranljivosti programske opreme, priljubljenih metodah napadov storilcev, pravni praksi in odškodninskih primerih ter zasnovi in ponudbi zavarovalnega kritja (Lloyd's, 2015, str. 25).

Zavarovalništvo deluje na osnovi zakona o velikih številih. Z večanjem števila udeležencev oz. zavarovancev se povprečna višina škode približuje pričakovani vrednosti škode (Harrington in Niehaus, 2003, str. 60). Poleg tega zavarovalništvo deluje na osnovi

razpršitve tveganja v prostoru in času. Vendar ravno geografska neomejenost kibernetskih tveganj predstavlja za zavarovalnice največje breme pri kibernetskem zavarovanju. Razširjenost kibernetskih napadov ima lahko za posledico sistemski dogodek, ki naenkrat vpliva na veliko število zavarovancev. Zavarovalnice izpostavljajo zahtevno ocenjevanje največje verjetne škode (angl. *probable maximum loss – PML*) kot ključni razlog za omejeno ponudbo kapacitet kibernetskega zavarovalnega trga (Lloyd's, 2015, str. 25).

Pri modeliranju agregatov premoženjskih rizikov za ocenjevanje izpostavljenosti pred naravnimi nesrečami zavarovalnice in pozavarovalnice uporabljajo uveljavljene modele, ki temeljijo na veliki količini podatkov iz preteklih dogodkov. Zaradi izostanka ustreznih škodnih podatkov se zavarovalnice za oceno možne škodne pogostosti in višine škode pri kibernetskem zavarovanju zanašajo na domneve strokovnjakov. Na osnovi teh obstajajo ocene z velikim razponom v pričakovanih stroških ob najbolj verjetnih scenarijih katastrofalnih škod zaradi (Marsh, 2015, str. 23):

- kršitve varnostne zaščite podatkov največjega ponudnika storitev v oblaku,
- posledic kibernetskega napada na upravljavca električnega omrežja,
- kršitev varnostne zaščite največjega ponudnika procesiranja plačilnih storitev,
- obratovalnega zastoja pri največjem ponudniku gostovanja uporabniških aplikacij v oblaku.

Tabela 12: Primerjava izpostavljenosti kibernetskih zavarovanj z globalnimi zavarovalnimi in pozavarovalnimi kapacitetami za ostale zavarovalne vrste

Globalna izpostavljenost zavarovalne industrije celotni vrednosti kibernetskih rizikov	100 mrd GBP
Največje globalne (po)zavarovalne kapacitete po dogodku za naravne katastrofe (potres v Tokiu ali Kaliforniji)	65 mrd GBP
Največje globalne (po)zavarovalne kapacitete za nuklearno škodo (bolj primerljivo s kibernetskim tveganjem)	3 mrd GBP
Razpon največje možne škode (PML)/celotni količnik izpostavljenosti za premoženjski portfelj	0,15 % (za premoženje v Veliki Britaniji) – 20 % (PML za hurikan za karibski otok z nizko izpostavljenostjo)
PML za kibernetsko zavarovanje (predpostavka enakega PML-ja/celotnega količnika izpostavljenosti za izbrani premoženjski portfelj)	150 mio–20 mrd GBP

Vir: Marsh, UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk. 2015, str. 24, tabela 12.

Alternativni pristop pri oceni sistemske izpostavljenosti je lahko upoštevanje celotne izpostavljenosti in kapacitet zavarovalnic. Po oceni Marsha (2015, str. 23) je v letu 2014 znašala celotna globalna izpostavljenost zavarovalne industrije pred kibernetskimi riziki

(izračunana kot celotni limit kritja za vsa sklenjena samostojna kibernetska zavarovanja) okoli 100 milijard GBP. Podrobnejši prikaz in primerjava je v Tabeli 12.

4 RAZISKAVA MANAGEMENTA KIBERNETSKIH TVEGANJ V SLOVENIJI

V uvodnem delu zastavljeno hipotezo, da v obravnavanih slovenskih podjetjih nimajo ustrezno umeščene funkcije managementa tveganj, sem raziskoval s pomočjo globinskega, delno strukturiranega intervjuja. V raziskavi sem se osredotočil na model managementa kibernetskih tveganj, ki ga imajo izbrana podjetja vzpostavljenega, in njihovo razumevanje vloge zavarovanja kot orodja managementa kibernetskih tveganj. Poleg tega sem želel ugotoviti percepcijo kibernetskih tveganj v podjetjih in njihovo zavedanje o možnosti prenosa dela kibernetskih tveganj na zavarovalnice.

4.1 Kvalitativno raziskovanje

Boyce in Neale (2006) opredelita metodo globinskega intervjuja kot kvalitativno tehniko raziskovanja, ki vključuje izvedbo podrobnega individualnega intervjuja z majhnim številom sodelujočih intervjuvancev, z namenom ugotavljanja njihovih pogledov na določeno idejo, program ali situacijo.

Metodo globinskega, delno strukturiranega intervjuja sem izbral zaradi možnosti pridobitve dodatnih informacij in spoznanj, ki jih je z uporabo drugih raziskovalnih metod težje zagotoviti. Lewis, McNaughton Nicholls, Ormston in Ritchie (2013, str. 56) kot glavno značilnost osebne interakcije, kot je izvedba kvalitativnega intervjuja, izpostavijo poglobljeno osredotočenost na posameznika. Zagotovljena je priložnost za temeljito poizvedbo posameznikovega osebnega pogleda na obravnavani predmet raziskovanja. Je logična izbira načina pridobivanja informacij, kjer se raziskuje občutljive ali večplastne teme ali kjer je pomembna ustrezna umestitev posameznikovih izkušenj.

Z globinskim intervjujem je možno pridobiti tudi zaupne in občutljive informacije, ki jih z drugimi neosebnimi tehnikami ni moč pridobiti. Zaradi osebnega pristopa se lahko pridobi tudi mnenje strokovnjakov oziroma zaposlenih na vodstvenih položajih, ki običajno pri drugih oblikah raziskovanja ne želijo sodelovati. Skozi intervju se sicer osredotoča na osnovno temo razgovora, vendar je glavna kvaliteta globinskega intervjuja raziskovanje skritih pomenov odgovorov (Malhotra & Peterson, 2006, str. 163).

4.1.1 Vzorec in potek raziskave

V raziskavi so sodelovali predstavniki 6 večjih slovenskih podjetij, večinoma zadolženi za management tveganj. Izbrana so bila podjetja iz dejavnosti finančnih institucij in trgovine, ki so po podatkih tuje strokovne literature med najbolj izpostavljenimi dejavnostmi pred kibernetskimi tveganji. Vsa podjetja, vključena v raziskavo, imajo pravnoorganizacijsko obliko delniške družbe in jih skladno z ZGD-1 uvrščamo med velike družbe.

Največji izziv pri izboru primernih kandidatov za intervju je predstavljala splošna percepcija v podjetjih, da je najustreznejši sogovornik za intervju njihov predstavnik oddelka za informatiko, kar je skladno z ugotovitvami raziskave, ki jo je izvedel Advisen (2015, str. 7). Na njihovo vprašanje, kateri oddelek v podjetju je zadolžen za management kibernetskih tveganj, je 79 % sodelujočih v raziskavi izpostavilo oddelek za informatiko.

Kljub temu da se pri kvalitativnem raziskovanju lahko uporabi manjše število neznačilnih primerov (Malhotra & Peterson, 2006, str. 151), vzorec ni bil določen naključno. V izbor podjetij so bila vključena tista, kjer imajo tako kadrovske kot tudi finančne možnosti vzpostavitve managementa kibernetskih tveganj in je izpostavljenost tovrstnim tveganjem nadpovprečna.

Upošteval sem tudi napotek avtoric Boyce in Neale (2006) glede lokacijske in tehnične izvedbe intervjuja. Zaradi delovne in časovne obremenjenosti udeležencev raziskave sem intervjuje opravil v njihovem delovnem okolju z možnostjo zvočnega snemanja razgovora, ob predhodno pridobljenem soglasju intervjuvancev. Domačnost delovnega okolja tudi spodbuja sproščen in prost razgovor o predmetu, kar lahko doprinese tudi k pridobitvi presenetljivih informacij.

Tabela 13: Značilnost vzorca raziskave

Udeleženec	**Dejavnost podjetja**	**Naziv področja zaposlitve**	**Datum intervjuja**
Udeleženec A	Bančništvo	Direktor službe skladnosti poslovanja	20. 5. 2016
Udeleženec B	Zavarovalništvo	Direktor upravljanja s tveganji	1. 6. 2016
Udeleženec C	Bančništvo	Direktor sektorja IT	9. 6. 2016
Udeleženec D	Bančništvo	Direktor službe upravljanja s tveganji	10. 6. 2016
Udeleženec E	Trgovina	Vodja IT in vodja upravljanja s tveganji	14 .6. 2016
Udeleženec F	Trgovina	Vodja zakladništva	17. 6. 2016

Namen predhodno pripravljenega nabora vprašanj v obliki opomnika je, da se udeleženci raziskave s svojimi odgovori oz. razmišljanjem ne oddaljijo od začrtanih ciljev raziskave, poleg tega je bila tudi lažja analiza in primerjava rezultatov intervjujev. S tem sem zagotovil vsebinsko primerljive informacije, pridobljene od udeležencev intervjuja. Vsebina opomnika je bila delno strukturirana skladno s temami predhodnih poglavij

magistrskega dela in v pretežnem delu uporabljena v vseh intervjujih. Vseeno se je vrstni red vprašanj prilagajal glede na potek razgovora in posebnosti posameznega udeleženca oziroma podjetja. Vprašanja intervjuvancem niso bila vnaprej posredovana.

Z namenom zaščite udeležencev raziskave sem jim pred začetkom intervjuja izročil podpisano izjavo o zaupnosti razgovora in zavezo o varovanju poslovnih informacij.

4.1.2 Omejitve in determiniranost okolja

Glede na to, da so bili intervjuvanci pretežno managerji s področja managementa tveganj, je potrebno upoštevati nevarnost nagnjenosti k pristranskosti. Boyce in Neale (2006) opozarjata na možnost dokazovanja uspešnosti in ustreznosti delovanja posameznikov, ki so znotraj podjetij odgovorni za predmetno področje raziskave.

V analizo pridobljenih informacij sem vključil tudi podatke iz kvantitativne raziskave, ki jo je z evropskimi predstavniki podjetij, večinoma zadolženimi za management tveganj, opravil Advisen (2015). Včasih se opravi kvalitativno raziskavo kot dopolnitev ugotovitev na podlagi druge kvantitativne raziskave, pri čemer je potrebno biti previden, da se ugotovitve kvalitativne raziskave ne smatra kot dokončne in osnovo za posplošitev na izbrano ciljno skupino (Malhotra & Peterson, 2006, str. 151).

