TAMPEREEN YLIOPISTO
Johtamiskorkeakoulu

KYBERRISKIEN ARVIOINTI JA KYBERVAKUUTTAMINEN – KOLMANNET OSAPUOLET KYBERRISKIEN LÄHTEENÄ

Vakuutustiede
Pro gradu -tutkielma
Huhtikuu 2018
Tekijä: Sakari Rytkönen

Ohjaaja: Lasse Koskinen

TIIVISTELMÄ

Tampereen yliopisto	Johtamiskorkeakoulu: vakuutustiede
Tekijä:	RYTKÖNEN, SAKARI
Tutkielman nimi:	Kyberriskien arviointi ja kybervakuuttaminen – kolmannet osapuolet kyberriskien lähteenä
Pro gradu -tutkielma:	86 sivua, 2 liitesivua
Aika:	Huhtikuu 2018
Avainsanat:	Kyberriski, kybervakuutus, kyberriskien hallinta, kyberturvallisuus, kolmas osapuoli, ulkoistaminen

---

Kyberriskit ovat nousseet nopeasti yhdeksi vakavimmista yrityksiä ja yhteiskuntia uhkaavista riskeistä. Ne ovat saaneet julkisuudessa paljon huomiota, koska suurissa tietomurroissa on vuotanut jopa kymmenien miljoonien asiakkaiden luottamuksellisia tietoja. Kyberriskit aiheuttavat yrityksille suoria taloudellisia haittoja sekä epäsuoria vahinkoja, kuten mainehaittoja. Yritykset käyttävät liiketoiminnassaan yhä enemmän kolmansia osapuolia, esimerkiksi alihankkijoita, joille he ulkoistavat tietojenkäsittelyä ja -säilytystä. Kolmannet osapuolet voivat olla haavoittuvuus koko toimitusketjulle, jolloin kyberrikolliset pääsevät yhden toimitusketjun jäsenen kautta murtautumaan muiden yritysten IT-järjestelmiin. Kolmansista osapuolista aiheutuvia kyberriskejä pidetäänkin yhtenä vakavimmista ja vaikeimmin hallittavista riskeistä.

Tämän tutkielman tavoitteena on syventyä kolmansista osapuolista aiheutuviin kyberriskeihin ja selvittää, miten niistä aiheutuvia kyberriskejä voidaan arvioida ja kuinka niitä voidaan hallita kybervakuutuksella. Lisäksi tutkielmassa syvennytään tarkastelemaan, kuinka pilvipalveluiden käyttäminen vaikuttaa yrityksen kyberturvallisuuteen. Tutkielmassa tarkasteltava aihepiiri on tieteellisessä kentässä toistaiseksi vähän kartoitettu alue, minkä vuoksi ilmiötä tutkitaan laadullisin tutkimusmenetelmin. Tutkielman empiirinen aineisto koostuu kuuden asiantuntijan teemahaastattelusta. Tutkimushaastatteluilla hankittua empiiristä aineistoa analysoidaan sisällönanalyysin keinoin.

Tutkielmassa havaitaan, että kolmansista osapuolista aiheutuvien kyberriskien arviointi on haastavaa. Tulosten perusteella kolmansista osapuolista aiheutuvia kyberriskejä arvioidaan toistaiseksi samankaltaisilla menetelmillä kuin yritykseen suoraan kohdistuvia kyberriskejä. Näkymän puuttuminen alihankkijaverkostoon ja sen IT-järjestelmiin tekee perinteisen riskienhallintatyön ongelmalliseksi, ja vakavat uhat sekä haavoittuvuudet kolmansissa osapuolissa voivat jäädä huomioimatta. Lisäksi tutkielmassa havaitaan, että pilvipalveluiden käyttäminen voi parantaa kyberturvallisuutta kokonaisuutena, jos ulkoistavan yrityksen kyberturvallisuus on heikompi kuin pilvipalveluntarjoajan. Toisaalta pilvipalveluiden käyttäminen voi heikentää kyberturvallisuutta, jos ulkoistavan yrityksen kyberturvallisuus on lähtökohtaisesti hyvä ja ulkoistettavat tiedot ovat hyvin luottamuksellisia. Tutkielmassa havaitaan, että suomalaisten vakuutusyhtiöiden tarjoamilla kybervakuutuksilla voi suojautua kolmansista osapuolista aiheutuvia vastuu- ja riippuvuuskeskeytysriskejä vastaan, kun niiden vakuuttaminen on huomioitu vakuutussopimusta tehtäessä.

ALKUSANAT

Tämä pro gradu -tutkielma tehtiin lukuvuonna 2017–2018 Tampereen yliopiston kauppatieteiden tutkinto-ohjelman vakuuksen ja riskienhallinnan opintosuunnassa. Lukuvuoden aikana toteutettu tutkimusprosessi on ollut tutkielman tekijälle kehittävä ja mielenkiintoinen ajanjakso, joka on antanut mahdollisuuden syventyä ajankohtaiseen ja vähän tunnettuun ilmiöön. Kyberriskit ja kybervakuuttaminen ovat teemoja, joiden merkitys liike-elämässä ja tieteen kentässä tulee kasvamaan tulevaisuudessa.