Pri presoji rezultatov raziskave je potrebno upoštevati tudi okolje za uvedbo prenosa kibernetskih tveganj na zavarovalni trg, predvsem z vidika razvitosti slovenskega zavarovalništva. Poleg tega je za razumevanje stanja managementa tveganj v slovenskih podjetij pomembno poznavanje veljavnega zakonodajnega okvira, ki opredeljuje obveznosti podjetij glede managementa tveganj. Zakon o bančništvu (Ur.l. RS, št. 25/2015, v nadaljevanju ZBan-2) in Zakon o zavarovalništvu (Ur.l. RS, št. 93/2015, v nadaljevanju ZZavar-1) kot krovna zakona dejavnosti bančništva in zavarovalništva opredeljujeta dolžnost upravljanja s tveganji kot tudi varovanja in uporabo zaupnih podatkov oziroma informacij. Predvidene so tudi globe zaradi kršitev v zvezi z varovanjem zaupnih podatkov. V ZZavar-1 je definiran tudi sistem upravljanja zavarovalnice, vključno s funkcijo upravljanja tveganj, strategijo, pisnimi pravili, procesi in postopki tveganj, medtem ko ZZban-2 zavezuje banke k ureditvi procesov upravljanja tveganj in dolžnostjo organiziranja funkcije upravljanja tveganj kot tudi k določanju strategije in politike upravljanja tveganj. Med drugim je opredeljeno tudi upravljanje operativnih tveganj banke.

Splošni zakonski okvir glede managementa tveganj je zapisan v ZGD-1, ki zavezuje podjetja k opisu bistvenih tveganj v poslovnem poročilu podjetja. V kolikor je pomembno za presojo premoženja in obveznosti družbe, morajo biti v poročilu zapisani tudi cilji in ukrepi upravljanja tveganj.

V Sloveniji Zakon o varstvu osebnih podatkov (Ur.l. RS, št. 86/2004) upravljavcem osebnih podatkov nalaga dolžnost zagotavljanja varstva osebnih podatkov na natančno

predpisan način z vsemi tehničnimi in organizacijskimi sredstvi. Zakon med drugim določa tudi globe v primeru kršitev določb o varovanju osebnih podatkov, ki pa ne presegajo 12.510 EUR za pravno osebo in 2.080 EUR za odgovorno osebo.

Na slovenskem zavarovalnem trgu je za zbiranje informacij o obsegu sklenjenih zavarovanj zadolženo Slovensko zavarovalno združenje, ki pa v svoji letni publikaciji, Statistični zavarovalniški bilten (SZZ, 2015) za zdaj ne vključuje informacije o kibernetskih zavarovanjih. Glede na to, da je kibernetsko zavarovanje primarno opredeljeno kot odgovornostno zavarovanje, in ko pogledamo strukturo sklenjenih zavarovanj pri slovenskih zavarovalnicah, se ob podatku, da odgovornostna zavarovanja predstavljajo zgolj 4,4-odstotni delež v zavarovalnem portfelju premoženjskih zavarovanj postavlja vprašanje, ali se slovenska podjetja zavedajo pomena odgovornostnih zavarovanj, ter znotraj njih kibernetskega zavarovanja. Sploh glede na primerljivi podatek za evropske zavarovalnice, kjer odgovornostna zavarovanja predstavljajo 7 % vseh premoženjskih zavarovanj (Insurance Europe, 2015, str. 14).

Glede na to, da nobena od zavarovalnic, ki imajo sedež družbe ali podružnice v Sloveniji, trenutno ne ponuja lastnega kibernetskega zavarovanja, lahko sklepamo, da je obseg zavarovanj sklenjenih pri slovenskih zavarovalnicah, relativno majhen. Slovenska podjetja imajo sicer možnost sklenitve kibernetskega zavarovanja pri kateri koli evropski zavarovalnici, ki ima pri slovenski Agenciji za zavarovalni nadzor priglašeno neposredno opravljanje zavarovalnih poslov. Kljub temu na podlagi poznavanja slovenskega zavarovalnega trga ocenjujem, da skupna letna premija iz naslova kibernetskih zavarovanj ne presega 1 mio EUR, kar je manj kot 0,05 % celotne zavarovalne premije, ki jo zberejo zavarovalnice v Sloveniji.

V okvir primerjave razvitosti slovenskega trga kibernetskih zavarovanj proti evropskemu je smiselno vključiti tudi podatek o deležu zavarovalno posredniških družb med vsemi prodajnimi potmi. Glede na že prej omenjeni razlog za nesklenitev kibernetskega zavarovanja, t. j. pomanjkljive informacije o zavarovalnem produktu in znanje s strani zavarovalnih posrednikov (Advisen, 2014a, str. 6), velja izpostaviti podatek o deležu zavarovalnih posrednikov med vsemi prodajnimi potmi. Osnovno poslanstvo zavarovalnega posrednika je namreč neodvisno svetovanje o možnostih zavarovanja tveganj zavarovanca na zavarovalnem trgu. V Sloveniji je delež zavarovalnih posrednikov med vsemi prodajnimi potmi premoženjskih zavarovanj, kamor sodi tudi kibernetsko zavarovanje, v letu 2012 znašal 5,5 % in je tretji najnižji med vsemi članicami evropskega zavarovalnega in pozavarovalnega združenja Insurance Europe. Najvišji delež imajo zavarovalni posredniki v Veliki Britaniji (55,2 %) in v Belgiji (61,4 %), medtem ko imajo v Avstriji 33-odstotni delež (Insurance Europe, 2015, str. 65).

4.2 Rezultati raziskave

Rezultati raziskave so predstavljeni v dveh delih. Najprej je podana analiza globinskih intervjujev po tematsko zaokroženih sklopih, kjer je povzeta vsebina odgovorov intervjuvancev. V drugem delu so predstavljene ugotovitve in domneve, ki temeljijo na analizi intervjujev, in primerjave z informacijami iz teoretičnega dela magistrskega dela in drugimi relevantnimi raziskavami.

4.2.1 Analiza globinskih intervjujev

Analiza globinskih intervjujev je narejena po vsebinsko zaokroženih sklopih vprašanj iz opomnika (Priloga 2). Po opravljenem intervjuju, ki je bil posnet z uporabo diktafona, so bili odgovori udeležencev intervjuja prepisani in nato povzeti po vsebinskih sklopih iz opomnika. Pri tem sem z navzkrižno analizo poskušal povezati odgovore vseh udeležencev na ista vprašanja v sklope vprašanj. Pozornost je bila usmerjena v iskanje vsebinskih povezav in podobnih vzorcev odgovorov v povzetkih intervjujev. V nadaljevanju je podana analiza odgovorov po posameznem sklopu.

Pridobil sem informacije za razumevanje umeščenosti funkcije managementa kibernetskih tveganj v podjetjih, zavedanja in aktivnosti v vezi evropske Splošne uredbe o varstvu podatkov, percepcije izpostavljenosti pred kibernetskimi tveganji, managementa tveganj kršitve zaupnosti podatkov in njihovega zavedanja o možnosti prenosa kibernetskih tveganj na zavarovalnice.

Model managementa tveganj. Udeleženci so imeli pri tem sklopu vprašanj največ težav z razumevanjem vsebine vprašanja. Zaradi teoretičnega izhodišča samega vprašanja in lažjega razumevanja sem jim podal dodatno opredelitev uvodnih pojmov. Udeleženci intervjuja izpostavljajo, da mednarodnega standarda managementa tveganj nimajo, vendar so zaradi regulatornih zahtev vzpostavili model managementa tveganj, ki je vsebinsko primerljiv s standardi v njihovi dejavnosti in zadosti zakonskim zahtevam glede managementa tveganj. Skupna značilnost je, da imajo vzpostavljen lastni model managementa tveganj, ki povzema izkušnje ali smernice mednarodnih standardov in dobre prakse, kar najbolje povzame komentar udeleženca B: »Nimamo vzpostavljenega mednarodnega standarda. Imamo lasten sistem, hibrid modelov standardov in dobre prakse.« V bankah imajo vzpostavljen splošni model tveganj, ki opredeljuje postopek identifikacije, analize, ovrednotenja in obdelave tveganj. Model je aplikativen tudi za kibernetska tveganja. V obeh trgovskih podjetjih so trenutno v postopku prenove managementa tveganj. Do zdaj je bila pri njih osredotočenost usmerjena na kreditna tveganja.

Zaradi zakonske zahteve imajo v bankah in zavarovalnicah umeščeno samostojno funkcijo vodje managementa s tveganji, ki je neposredno odgovoren upravi. Iz izjave udeleženca B je razvidno, da je zakonodaja glavni razlog za formaliziran model managementa tveganj:

»Zaradi Solventnosti II imamo sprejeto politiko managementa tveganj in pripravljene krovne dokumente.« Podobno lahko razberemo iz komentarja udeleženca D: »V bančništvu je zakonodaja tista, ki opredeljuje področje managementa tveganj. Zakon o bančništvu in evropski predpisi s strani EBA – Evropskega bančnega združenja za evro in Evropske centralne banke.«

Kibernetska tveganja smatrajo v vseh podjetjih kot operativna tveganja. Enotno je tudi stališče, da se uprava podjetja zaveda kibernetskega tveganja. Udeleženci B, C, D in E imajo vzpostavljene odbore za management tveganj, v katere so vključeni tudi člani uprave. Uprave tudi podpirajo investicije v opremo za preprečevanje in odpravljanje kibernetskih tveganj. V večini podjetij je oddelek za informatiko zadolžen za management kibernetskih tveganj, ali vsaj vključen. Intervjuvanec D je tezo podkrepil z besedami: »Splošna percepcija je, da so kibernetska tveganja del IT-oddelka.« Tudi pri drugih podjetjih na podlagi njihovih izjav prevladuje podoben občutek.

V podjetjih imajo vzpostavljen sistem rednega izobraževanja zaposlenih o informacijski varnosti. V podjetju A in C so izpostavili, da ob informacijsko-varnostnih incidentih zaposlene osveščajo o tveganjih. Iz izjave udeleženca C je očitno, da zaposlene obveščajo o aktualnih tveganjih: »Prejšnji teden je bilo aktualno ozaveščanje zaposlenih o kripto virusih.« V vseh podjetjih imajo dokumentirane tudi pravilnike za uporabo elektronskih naprav in družabnih omrežij.

Vpliv evropske Splošne uredbe o varstvu podatkov. Večina intervjuvancev je le okvirno seznanjena z vsebino uredbe. V postopku priprave na zagotavljanje skladnosti poslovanja z zahtevami uredbe so v fazi preučevanja in internega seznanjanja z vsebino uredbe. Na vprašanje o oceni poglavitnih novostih v primerjavi z obstoječo uredbo sta predstavnika podjetij, kjer so bolje seznanjeni z vsebino uredbe, izpostavila predvidene visoke kazni za kršitelje. Iz opravljenih pogovorov ugotavljam, da je za implementacijo uredbe v večini podjetij zadolžen pravni oddelek.

Upoštevanje obveznosti iz naslova varovanja osebnih podatkov, na podlagi veljavne bančne zakonodaje, sta izpostavila dva udeleženca iz dejavnosti bančništva. Intervjuvanec A je izpostavil: »Z uredbo nisem natančno seznanjen. Vseeno že danes zaradi obvez iz zakonodaje ustrezno upravljamo s tovrstnimi tveganji. To je bančni standard.« Podoben komentar je podal tudi intervjuvanec D: »Z uredbo nismo seznanjeni. Banka mora pri kršitvah kreditnih kartic že zaradi zakonodaje imeti urejeno obveščanje komitentov.«

Intervjuvanci so v pogovoru o prenosu pogodbene odgovornosti za zagotavljanje varovanja osebnih podatkov poudarili, da od svojih pogodbenih partnerjev zahtevajo upoštevanje enakih zakonskih zahtev kot veljajo za njih.

Na koncu je bila udeležencem podana kratka informacija o ključnih spremembah, ki jih prinaša nova uredba. Prevladuje občutek, da z vidika managmenta kibernetskih tveganj večina smatra predvidene globe kot največjo izpostavljenost.

Izpostavljenost kibernetskim tveganjem. V vseh podjetjih, vključenih v raziskavo, so že imeli izkušnjo s kibernetskim incidentom, vendar finančnih posledic niso utrpeli. Predvsem je šlo za poskuse kibernetskih napadov, ki pa so bili zaradi dobre tehnološke opremljenosti v podjetjih neuspešni. Komentar udeleženca E povzema stanje na področju izpostavljenosti kibernetskim tveganjem v podjetjih: »Dnevno se dogajajo poskusi napadov. Tehnično smo dobro opremljeni in spremljamo dogajanje.« Nihče od intervjuvancev tudi nima izkušnje s poskusom kibernetskega izsiljevanja (angl. *cyber extortion*) podjetja, razen pri udeležencu E, kjer so bili obveščeni o primeru izsiljevalskega programja pri uporabniku (angl. *ransomware*).

V bankah so večkrat na leto soočeni s prevarami v obliki t. i. "skimminga" na bankomatih. Največ kršitev zaznavajo pri njihovih komitentih ob uporabi spletnega bančništva. Pri tem so predstavniki bank izpostavili, da kibernetski incidenti nastanejo predvsem zaradi nevestnega ravnanja uporabnikov njihovih bančnih storitev. Udeleženec D je njihove izkušnje podkrepil z izjavo: »Pri komitentih je bilo nekaj vdorov pri spletnem bančništvu in odtujitev denarja z računa zaradi njihove neprevidnosti.« Pri enem izmed trgovcev so prav tako imeli primer skimminga, vendar na POS-terminalih v trgovini. Njihovi kupci so utrpeli škodo zaradi dvigov gotovine v tujini z njihovih kartic. Ob tej informaciji je bil podan komentar: »Tega tveganja se najbolj bojimo zaradi pogodbenih sankcij s strani bank.« V dveh bankah so omenili tudi primere onemogočanja izvajanja spletnih storitev banke, ki so bili posledica kibernetskega napada z uporabo metode porazdeljene ohromitve storitve. Pri preprečitvi napada oziroma odpravi posledic napada so aktivno sodelovali z Nacionalnim odzivnim centrom za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij (SI-CERT).

Za preverjanje notranjih sistemov in z namenom preprečevanja kibernetskih napadov v vseh podjetjih izvajajo t. i. penetracijske teste. V ta namen najamejo zunanje izvajalce, ki poskušajo s poskusom vdora v informacijsko omrežje identificirati šibke točke, ki jih je potrebno odpraviti. Izjema je le trgovsko podjetje, kjer zaradi postopka finančnega prestrukturiranja podjetja za ta namen trenutno nimajo razpoložljivih sredstev.

V nadaljevanju so povzeti odgovori na vprašanje o največjih tveganjih, ki so jim v podjetju izpostavljeni. Za lažjo primerjavo med odgovori in v pomoč intervjuvancev so jim bili predstavljeni možni kibernetski dogodki oziroma tveganja, ki so jih morali ovrednotiti s pomočjo lestvice od 1 do 5, pri čemer (1) predstavlja zelo nizko tveganje in (5) zelo visoko tveganje za podjetje. Hkrati so na enak način ovrednotili možne posledice kibernetskega dogodka.

Udeleženec A: Največje tveganje predstavlja (5) kršitev zaupnosti njihovih strank, porazdeljena ohromitev storitve in škodljiva programska oprema. Pri posledicah dogodka pa jih najbolj skrbi padec ugleda zaradi kršitve zaupnosti podatkov na splošno kot tudi preko družbenih omrežij.

Udeleženec B: Največje tveganje predstavlja (5) kršitev zaupnosti njihovih strank in (4) škodljiva programska oprema. Pri posledicah dogodka jih najbolj skrbi (5) obratovalni zastoj zaradi prekinitve poslovanja, posledica zaustavitve plačilnega prometa.

Udeleženec C: Največje tveganje predstavlja (5) kršitev zaupnosti podatkov bančnih komitentov zaradi ugleda banke. Pri posledicah je največji problem (5) obratovalni zastoj zaradi prekinitve poslovanja banke. Družbena omrežja so z vidika posledic problematična, zato so se zavestno odpovedali uporabi družbenih omrežij za trženjske namene.

Udeleženec D: Največje tveganje predstavlja (5) škodljiva programska oprema v sistemu banke in kršitev zaupnosti podatkov zaradi uporabe osebnih pripomočkov za službene namene, vendar imajo vzpostavljene omejitve uporabe (pravilniki). Pri posledicah dogodka jih najbolj skrbi (5) obratovalni zastoj zaradi prekinitve poslovanja in zaradi dobavitelja telekomunikacijskih storitev.

Udeleženec E: Največje tveganje predstavlja (5) kršitev zaupnosti podatkov strank, sledita porazdeljena ohromitev storitve in škodljiva programska oprema. Pri posledicah je tveganje največje (5) pri padcu ugleda zaradi kršitve zaupnosti podatkov in obratovalni zastoj zaradi kibernetskega napada pri dobavitelju električne energije.

Udeleženec F: Največje tveganje predstavljata (4) porazdeljena ohromitev storitve in škodljiva programska oprema v njihovem omrežju. Pri posledicah je tveganje največje (4) pri obratovalnem zastoju zaradi prekinitve poslovanja in napada pri dobavitelju. Težave bi imeli tudi ob povečanih stroških zaradi kibernetskega napada.

Z vidika ocene izpostavljenosti kibernetskim tveganjem je zanimiva izjava udeleženca F: »Vsi deležniki se ne zavedajo dovolj kibernetskih tveganj. Trenutno se s tem področjem ukvarja samo IT- in pravni oddelek.« O percepciji izpostavljenosti kibernetskim tveganjem je še bolj neposreden komentar udeleženca B: »Kibernetska tveganja niso upoštevana kot največja tveganja. V Sloveniji ni dogodkov s tega področja. Ob prvem dogodku, ki se bo zgodil, in samo vprašanje časa je kdaj se bo zgodil, se bo percepcija spremenila.«

Ob ovrednotenju kibernetskih tveganj se je izkazalo, da imajo vsa podjetja v veljavi pravilnike o uporabi osebnih pripomočkov zaposlenih za službene namene ali uporabi službenih računalnikov ali drugih naprav za privatne namene. Posebej so izpostavili omejitve uporabe interneta (onemogočen dostop do določenih spletnih strani), privatne spletne pošte in družbenih omrežij. Pri družbenih omrežjih je bila največkrat izpostavljena

prepoved uporabe ali vsaj zelo omejena možnost uporabe. Udeleženec E je izpostavil: »Uporaba družbenih omrežij je zelo omejena, na 15 minut dnevno.«

Management tveganja kršitve zaupnosti podatkov. V podjetjih imajo različno organizacijsko umeščen management kršitve zaupnosti podatkov. Samostojna funkcija direktorja ali vodje za varstvo podatkov (angl. *Chief Privacy Officer*) obstaja samo v enem podjetju. V ostalih podjetjih so za varstvo zaupnosti podatkov zadolženi različni oddelki ali službe, in sicer:

- oddelek pravne podpore,
- služba za zagotavljanje skladnosti delovanja oz. poslovanja,
- vodja informacijske zaščite.

V primeru kršitve zaupnosti podatkov morajo v podjetjih slediti postopkom, ki so zapisani v internih dokumentih. V podjetju udeleženca E imajo izdelan dokument za splošni odziv na varnostne incidente, v podjetjih iz dejavnosti bančništva in zavarovalništva (udeleženci A, B, C in D) pa so postopki zapisani v okviru načrta za neprekinjeno poslovanje. Udeleženec D je sicer podal še dodatno pojasnilo: »V banki obstajajo politike in načrti v primeru kršitve zaupnosti podatkov.« Medtem ko v podjetju udeleženca F nimajo sistemskega dokumenta, ki bi predvidel postopke ukrepanja v primeru kibernetskega napada ali kršitve zaupnosti podatkov. Imajo pa dokumentiran postopek varovanja osebnih podatkov, katerega skrbnik je pravna služba.

Ključno vlogo v primeru kršitve zaupnosti podatkov imajo v podjetju sledeči oddelki oziroma področja:

Udeleženec A: služba skladnosti poslovanja in notranja revizija
Udeleženec B: oddelek pravne podpore
Udeleženec C: varnostni inženir in krizni štab (IT-oddelek, sektor upravljanja s tveganji, uprava, PR-služba)
Udeleženec D: direktor za varstvo podatkov in IT-oddelek
Udeleženec E: IT-oddelek, PR služba, pravno področje in vodja za varstvo podatkov
Udeleženec F: pravna služba in oddelek informatike

Pomembnost zavedanja in managementa tveganja kršitve zaupnosti podatkov je posebej izpostavil udeleženec B: »Zbiramo veliko količino osebnih podatkov. Če nam ukradejo baze podatkov, ima to lahko za nas finančne posledice in vpliv na naš ugled, zato tveganja obvladujemo.«

Kibernetsko zavarovanje kot orodje managementa tveganj. V nobenem podjetju, vključenem v raziskavo, trenutno nimajo sklenjenega kibernetskega zavarovanja, prav tako še niso začeli s postopkom pridobivanja ponudb za sklenitev zavarovanja. Udeleženec C je bil celo presenečen nad možnostjo zavarovanja kibernetskih tveganj: »Nisem še razmišljal, da se sploh lahko zavaruješ za tovrstne rizike.« Podobno je izjavil tudi udeleženec D: »Prvič slišim, da takšno zavarovanje obstaja.«

Na večino predvidenih vprašanj iz tega sklopa udeleženci zaradi nepoznavanja značilnosti kibernetskega zavarovanja niso mogli podati komentarja, vključno z osnovnim stališčem intervjuvancev o kibernetskem zavarovanju kot orodju managementa tveganj. Z namenom pridobitve stališča intervjuvancev na predvidena vprašanja sem jim podal pojasnilo o osnovnih funkcijah kibernetskega zavarovanja. Na tej osnovi je večina mnenja, da kibernetsko tveganje sicer obstaja, vendar ob majhni verjetnosti manifestacije dogodka. Udeleženca A in B sta se podobno izrazila: »Sicer je tveganje prisotno, vendar sta verjetnost in število dogodkov majhna.« Večina udeležencev je največ zanimanja za kibernetsko zavarovanje izrazila ob omembi možnosti zavarovanja glob zaradi kršitev evropske Splošne uredbe o varstvu podatkov.

V polovici primerov je bila kot glavni razlog za neobstoj kibernetskega zavarovanja izpostavljena nerazvitost lokalnega zavarovalnega trga: »Lokalni zavarovalni trg kibernetskega zavarovanja ne ponuja.«

Pri ugotavljanju percepcije vloge zavarovanja v okviru managementa tveganj je, ob poznavanju zavarovalne kulture v Sloveniji, večina presenetljivo poudarila podobno, kot je izjavil udeleženec B: »Zavarovanje prepoznavamo kot orodje za nadomestitev katastrofalne škode«.

4.2.2 Ugotovitve in oblikovanje domnev

Za predmetno raziskavo managementa kibernetskih tveganj se je izbrana raziskovalna tehnika izkazala za učinkovito, saj so udeleženci intervjuja razkrili ozadje organizacijske umeščenosti managementa tveganj. Hkrati so bile pridobljene tudi občutljive informacije o njihovi informacijski varnosti in izkušnjah s kibernetskimi varnostnimi incidenti. Podjetja običajno zaradi možnih negativnih posledic na ugled podjetja ne želijo javno razkrivati takšnih informacij.

Za lažji vpogled v ugotovitve in domneve so v Tabelah 14 in 15 izpostavljeni bistveni citati iz odgovorov udeležencev intervjuja. Ob primerjavi s teoretičnim delom managementa kibernetskih tveganj, primeri iz prakse in drugimi raziskavami s področja managementa kibernetskih tveganj so na koncu ugotovitev iz naslova posameznega sklopa vprašanj zapisane domneve.

Model managementa tveganj. Na podlagi odgovorov sodelujočih v raziskavi se v uvodu zastavljena hipoteza, da v obravnavanih slovenskih podjetjih nimajo ustrezno umeščene funkcije managementa tveganj, lahko ovrže. Kljub temu, da imajo v večini podjetij, vključenih v raziskavo, oblikovano neodvisno in upravi neposredno odgovorno funkcijo managementa tveganj, iz pojasnil intervjuvancev izhaja, da je zakonska obveza glavni razlog za njeno vzpostavitev. Podobno ugotovitev lahko zapišem za model managementa tveganj, ki je v podjetjih iz dejavnosti bančništva in zavarovalništva vzpostavljen zaradi zakonske dolžnosti upravljanja s tveganji kot tudi varovanja in uporabo zaupnih podatkov.

Zdi se, da glavni motiv ni ustrezna umeščenost managementa kibernetskih tveganj, kot bi pričakovali na podlagi raziskave percepcije največjih tveganj v podjetjih (Allianz, 2016; World Economic Forum, 2016), temveč izogibanje sankcijam ob neupoštevanju zakonskih določil, kjer so predvidene tudi visoke kazni za kršitelje. V drugih državah se kibernetsko tveganje v zadnjih letih namreč strmo dviga po lestvici največjih poslovnih tveganj. Ocenjujem, da v okviru veljavnih modelov managementa tveganj, v nasprotju s predvidenim modelom Gordon et al. (2013), podjetja za kibernetska tveganja nimajo vzpostavljenega postopka za preverjanje možnosti prenosa tveganj na zavarovalnico.

V večini primerov je IT oddelek zadolžen ali vsaj vključen v management kibernetskih tveganj. Splošna percepcija, da je za management kibernetskih tveganj najprimernejši IT-oddelek, se je pokazala že pri organizaciji intervjujev, saj so v večini podjetij predlagali, da se v raziskavo vključi njihov predstavnik IT-oddelka. Pri večini tistih, ki niso bili predstavniki IT-oddelkov, pa je bilo zaznati opazno slabše poznavanje vsebine kibernetskih tveganj. Pomanjkanje razumevanja kompleksnosti kibernetskega tveganja je v raziskavi, ki jo je izvedel Allianz (2016, str. 10), izpostavljeno kot glavna ovira za boljšo pripravljenost podjetij pred kibernetskimi nevarnostmi. Ugotavljam, da je splošna raven razumevanja kibernetskih tveganj in njihovih posledic v podjetjih nizka, zaznavanje, da so kibernetska tveganja del IT-oddelka, pa napačna. Evropska podjetja, ki so bila vključena v raziskavo Advisen (2015), se v večini primerov (45 %) odločajo za pristop, kjer je v management kibernetskih tveganj vključenih več različnih oddelkov podjetja. Kljub temu je tudi v teh podjetjih IT-oddelek z najvišjim odstotkom (78,6 %) zaznan kot prva obrambna linija za preprečitev izgube informacij in drugih kibernetskih tveganj.

Med preventivnimi ukrepi, ki skladno s študijo Ponemon (2015b) in priporočili Giblina (2015) zmanjšujejo možnost kibernetskega napada in znižujejo stroške kršitev zaupnosti podatkov v primeru varnostnega incidenta, sodi tudi izobraževanje zaposlenih o varnostni politiki in kibernetskih tveganjih. Na osnovi analize intervjujev lahko ugotovimo, da imajo podjetja vzpostavljen ustrezen sistem izobraževanja o kibernetskih tveganjih.

Domneva: Funkcija managementa tveganj je v podjetjih ustrezno umeščena in model managementa tveganj vzpostavljen, vendar sta v osnovi pogojena z zakonskimi zahtevami, in ne odraz poznavanja aktualnih ključnih poslovnih tveganj. Enako velja za management kibernetskih tveganj.

Tabela 14: Predstavitev citatov globinskih intervjujev za posamezne sklope

Model managementa tveganj	**Vpliv evropske Splošne uredbe o varstvu podatkov**	**Izpostavljenost kibernetskim tveganjem**
»Kibernetska tveganja so domena oddelka za skladnost poslovanja, nekoč so bila del IT-oddelka.« »Redno izvajamo izobraževanja, še posebej ob incidentih.« (udeleženec A)	»Nisem natančno seznanjen. Vseeno že danes zaradi zavez iz zakonodaje ustrezno upravljamo s tovrstnimi tveganji. To je bančni standard.« (udeleženec A)	»Kibernetske napade smo zaznali v obliki skimminga. Nekaj primerov na leto. Banka ni bila oškodovana. Škodo so v nekaterih drugih primerih utrpeli posamezniki, zaradi nevestnosti.« (udeleženec A)
»Zaradi Solventnosti II imamo sprejeto politiko managementa tveganj.« »IT-oddelek je skrbnik kibernetskih tveganj, ker tveganja nastajajo na njihovem področju.« (udeleženec B)	»Smo bili seznanjeni, vemo kakšne so spremembe in kakšne so posledice kršitev uredbe. Izpostavljene so bile visoke kazni.« (udeleženec B)	»Sicer je tveganje prisotno, vendar je verjetnost nizka in število dogodkov do zdaj majhno. Ob prvem odmevnem dogodku, ki se bo zgodil, se bo percepcija spremenila. Je samo vprašanje časa.« (udeleženec B)
»Uprava podpira projekte IT-varnosti, vendar so odločitve racionalne. Absolutne varnosti ni.« »Zaposlene osveščamo kako ravnati v primerih hekerskih vdorov.« (udeleženec C)	»Smo okvirno seznanjeni.« (udeleženec C)	»Ko so nas pred dvema letoma napadli Anonymusi, so nas napadli z DDOS. Aktivno smo spremljali in preprečevali napade ter sodelovali s SI-CERT.« (udeleženec C)
»V bančništvu je zakonodaja tista, ki opredeljuje področje managementa tveganj.« »Splošna percepcija je, da so kibernetska tveganja del IT-oddelka.« (udeleženec D)	»Z uredbo nismo seznanjeni. Banka mora imeti pri kršitvah kreditnih kartic že zaradi zakonodaje urejeno obveščanje komitentov.« (udeleženec D)	»Večkrat smo že imeli primere kršitev. Največ je bilo napadov na bankomate – skimming.« »V banki imamo dobre zaščite.« »Pri komitentih je bilo nekaj vdorov pri spletnem bančništvu, zaradi njihove neprevidnosti.« (udeleženec D)
»Kibernetska tveganja se tudi pri nas prelaga na IT-oddelek.« »Za tiste, ki imajo opravka s kreditnimi karticami, so še dodatna izobraževanja.« (udeleženec E)	»Smo seznanjeni z uredbo. Pravni oddelek nas je obvestil. Izpostavili so predvidene visoke kazni.« (udeleženec E)	»Dnevno se dogajajo poskusi. Tehnično smo dobro opremljeni in spremljamo dogajanje.« (udeleženec E)
»Največ se posvečamo upoštevanju zakonskih zahtev.« »Trenutno je za kibernetska tveganja zadolženo področje IT-ja.« (udeleženec F)	»Z uredbo smo na splošno seznanjeni, vendar je natančno še nismo preučili.« (udeleženec F)	»Imeli pa smo primer skimminga na POS-terminalih v trgovini. « »Vsi deležniki se ne zavedajo dovolj kibernetskih tveganj.« »Ocenjujem, da je pri kibernetskem tveganju najbolj izpostavljen ugled družbe.« (udeleženec F)

Vpliv evropske Splošne uredbe o varstvu podatkov. Glede na to, da je bila nova evropska Splošna uredba o varstvu podatkov sprejeta aprila 2016 in bo stopila v veljavo čez dve leti, ni presenetljivo, da v večini podjetij še niso v popolnosti seznanjeni z vsebino uredbe.

V bankah so mnenja, da imajo že danes ustrezno urejeno področje varovanja osebnih podatkov. Kljub temu velja izpostaviti strah pred visokimi kaznimi, ki so predvidene s spremembo uredbe. Če upoštevamo še stroške zaradi obveznega obveščanja o kršitvah zaupnosti podatkov in izraženo zanimanje udeležencev za možnost zavarovanja plačila glob, lahko pričakujemo povečano zanimanje za sklenitev kibernetskega zavarovanja.

Pričakujemo lahko, da se bo povpraševanje za sklenitev kibernetskega zavarovanja tudi v Sloveniji znatno povečalo šele ob uveljavitvi Splošne uredbe o varstvu podatkov v letu 2018.

Domneva: Zaradi obstoječih veljavnih zakonskih obveznosti imajo v podjetjih že danes vzpostavljen ustrezen management tveganj v primeru kršitve zaupnosti podatkov. Zaradi z uredbo predvidenih visokih kaznih se bo zanimanje za sklenitev kibernetskega zavarovanja povečalo.

Izpostavljenost kibernetskim tveganjem. Nihče od intervjuvancev kibernetskih tveganj ni označil kot nepomembnih. Hkrati prevladuje prepričanje o dobri tehnološki zaščiti pred napadalci in nizkem tveganju. Občutek varnosti temelji na dejstvu, da do sedaj niso utrpeli finančnih posledic ob varnostnih incidentih. Pri tem je zanemarjeno, da je večina kibernetskih incidentov posledica zlonamernega delovanja ali nepazljivosti zaposlenih v podjetju (IBM, 2016), in ne delovanja zunanjih hekerjev, kot bi lahko napačno sklepali na podlagi pogostega medijskega poročanja o napadih zlonamernih hekerjev iz tujine.

Izraženo razmišljanje o managementu kibernetskih rizikov (udeleženca D in E) se kljub nadpovprečnim investicijam v preprečevanje dogodkov zdi naivno. Primeri iz prakse kažejo, da so predmet kibernetskega napada lahko tudi poslovno uspešna in finančno trdna podjetja, ki imajo sicer vzpostavljene ustrezne sisteme managementa tveganj. Ali kot se je izrazil udeleženec C: »Absolutne varnosti ni.«

Občutek udeležencev, da je Slovenija premajhna za izrazito zanimanje hekerjev je zavajajoč. Po mnenju McAfee (2014) kibernetski kriminal ob majhnem tveganju in nizkih stroških ustvarja visoke donose. Zato geografskih omejitev ob uporabi sodobnih tehnologij ni. V primeru nezadostnega zavedanja o možni višini škode ali podcenjevanju ranljivosti so tveganja v podjetjih lahko podcenjena.

Zanimiva je trditev enega od intervjuvancev, da v Sloveniji ni tovrstnih dogodkov. V raziskavi Ponemon (2015a, str. 9) je naveden podatek, da je ena tretjina podjetij, ki so utrpela kršitev zaupnosti podatkov zaradi hekerskega napada, odkrila kršitev šele dve leti

in več po incidentu. Druge raziskave kažejo, da podjetja v povprečju potrebujejo 90 dni za odkritje hekerskega napada. Pogosto so incidenti identificirani s strani strank ali drugih deležnikov, kar je še dodatni razlog za tveganje izgube ugleda podjetja (Allianz, 2016).

Udeleženec B izpostavlja, da se bo percepcija o izpostavljenosti kibernetskim tveganjem spremenila ob prvem odmevnejšem primeru v Sloveniji. Tej tezi pritrjuje ugotovitev, da se je po kibernetskem incidentu v ameriškem trgovskem podjetju Target stopnja zaskrbljenosti pri najvišjem managementu v podjetjih, vključenih v raziskavo, na lestvici od 1 do 10, povišala s 5,7 na 7,8 (Ponemon, 2015a, str. 1 in 3).

Udeleženci iz bank so izpostavili predvsem napade na njihove bankomate, vdore v račune komitentov in poskuse prevar pri uporabi spletnega bančništva. Slednji so omenjeni tudi v letnem poročilu Nacionalnega odzivnega centra za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij (SI-CERT) za leto 2015. Hekerji iz tujine so izvedli napad z zvabljanjem (angl. *phishing*) komitentov šestih slovenskih bank. Napadalci so poskušali s pošiljanjem sporočil z izmišljenih elektronskih naslovov bančne komitente usmeriti na lažne spletne strani bank (SI-CERT, 2016, str. 24).

Kljub temu da imajo v vseh podjetjih dokumentirane tudi pravilnike za uporabo elektronskih naprav in družabnih omrežij je na podlagi raziskave o vplivu družbenih medijev (Chatzilia, 2014) razvidno, da poskušajo podjetja omejiti uporabo družbenih omrežij predvsem z namenom ohranjanja produktivnosti zaposlenih in ne zaradi kibernetskih tveganj.

Intervjuvanci največkrat izpostavljajo tveganje kršitve zaupnosti njihovih strank. Pri posledicah dogodka pa je največja skrb zaradi padca ugleda podjetja. Podobno lahko razberemo iz raziskave, ki jo je izvedla zavarovalnica Allianz (2016), kjer je med glavnimi razlogi za ekonomsko škodo po kibernetskem incidentu na prvem mestu navedena izguba ugleda podjetja, sledita obratovalni zastoj in tožbe iz naslova odškodninske odgovornosti in iz naslova kršitve zaupnosti podatkov. Največjo skrb zaradi kršitve zaupnosti podatkov so respondenti namenili padcu ugleda tudi v raziskavi Advisen (2015).

Domneva: Zaradi nezadostnega zavedanja o kibernetskih tveganjih in izostanka odmevnih primerov v lokalnem okolju podjetja podcenjujejo kibernetska tveganja.

Tabela 15: Predstavitev citatov globinskih intervjujev za posamezne sklope

Management tveganja kršitve zaupnosti podatkov	**Kibernetsko zavarovanje kot orodje managementa tveganj**
»V primeru kršitve zaupnosti podatkov je osrednja vloga namenjena službi skladnosti poslovanja in notranji reviziji. Imamo izdelan načrt za neprekinjeno poslovanje.« (udeleženec A)	»Lokalni zavarovalni trg kibernetskega zavarovanja ne ponuja. Tveganje je prisotno, vendar je verjetnost nizka. Na splošno se zavarovanja poslužujemo, ko so drugi ukrepi predragi.« (udeleženec A)
»Ključni je oddelek pravne podpore, ki je skrbnik osebnih podatkov. Za vdore, povezane z IT-sistemom, je odgovoren IT-oddelek. V primeru internih kršitev je odgovoren oddelek skladnosti poslovanja.« »Zbiramo veliko količino osebnih podatkov. Če nam ukradejo baze podatkov ima to lahko za nas finančne posledice in vpliv na naš ugled.« (udeleženec B)	»Zavarovanja nimamo sklenjenega, ker lokalni zavarovalni trg tega zavarovanja ne ponuja in ni bilo vedenja do sedaj.« » V podjetju prevladuje mnenje, da tveganja znamo obvladovati sami. Ko se bo zgodil prvi primer v Sloveniji, se bo stališče spremenilo.« (udeleženec B)
»V primeru incidenta varovanja varstva podatkov je v prvi vrsti odgovoren varnostni inženir in krizni štab (IT oddelek, sektor upravljanja s tveganji, uprava in PR). IT poskuša normalizirati stanje, PR pa se odloči o načinu komunikacije.« (udeleženec C).	»Nisem še razmišljal, da se lahko sploh zavaruješ za tovrstne rizike.« (udeleženec C)
»V primeru kršitve zaupnosti podatkov je PR odgovoren za komunikacijo z javnostmi, direktor za varstvo podatkov in IT-oddelek pa za obvladovanje incidenta.« (udeleženec D)	»Prvič slišim, da takšno zavarovanje obstaja.« (udeleženec D)
»Ob varnostnem incidentu bi IT-oddelek poskrbel za sanacijo ob sodelovanju s PR-službo, pravnim področjem, upravljanjem s tveganji in vodjo za varstvo podatkov. V primeru kršitve zaupnosti podatkov je zapisan dokument za splošni odziv na varnostne incidente.« (udeleženec E)	»Omejitev za sklenitev kibernetskega zavarovanja je razumevanje kritja.« (udeleženec E)
»V reševanje primera bi se najprej vključila pravna služba in IT-oddelek.« (udeleženec F)	»O zavarovanju do nedavnega nismo imeli vedenja. Slovenski zavarovalni trg tega ne ponuja.«. (udeleženec F)

Management tveganja kršitve zaupnosti podatkov. Na osnovi analize odgovorov udeležencev lahko ugotovimo, da so za varstvo zaupnosti podatkov zadolžena različna organizacijska področja v podjetjih, v odvisnosti od vzroka kršitve zaupnosti podatkov. Samo v dveh podjetjih imajo vzpostavljeno funkcijo vodje za varstvo podatkov. Pri večini podjetij je v primeru kršitve zaupnosti podatkov v postopek omejitve ali odprave posledic vključen tudi IT-oddelek. Za primerjavo lahko omenimo raziskavo managementa kibernetskih tveganj v evropskih podjetjih (Advisen, 2015), kjer je IT-oddelek največkrat, v 36 % primerih vprašanih, zadolžen za zagotavljanje skladnosti z zakonskimi zahtevami o

varstvu podatkov. Sledita mu s 26 % oddelek za skladnost poslovanja in z 19 % pravni oddelek.

Na osnovi razgovorov z udeleženci je razvidno, da imajo v podjetjih na podlagi internih dokumentov predvidene splošne postopke obravnave kršitve zaupnosti podatkov. Ob tem je bilo zaznati, da ti postopki izvirajo iz zakonskih predpisov, in ne iz poznavanja in upoštevanja posebnosti kibernetskih tveganj.

Za preprečevanje kibernetskega napada in zniževanje stroškov ob kršitvi zaupnosti podatkov je pomemben tudi vzpostavljen sistem za neprekinjeno poslovanje (Ponemon, 2015b; Giblin, 2015). Iz analize intervjujev je razvidno, da imajo vsa podjetja v veljavi izdelan načrt neprekinjenega poslovanja, v bankah in zavarovalnicah predvsem zaradi zakonskih zahtev in preverjanja nadzornih institucij.

V raziskavi Ponemon (2015a) je kot največja posledica kršitve zaupnosti podatkov naveden padec ugleda podjetja in vrednosti znamke. Padec ugleda je bil z 69 % med največkrat navedenimi razlogi za ekonomsko škodo, kot posledica kibernetskega incidenta, na prvem mestu tudi v raziskavi zavarovalnice Allianz (2016). Tega se zaveda udeleženec B, ki je izpostavil, da bi zloraba osebnih podatkov, ki jih pri poslovanju zbirajo, lahko poleg finančne škode imela vpliv tudi na ugled podjetja.

Domneva: V management tveganja kršitve zaupnosti podatkov je največkrat vključen oddelek informatike zaradi hrambe baz osebnih in poslovnih podatkov v elektronski obliki. Načrt neprekinjenega poslovanja je vzpostavljen zaradi zakonskih zahtev, in ne zaradi zavedanja pomembnosti zaščite integritete informacij in posledic, ki lahko povzročijo padec ugleda podjetja.

Kibernetsko zavarovanje kot orodje managementa tveganj. V nobenem podjetju, vključenem v raziskavo, trenutno nimajo sklenjenega kibernetskega zavarovanja. Razen enega intervjuvanca so drugi izpostavili, da niso seznanjeni z možnostjo prenosa kibernetskih tveganj na zavarovalnice. Večina jih je izpostavila, da kibernetskega zavarovanja lokalni zavarovalni trg ne ponuja. Na osnovi tega lahko ugotovimo, da v podjetjih niso seznanjeni z možnostjo sklenitve kibernetskega zavarovanja na evropskem zavarovalnem trgu ali pri lokalnih zavarovalnicah. Kljub temu da slovenske zavarovalnice nimajo lastnega produkta za kibernetsko zavarovanje, imajo možnost zagotovitve fakultativnega pozavarovalnega kritja in s tem možnost priprave ponudbe na osnovi povpraševanja s strani slovenskih podjetij.

Iz odgovorov tudi izhaja, da se v podjetjih zgolj odzivajo na ponudbo lokalnih zavarovalnic in ne raziskujejo proaktivno možnosti prenosa tveganj na zavarovalnice, kar je bilo razvidno že pri analizi modela managementa kibernetskih tveganj. Pomemben dejavnik za nepoznavanje kibernetskega zavarovanja je tudi nizka stopnja razvitosti dejavnosti zavarovalnega posredovanja v Sloveniji, kot je razvidno iz podatkov publikacije

Insurance Europe (2015). Ena temeljnih funkcij zavarovalnega posredovanja je tudi podajanje informacij o možnosti prenosa tveganja na zavarovalnice.

Iz izjav sodelujočih lahko razberemo, da kljub zavedanju obstoja kibernetskega tveganja ocenjujejo verjetnost nastanka kibernetskega incidenta kot relativno nizko. Ob takšni oceni se postavlja vprašanje o zavedanju možnih posledic dogodka, ki lahko kljub manjši škodni pogostosti povzroči veliko škodo. Iz podatkov o povprečnem strošku kršitve zaupnosti podatkov izhaja, da so podjetja lahko soočena z večmilijonskimi škodami (Ponemon, 2015b). Udeleženci so sicer ob preverjanju zaznavanja vloge zavarovanja na splošno izrazili mnenje, da je zavarovanje namenjeno nadomestitvi katastrofalne škode. Toda takšen odgovor je sledil šele po predstavitvi možnih odgovorov. Pred tem so imeli težave s pravilno umestitvijo vsebine zastavljenega vprašanja. Praksa slovenskih podjetij pri sklepanju zavarovanj je drugačna in kaže na razumevanje namena zavarovanja v funkciji nadomestitve vsake, tudi najmanjše škode. Podjetja namreč še vedno sklepajo večino zavarovanj brez odbitne franšize, hkrati pa ne zavarujejo ključnih tveganj (npr. potres, obratovalni zastoj in komercialni kriminal), ki lahko ogrozijo obstoj podjetja. Zaskrbljujoč je tudi komentar, da se bodo za sklenitev zavarovanja verjetno odločili šele v primeru realizacije kibernetskega dogodka. Na osnovi komentarjev udeležencev ocenjujem, da podjetja neustrezno pristopajo k managementu tveganj in podcenjujejo možne finančne posledice realizacije kibernetskega tveganja ter vpliva na ugled podjetja.

Iz raziskave Advisen (2014a) je razvidno, da so glavni dejavnik rasti povpraševanja po kibernetskih zavarovanjih novice o škodah zaradi kibernetskih napadov. S tem se sklada mnenje udeleženca B, da se bo zaznavanje o izpostavljenosti kibernetskim tveganjem spremenilo ob prvem odmevnejšem primeru v Sloveniji. Če k temu dodamo naslednji, iz raziskave Advisen (2014a) najpomembnejši dejavnik rasti povpraševanja, izobraževanje, ter med intervjuji ugotovljen izostanek zavedanja o možnosti zavarovanja kibernetskih tveganj, lahko ugotovimo glavne razloge za slabo razvit trg kibernetskih zavarovanj v Sloveniji.

Kljub temu da v podjetjih večinoma niso seznanjeni z možnostjo zavarovanja kibernetskih tveganj lahko ugotovimo, da so razlogi za nesklenitev zavarovanja podobni kot pri podjetjih, ki so bila vključena v raziskavo Advisen (2014a, str. 6). Tam je 73 % vprašanih kot glavno oviro pri sklepanju tovrstnih zavarovanj navedlo pomanjkanje razumevanja izpostavljenosti pred kibernetskimi tveganji. Med glavnimi razlogi so navedeni: nesprejemanje s strani IT-strokovnjakov, da so njihovi sistemi lahko ogroženi, in zanikanje zavarovancev o izpostavljenosti kibernetskim tveganjem. Skoraj polovica vključenih v raziskavo je kot naslednja najpomembnejša razloga za nesklenitev zavarovanja izpostavila pomanjkljive informacije o zavarovalnem produktu in znanje s strani zavarovalnih posrednikov ter strošek zavarovanja oz. natančneje izostanek planiranih sredstev za kibernetsko zavarovanje.

Ob osnovni predstavitvi kibernetskega zavarovanja in predvidenih postopkov pri uveljavljanju pravic iz naslova kibernetskega zavarovanja so udeleženci med vsemi sklopi zavarovalnega kritja največ zanimanja pokazali za kritje visokih glob regulatorjev, ki jih predvideva nova evropska Splošna uredba o varstvu podatkov. Odziv ni presenetljiv glede na pričakovanja zavarovalnega trga, da se bo povpraševanje po kibernetskih zavarovanjih v Evropi povečalo na podlagi izkušenj iz ZDA zaradi zaščite podjetij pred povečanimi stroški, povezanimi s strožjo zakonodajo s področja varstva podatkov (Glascott & Eisen, 2013; Allianz, 2016). Vendar kot ugotavlja Hillyer (2014, str. 36) so potencialne finančne posledice zaradi kršitve zaupnosti podatkov lahko mnogo večje od prisojenih glob in pogosto spregledane s strani poslovodstva.

Domneva: Zaradi nerazvitega lokalnega zavarovalnega trga kibernetskih zavarovanj in nerazvitosti zavarovalnega posredovanja v Sloveniji ni zavedanja o možnosti prenosa kibernetskega tveganja na zavarovalnice.

SKLEP

Do nedavnega je bila kibernetska varnost samoumevna, v podjetjih so zanjo skrbeli izključno predstavniki oddelkov informatike. V poslovnem in družbenem svetu se srečujemo z vprašanjem začetka nove svetovne tehnološke revolucije, ki jo naznanjajo inovacije v tehnologiji storitev v oblaku, mobilnosti, družbenih medijev, virtualizacije in interneta stvari. Preobrazba globalne ekonomije gre v smeri digitalizacije, ki poleg pozitivnih plati prinaša tudi nova tveganja, pri čemer management podjetij na prvo mesto v prihodnjih letih postavlja kibernetska tveganja. Neopredmetena sredstva v obliki podatkov, informacij, znanja in pravic iz naslova intelektualne lastnine so že danes osnova poslovnega modela največjih in najuspešnejših podjetij. Globalna poslovna in družbena povezanost in dostopnost sodobnih tehnologij na drugi strani omogočajo hitro rast in uspešnost kibernetskega kriminala, kar dokazujejo številne raziskave. Tako lahko v prihodnje upravičeno pričakujemo povečanje tveganja iz naslova različnih nevarnostnih dejavnikov.

Zagotavljanje kibernetske varnosti mora biti zato sestavni del vsakega programa managementa tveganj. Ustrezni postopki pri implementaciji preventivnih ukrepov za preprečitev manifestacije kibernetskih tveganj morajo biti del robustne infrastrukture managementa tveganj, ki ne vključuje samo oddelka informatike, temveč morajo biti podprti in usmerjani s strani najvišjega poslovodstva v podjetjih.

Z uvedbo strožje zakonodaje s področja varstva osebnih podatkov so ob kibernetskem incidentu, ki ima za posledico kršitev zaupnosti podatkov, podjetja poleg neposrednih stroškov za reševanje primera in običajno tudi izgubi ugleda izpostavljene finančni obremenitvi zaradi predvidenih postopkov obveznega obveščanja oškodovancev in visokih glob regulatorjev.

Podjetja so se v preteklosti pri managementu kibernetskih tveganj osredotočala na investicije v sisteme varovanja in strokovnjake z informacijskih znanjem, z namenom zmanjševanja tveganj. Na ta način se možnost kibernetskega incidenta omeji, vendar tveganje ostaja, zato je pomembna ocena optimalnega obsega sredstev, namenjenih za kibernetsko varnost, in finančna izpostavljenost premostitve posledic kibernetskega dogodka. Zavarovanje omogoča prenos finančnih posledic kibernetskega incidenta na zavarovalnice. Kibernetsko zavarovanje z omogočanjem in plačilom storitev zunanjih strokovnjakov, kar je posebnost v primerjavi z drugimi zavarovanji, podjetjem zagotavlja dodano vrednost v procesu managementa tveganj. Zato lahko potrdim hipotezo, da kibernetsko zavarovanje predstavlja ustrezno orodje za management kibernetskih tveganj. Sklenitev kibernetskega zavarovanja mora biti le ena od komponent celostnega načrta managementa kibernetskih tveganj, in ne samo izhod v sili v primeru kibernetskega incidenta. Pri managementu kibernetskih tveganj je ključna ugotovitev, da popolne kibernetske varnosti z odpravo ali znižanjem tveganj ni možno zagotoviti.

Zavarovalnice trenutno zagotavljajo kombinacijo kritja zahtevkov tretjih oseb iz naslova odgovornosti in lastne škode v primeru kibernetskega incidenta, ki sovpade z vsebino zavarovane nevarnosti. Kljub temu pa zavarovanje ne zagotavlja kritja za povrnitev izgubljenega ugleda in intelektualne lastnine podjetja. Zaradi sistemskega tveganja, s katerim so soočene zavarovalnice, in nenehnega razvoja tehnologij je prihodnji razvoj kibernetskega zavarovanja nepredvidljiv.

Trenutno stanje na zavarovalnem trgu je ovira za hitrejši razvoj uporabe kibernetskega zavarovanja v okviru managementa kibernetskih tveganj. Na osnovi različnih raziskav trga kibernetskega zavarovanja lahko ugotovimo, da je penetracija še vedno na zelo nizki ravni. Na omejeno ponudbo imajo največji vpliv asimetrija informacij, s tem povezana negativna selekcija in moralni hazard ter visoka korelacija rizikov in posledično velika verjetnost nenadzorovane akumulacije rizikov. Na strani povpraševanja se kot pomembna ovira izpostavlja zapletenost zavarovalnih pogojev in negotovost glede dejanskega kritja, posledica številnih izključitev kritja in spreminjajoče se narave kibernetskih tveganj. Pomanjkanje razumevanja izpostavljenosti podjetij pred kibernetskimi tveganji in pomanjkljive informacije o kibernetskem zavarovanju vodijo v napačno percepcijo, da so ključna tveganja že pokrita z drugimi zavarovanji.

Pri podjetjih, vključenih v raziskavo managementa kibernetskih tveganj v Sloveniji, je razvidno, da zaradi nezadostnega zavedanja o kibernetskih tveganjih in izostanka odmevnih primerov v lokalnem okolju podjetja podcenjujejo kibernetska tveganja. Zaradi nerazvitega trga kibernetskih zavarovanj v Sloveniji in nizke stopnje znanja o kibernetskih tveganjih oz. zavarovanjih vseh udeležencev zavarovalnega trga podjetja niso seznanjena z možnostmi prenosa kibernetskega tveganja na zavarovalnice. Tu je izrazito nezadostna vloga zavarovalnega posredništva v procesu prenosa tveganja na zavarovalnice.

Z novo evropsko Uredbo o varstvu podatkov lahko pričakujemo povečano povpraševanje, zmanjšanje problema negativne selekcije in moralnega hazarda. Hkrati bodo podjetja doumela, da je izgubljeni ugled podjetja ključno tveganje. Pomembna spodbuda za dvig zavedanja pomembnosti kibernetskih tveganj so medijsko odmevni primeri kibernetskih incidentov.

Kljub temu da na osnovi rezultatov raziskave managementa tveganj v izbranih slovenskih podjetjih lahko načeloma potrdim ustrezno umeščenost funkcije managementa tveganj, je iz vsebine odgovorov razviden razlog, in sicer ne proaktivnost podjetij temveč odziv na zakonske zahteve. To nakazuje na vsebinsko neustrezno umeščenost managementa ključnih tveganj v organizacijsko strukturo podjetij.

Podobno kot pri evropskih podjetjih je v večini primerov za management kibernetskih tveganj zadolžen oddelek informatike. Pomanjkanje razumevanja kompleksnosti kibernetskega tveganja in nezavedanja poslovodstev o spremembah globalnega okolja je v podjetjih na splošno glavna ovira za boljšo pripravljenost pred kibernetskimi nevarnostmi. Ugotavljam, da je splošna raven razumevanja kibernetskih tveganj in njihovih posledic v podjetjih, vključenih v raziskavo, nizka, zaznavanje, da je management kibernetskih tveganj delo IT-oddelka, pa napačna.

Zaradi omejitvenih dejavnikov načina raziskave ugotovitve in rezultatov ni mogoče šteti za dokončne. Na osnovi izvedene kvalitativne raziskave tudi ni možno posploševanje za celotno slovensko gospodarstvo. Za nadaljnjo raziskavo in preverjanje domnev je smiselna izvedba kvantitativne raziskave na večjem vzorcu podjetij. Kljub temu se je izbrana tehnika raziskovanja izkazala za ustrezno, saj je bilo ugotovljeno ozadje organizacijske umeščenosti managementa tveganj in pridobljene informacije, ki jih s kvalitativnimi tehnikami ni možno pridobiti.

LITERATURA IN VIRI

1. Advisen. (2013). *2013 Information Security Cyber Liability & Risk Management*. New York: Advisen.
2. Advisen. (2014a). *Cyber Liabiliy Insurance Market Trends: Survey*. New York: Advisen.
3. Advisen. (2014b). *Cyber Insurance Underwriting: A High-Tech, Evolving Discipline*. New York: Advisen.
4. Advisen. (2015). *2015 Network Security & Cyber Risk Management*. New York: Advisen.
5. Advisio d.o.o. (2016). *Cyber zavarovanje* (interno gradivo). Ljubljana: Advisio d.o.o.
6. Allianz. (2015). *A Guide to Cyber Risk*. Munich: Allianz Global Corporate & Specialty SE.
7. Allianz. (2016). *Allianz Risk Barometer – Top Business Risks 2016*. Munich: Allianz SE and Allianz Global Corporate & Specialty SE.
8. Bailey, T., Kaplan, J., & Rezek, C. (2014). Why senior leaders are the front line against cyber attacks. Najdeno 11. marca 2016 na spletnem naslovu http://www.mckinsey.com/business-functions/business-technology/our-insights/why-senior-leaders-are-the-front-line-against-cyberattacks
9. Bandyopadhyay, T, Mookerjee, V.S., & Rao, R.C. (2009). Why IT Managers Don't Go for Cyber-Insurance Products. *Communication of the ACM, 52*(11), 68–73.
10. Berliner, B. (1985). Large Risks and Limits of Insurability. *The Geneva Papers on Risk and Insurance – Issues and Practice 37*, 313–329.
11. Biener, C., Eling, M., & Wirfs, J.H. (2015). Insurability of Cyber Risk: An Empirical Analysis. *The Geneva Papers on Risk and Insurance – Issues and Practice 40*, 131–158.
12. Bolot, C., & Lelarge, M. (2009). Cyber Insurance as an Incentive for Internet Security. V *Managing Information Risk and the Economics of Security* (str. 269-290). New York: Springer.
13. Boyce, C., & Neale, P. (2006). *Conducting In-Depth Interviews: A Guide for Designingand Conducting In-Depth Interviews for Evaluation Input*. Najdeno 16. maja 2016 na spletnem naslovu http://www2.pathfinder.org/site/DocServer/m_e_tool_series_indepth_interviews.pdf
14. Böhme, R., & Kataria, G. (2006). *Models and Measures for Correlation in Cyber-Insurance*. Cambridge: University of Cambridge.
15. Böhme, R., & Schwartz, G. (2010). *Modeling Cyber Insurance: Towards a Unifying Framework.* Cambridge (MA): Harvard University.
16. Canham, D. (2014). Governance of Cyber Threat. V *Cyber Risk – Resources for Practitioners* (str. 41-58). London: The Institute of Risk Management.
17. Cebula, J. J., & Young, L.R. (2010). *A Taxonomy of Operational Cyber Security Risks*. Software Engineering Institute, Carnegie Mellon University.

18. Chatzilia, A. (2014). Social Media – Managing Risks and Seizing Opportunities. V *Cyber Risk – Resources for Practitioners* (str. 141–160). London: The Institute of Risk Management.
19. Chertoff, M., & Pflaging, J. (2015). The Three Ts of the Cyber Economy. V M. Rosenquist (ur.), *Navigating the Digital Age* (str. 9–15). Chicago: Caxton Business & Legal, Inc.
20. DaSilva, C. M., Trkman, P., Desouza, K., & Lindič, J. (2013). Disruptive technologies: a business model perspective on cloud computing. *Technology Analysis & Strategic Management, 25*(10), 1161–1173.
21. Eling, M., & Wirfs, J.H. (2015). *Modelling and Management of Cyber Risk*. Institute of Insurance Economics, University of St. Gallen.
22. ENISA. (2012). *Incentives and Barriers of the Cyber Insurance Market in Europe.* European Network and Information Security Agency.
23. Eurostat. (2014). *Cloud computing – statistics on the use by enterprises*. Najdeno 11. marca 2016 na spletnem naslovu: http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises
24. Eurostat. (2015). *ICT Security in enterprises*. Najdeno 11. marca 2016 na spletnem naslovu: http://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_security_in_enterprises
25. Evropska komisija. (2012). *Predlog Uredbe evropskega parlamenta in sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (Splošna uredba o varstvu podatkov).*
26. Evropska komisija. (2014). *Politike Evropske unije: Digitalna agenda*. Najdeno 4. junija 2016 na spletnem naslovu http://europa.eu/pol/pdf/flipbook/sl/digital_agenda_sl.pdf
27. Evropska komisija. (2016). *Commission sets out path to digitise European industry.* Najdeno 23. aprila 2016 na spletnem naslovu: http://europa.eu/rapid/press-release_IP-16-1407_en.htm
28. Evropski parlament. (2013). *Resolucija Evropskega parlamenta z dne 12. septembra 2013 o strategiji Evropske unije za kibernetsko varnost: odprt, varen in zanesljiv kibernetski prostor.* Najdeno na spletnem naslovu: http://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:52013IP0376&from=SL
29. Evropski parlament. (2016). *Data protection reform – Parliament approves new rules fit for the digital era.* Najdeno 1. junija 2016 na spletnem naslovu: http://www.europarl.europa.eu/news/en/news-room/20160407IPR21776/Data-protection-reform-Parliament-approves-new-rules-fit-for-the-digital-era
30. Fenz, S., & Heurix, J. (2014). Current challenges in information security risk management. *Information Management & Computer Security 22*(5), 410–430.
31. FERMA. (2003). *A Risk Management Standard*. Bruselj: Federation of European Risk Management Associations.
32. Ferrillo, A. P. (2015). *Navigating the Cybersecurity Storm*. New York: Advisen.

33. Giblin, A. (2015). Insurance is Important Tool in Cyber Risk Mitigation. Philadelphia: *The RMA Journal*. 32–37.
34. Glascott, T. M., & Aisen, J. A. (2013). The Emperor's New Clotes and Cyber Insurance. *FDCC Quarterly, pomlad 2013,* 200–225.
35. Gordon, A.L., Loeb, P. M., & Sohail, T. (2003). A Framework for Using Insurance for Cyber-Risk Management. *Communication of the ACM, 46*(3), 81–85.
36. Harrington, E. S., & Niehaus, R. G. (2003). *Risk Management and Insurance (2nd ed.)*. Boston: McGraw – Hill/Irwin.
37. Hillyer, M. (2014). The Iceberg Impact of a Cyber Loss. V *Cyber Risk – Resources for Practitioners* (str. 30–40). London: The Institute of Risk Management.
38. IBM. (2016). *IBM 2016 Cyber Security Intelligence Index*. Najdeno 1. junija 2016 na spletnem naslovu http://public.dhe.ibm.com/common/ssi/ecm/se/en/sej03320usen/SEJ03320USEN.PDF
39. Insurance Europe. (2015). *European Insurance — Key Facts*. Najdeno 16. maja 2016 na spletnem naslovu http://www.insuranceeurope.eu/sites/default/files/attachments/EuropeanInsurance-KeyFacts-August2015.pdf
40. IRM. (2002). *A Risk Management Standard*. London: The Institute of Risk Management.
41. IRM. (2014). *Cyber Risk – Resources for Practitioners*. London: The Institute of Risk Management.
42. Jones, R. (2015). Cyber Insurance: What You Should Know. *Insurance Advocate, 126*(20), 28–30.
43. Kannry, S., & White, D. (2015). *Optimizing Investment to Minimaze Cyber Exposure.* V M. Rosenquist (ur.), *Navigating the Digital Age* (str. 283–287). Chicago: Caxton Business & Legal, Inc.
44. Kraševec, H. (2006). *Slovar zavarovalništva: angleško-slovenski in slovensko-angleški*. Ljubljana: Pegaz International.
45. Kwon, W. J. (2003). The Role of Insurance in Corporate Risk Finance. *Review of Business, jesen 2003,* 36–40.
46. Lewis, J. A. (2016). *Managing Risk for the Internet of Things*. Washington: Center for Strategic and International Studies.
47. Lewis, J., McNaughton Nicholls, C., Ormston, R., & Ritchie, J. (2013). *Qualitative Research Practice: A Guide for Social Science Students and Researchers*. London: Sage.
48. Lloyd's. (2014). *Market Bulletin: Cyber Risks & Exposures*. Najdeno 19. junija 2016 na spletnem naslovu https://www.lloyds.com/~/media/files/the%20market/communications/market%20bulletins/2014/11/y4842.pdf
49. Lloyd's. (2015). *Emerging Risk Report – 2015: Business Blackout.* Cambridge: Cambridge Centre for Risk Studies. University of Cambridge Judge Business School.
50. Lloyd's. (2016). *Lloyd's Cyber Attack Strategy*. Najdeno 27. junija 2016 na spletnem naslovu https://www.lloyds.com/~/media/files/the%20market/operating%20at%20lloyds/lloyds%20cyber%20attack.pdf

51. Malhotra, K. N., & Peterson, M. (2006). *Basic Marketing Research: A Decision-Making Approach*. Upper Saddle River: Pearson Education.
52. Marsh. (2015). *UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk*. Najdeno 13. marca 2016 na spletnem naslovu https://www.gov.uk/government/publications/uk-cyber-security-the-role-of-insurance
53. McAfee. (2014). *Net Losses: Estimating the Global Cost of Cybercrime*. Washington: Center for Strategic and International Studies. Najdeno 14. marca 2106 na spletnem naslovu http://csis.org/event/2014-mcafee-report-global-cost-cybercrime
54. Pearson, N. (2014). A Larger Problem: Financial and Reputational Risks. *Computer Fraud & Security*, *2014*(4), 11–13.
55. Ponemon. (2015a). *2014 – A Year of Mega Breaches*. North Traverse City: Ponemon Institute LLC.
56. Ponemon. (2015b). *2015 Cost of Data Breach Study – Global Analysis*. North Traverse City: Ponemon Institute LLC.
57. PwC. (2015a). *Insurance 2020 & beyond – Reaping the dividends of cyber resilience*. PwC.
58. PwC. (2015b). *The Global State of Information Security Survey 2016*. Najdeno 13. marca 2016 na spletnem naslovu http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html
59. Refsdal, A., Solhaug, B., & Stølen, K. (2015). *Cyber-Risk Management*. B.k.: SpringerBriefs in Computer Science.
60. Risk Nexus. (2014). *Beyond Data Breaches – Global Interconnections of Cyber Risk*. Zurich: Zurich Insurance Company Ltd and Atlantic Council of the United States.
61. Roberts, D. (2014). Cloud: Cyber Risk and Reality. V *Cyber Risk – Resources for Practitioners* (str. 101–120). London: The Institute of Risk Management.
62. Ruffle, S., Coburn, A., Ralph, D., & Bowman, G. (2013). *Profile of a Macro-Catastrophe Threat Type: Cyber Catastrophe*. Najdeno 10. marca 2016 na spletnem naslovu http://cambridgeriskframework.com/downloads
63. SI-CERT. (2016). *Poročilo o omrežni varnosti za leto 2015*. Najdeno 30. junija 2016 na spletnem naslovu https://www.cert.si/wp-content/uploads/2016/06/SI-CERT_LP_2015.pdf
64. Siegel, A. C., Sagalow, R. T., & Serritella, P. (2002). Cyber Risk Management – Technical and Insurance Controls for Enterprise – Level Security. *Information System Security*, *11*(4), 33–49.
65. SZZ. (2015). *Statistični zavarovalniški bilten 2015*. Ljubljana: Slovensko zavarovalno združenje.
66. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications, 34*(1), 1–11.
67. The Economist. (2014). Special Report – Cyber Security, 12. julij 2014.
68. Timetric. (2015) *Insight Report: The Future of Cyber Risk Insurance*. London: Timetric.

69. Trkman, P., Oliveira, M. P. V., & McCormack, K. (2016). Value-Oriented Supply Chain Risk Management: You Get What You Expect. *Industrial Management & Data Systems*, *116*(5), 1061–1083.
70. Uredba (EU) št. 679/2016 Evropskega parlamenta in Sveta EU z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov). *Uradni list EU* L119.
71. Verizon. (2015). 2015 *Data Breach Investigation Report.* Najdeno 13. marca 2016 na spletnem naslovu http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf
72. Von Solms, R., & Van Niekerk, J. (2013). From Information Security to Cyber Security. *Computers and Security*, *oktober 2013, 38*, 97–102.
73. Williams, C. (2014). Cyber Risk and Risk Management. V *Cyber Risk – Resources for Practitioners* (str. 9–18). London: The Institute of Risk Management.
74. World Economic Forum. (2016). *The Global Risks Report 2016* (11th Edition). Geneva: World Economic Forum.
75. *World's Biggest Data Breaches*. Najdeno 14. junija 2016 na spletnem naslovu http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
76. Zakon o bančništvu. *Uradni list RS*, št. 25/2015.
77. Zakon o gospodarskih družbah. *Uradni list RS*, št. 42/2006.
78. Zakon o varstvu osebnih podatkov. *Uradni list RS*, št. 86/2004.
79. Zakon o zavarovalništvu. *Uradni list RS*, št. 93/2015.

PRILOGE

KAZALO PRILOG

PRILOGA 1: Slovarček izrazov

Informacijska varnost (angl. *information security*)
Zaščita zaupnosti, celovitosti in razpoložljivosti informacij, ki so lahko v kakršni koli pojavni obliki (elektronski, fizični ali kot znanje zaposlenih).

Internet stvari (angl. *internet of things*)
Povezljivost avtonomnih naprav preko interneta. Naprave imajo običajno svoj IP-naslov, vgrajen računalniški sistem, napravo za zaznavanje okolice in večinoma brezžično omrežno povezljivost.

Kibernetska varnost (angl. *cybersecurity*)
Zaščita pred nevarnostmi v kibernetskem prostoru. Kibernetska varnost ni omejena samo na informacijska sredstva, temveč vključuje tudi infrastrukturo in sredstva, kot so življenje, zdravje, ugled in drugo.

Kibernetski kriminal (angl. *cybercrime)*
Protipravno dejanje z namenom pridobitve premoženjske koristi s pomočjo komunikacijskih naprav v omrežju.

Kibernetski oz. varnostni incident (angl. c*yber or security incident*)
Kibernetski napad in/ali varnostni dogodek, ki ga je preveril varnostni analitik in ga ovrednotil kot varnostni incident, vreden nadaljnje preiskave. Dogodek, ki ogroža zaupnost, celovitost ali razpoložljivost informacijskih sredstev.

Kibernetski oz. varnostni napad (angl. *cyber or security attack*)
Varnostni dogodek, prepoznan z analitskim orodjem in v povezavi z zlonamernim delovanjem, ki poskuša zbrati, prekiniti, zavračati, škoditi ali uničiti sredstva informacijskega omrežja ali informacijo samo.

Kibernetski prostor (angl. *cyberspace*)
Medsebojno povezano področje, ki je sestavljeno iz vseh digitalnih omrežij za shranjevanje, obdelavo in komunikacijo informacij.

Kršitev zaupnosti podatkov (angl. *data security breach)*
Kibernetski oz. varnostni incident, ki je potrjeno povzročil razkritje podatkov nepooblaščeni tretji osebi.

Porazdeljena ohromitev storitve (angl. *distributed denial of service*)
Poskus obremenitve računalniškega strežnika ali omrežja z velikim obsegom prometa ali zlonamernega prometa, ki povzroči nedelovanje naprave.

Socialni inženiring (angl. *social engineering*)
Način prevare, kjer napadalec s pomočjo zvijače žrtev prepriča v izvedbo dejanja, ki ga običajno ne bi storila. Značilno je, da takšna dejanja povzročijo odpiranje zlonamerne spletne strani ali zaženejo neželeno pripeto datoteko. Napadalci s tem pridobijo osebne informacije in gesla, ki jih uporabijo za pridobitev premoženjske koristi. Najbolj pogoste prevare so napadi z zvabljanjem (angl. *phishing*), pharming napadi, trojanski konji, virusi, črvi in vishing.

Storitve v oblaku (angl. *cloud services*)
Aplikacije in strojna oprema, dostavljena kot storitev preko interneta.

Varnostni dogodek (angl. *security event*)
Dogodek, ki se zgodi v sistemu ali omrežju in je zaznan z varnostno napravo ali aplikacijo.

PRILOGA 2: Opomnik za globinski intervju

Model managementa tveganj

- Kakšen model managementa tveganj imate vzpostavljen v podjetju? Kakšen mednarodni standard managementa tveganj imate v veljavi?
- Kakšna je vaša definicija kategorije operativnih kibernetskih tveganj?
- Ali v podjetju obstaja samostojna funkcija Direktor/Vodja upravljanja s tveganji (angl. *Chief Risk Officer*) in kje v organizacijski strukturi podjetja je umeščena?
- Kako uprava podjetja na splošno ocenjuje izpostavljenost pred kibernetskimi tveganji. Ali se smatra kot problem IT-oddelka?
- Kako imate v podjetju dokumentirano oz. zapisano politiko informacijske varnosti?
- Na kakšen način se pravilniki/postopki izvajajo? Na kakšen način se izvajajo interna izobraževanja na temo informacijske varnosti v podjetju?

Vpliv nove Splošne evropske uredbe o varstvu podatkov

- Ali ste seznanjeni s Splošno uredbo o varstvu podatkov, sprejeto aprila 2016?
- Kako ocenjujete poglavitne novosti v primerjavi z obstoječo Uredbo?
- Kako se v podjetju pripravljate na zagotavljanje skladnosti z uredbo?
- Kako imate v podjetju urejeno pogodbeno odgovornost poslovnih partnerjev za zagotavljanje varovanja osebnih podatkov?

Izpostavljenost kibernetskim tveganjem

- Ali je bilo vaše podjetje že predmet kibernetskega napada in kakšnega?
- Z vidika vašega podjetja razvrstite sledeče na lestvici od 1 do 5, pri čemer 5 predstavlja zelo visoko tveganje in 1 zelo nizko tveganje. Dogodek oz. tveganje:
- Kršitev zaupnosti podatkov vaših strank
- Kršitev zaupnosti podatkov oz. kibernetski napad zaradi t. i. BYOD (*Bring your own device*); uporabe osebnih pripomočkov zaposlenih za službene namene ali uporaba službenih računalnikov za privatne namene (Facebook, Gmail, idr.)
- Kraja/izguba sredstev/intelektualne lastnine podjetja
- Kraja/izguba intelektualne lastnine strank
- »Denial of service attack« v primerjavi z vašim sistemom/omrežjem
- »Malware« v vašem sistemu/omrežju

Posledice dogodka:

- Razvrednotenje ugleda podjetja zaradi kršitve zaupnosti podatkov
- Padec ugleda podjetja preko družbenih omrežij
- Povečani stroški podjetja zaradi kibernetskega napada
- Obratovalni zastoj zaradi prekinitve poslovanja podjetja
- Obratovalni zastoj zaradi kibernetskega napada pri dobavitelju
- Obratovalni zastoj zaradi kibernetskega napada pri vaši stranki

Management tveganja kršitve zaupnosti podatkov

- Kakšna je vloga/odgovornost naslednjih sektorjev v vašem podjetju v primeru kršitve zaupnosti podatkov pri zagotavljanju skladnosti z Zakonom o varovanju osebnih podatkov?
- Prodaja/marketing
- Podpora uporabnikom
- IT
- Splošne/pravne zadeve
- Upravljanje s tveganji/zavarovanji
- Skladnost poslovanja
- Direktor/vodja za varstvo osebnih podatkov (angl. *Chief Privacy Officer*)
- Ali imate izdelan načrt odziva v primeru kršitve zaupnosti podatkov in kdo je odgovoren za koordinacijo aktivnosti?

Kibernetsko zavarovanje kot orodje managementa tveganj

- Kakšno je vaše stališče do kibernetskega zavarovanja kot orodja managementa kibernetskih tveganj?
- Katere so po vašem mnenju omejitve kibernetskega zavarovanja? Katera zavarovanja po vašem mnenju krijejo kibernetska tveganja?
- Ali ima vaše podjetje sklenjeno »cyber« oz. kibernetsko zavarovanje in kakšen limit kritja kupujete?
- Zakaj vaše podjetje nima sklenjenega kibernetskega zavarovanja in ali načrtujete sklenitev v prihodnje? Kakšen je dostop do zavarovalnega trga kibernetskih zavarovanj?
- Kakšna je vaša percepcija vloge zavarovanja na splošno in pri kibernetskih tveganjih?