Tutkimusprosessin eri vaiheissa olen saanut arvokasta tukea ja apua useilta eri henkilöiltä ja tahoilta, joille haluan osoittaa kiitokseni. Aluksi haluan kiittää Tampereen yliopiston vakuutuksen ja riskienhallinnan opintosuunnan professori Lasse Koskista, joka on ollut tutkielmani ohjaaja ja jolta olen saanut arvokkaita kommentteja ja kehitysehdotuksia tutkimusprosessin edetessä. Lisäksi haluan kiittää vertaisiani tutkimusseminaarissa esitetyistä näkemyksistä ja kehitysehdotuksista, jotka ovat olleet hyödyllisiä erityisesti tutkimusprosessin alkuvaiheissa. Suuren kiitoksen ansaitsevat tutkielman viimeistelyssä auttaneet läheiseni ja tuttavani, joiden kehitysehdotukset ja kommentit ovat olleet tärkeitä ja arvokkaita.

Suurin kiitos kuuluu tutkielmaa varten haastatelluille kuudelle kybervakuutus- ja kyberturvallisuusasiantuntijalle, joiden onnistuneet haastattelut sekä vankka asiantuntemus ja kokemus mahdollistivat tämän tutkielman suorittamisen. Lopuksi haluan kiittää Kansan Sivistysrahastoa ja Suomen Vakuutusyhdistys ry:tä, jotka ovat tukeneet tutkimusprosessiani apurahalla.

Sakari Rytkönen

Tampereella 28.4.2018

SISÄLLYSLUETTELO

1 JOHDANTO

1.1 Tutkielman taustaa

Moderni yhteiskunta on riippuvainen informaatioteknologiasta ja sitä hyödynnetään lähes jokaisella toimialalla. Laitteiden ja tietoverkkojen häiriöt paljastavat riippuvuutemme teknologiasta, kun monet toiminnot keskeytyvät esimerkiksi tietoliikennekatkosten vuoksi. Häiriötilanteissa ilmenee, kuinka nopeasti vaikutukset leviävät verkossa eri laitteiden, liiketoimintaprosessien ja toimitusketjujen välityksellä jopa maailmanlaajuisesti. Informaatioteknologiasta on tullut myös keskeinen osa yhteiskuntien kriittistä infrastruktuuria, kuten sähkönjakelua, maksuliikennettä ja terveydenhoitoa. (Franke 2017)

Yhteiskuntien, organisaatioiden ja yksityishenkilöiden riippuvuus informaatioteknologiasta on nostanut niihin liittyvät kyberriskit viime vuosina nopeasti yhdeksi merkittävimmistä riskeistä. Kyberriskit ovat yhä monimuotoisempia ja perinteisten tietovuotojen, tietomurtojen ja palvelunestohyökkäysten lisäksi on tullut vakavana uhkana esimerkiksi kybersodankäynti, joka voi lamaannuttaa kokonaisen valtion kriittisen infrastruktuurin. Yhdeksi merkittävimmistä kyberriskeistä on nostettu riippuvuus, koska eri laitteet, ihmiset ja organisaatiot ovat koko ajan yhdistetty toisiinsa verkon välityksellä. Kyberriskin toteutuessa seuraukset voivat levitä nopeasti maailmanlaajuisiksi. (World Economic Forum 2017) Myös vakuutusyhtiö Allianzin (2016) tekemissä tutkimuksissa yritykset ovat nostaneet kyberriskit kolmen merkittävimmän liiketoimintaan liittyvän riskin joukkoon.

Kyberriskien taloudelliset vaikutukset ovat huomattavan suuria. Kyberriskien maailmanlaajuisten kustannusten arvioidaan olevan yli 100 miljardia Yhdysvaltain dollaria[1] vuosittain. Arviot maailmanlaajuisista kustannuksista vaihtelevat huomattavasti, koska kyberriskit aiheuttavat suorien vahinkojen lisäksi epäsuoria vahinkoja, kuten maineen heikkenemistä, joita ei

[1] Kansainvälisessä tutkimuskirjallisuudessa kyberriskien kustannukset ilmoitetaan tavanomaisesti Yhdysvaltain dollareina. Myös tässä tutkielmassa kustannusten valuuttayksikkönä käytetään Yhdysvaltain dollaria.

kaikissa arvioissa ole otettu huomioon. Yksittäisen tietomurron keskimääräiseksi kustannukseksi on arvioitu 2,1–3,8 miljoonaa dollaria. (Eling & Schnell 2016) Myös maantieteellinen alue ja yrityksen toimiala vaikuttavat huomattavasti kyberriskien taloudellisiin vaikutuksiin. Esimerkiksi Yhdysvalloissa tietomurron kustannukset ovat yli kolminkertaiset verrattuna Intiaan, missä tietosuojaan liittyvät vaatimukset eivät ole yhtä tiukkoja kuin Yhdysvalloissa. Vastaavasti terveydenhuoltoalalla toimivan yrityksen tietomurron kustannukset ovat lähes kaksinkertaiset keskimääräiseen verrattuna. (Ponemon Institute 2017)

Erityisesti riippuvuus ulkopuolisista palveluntarjoajista aiheuttaa merkittävän riskin. Yrityksillä on usein paljon erilaisia yhteistyökumppaneita eli kolmansia osapuolia, jotka voivat olla esimerkiksi alihankkijoita, tietojärjestelmien ja -palveluidentarjoajia sekä lakiasiaintoimistoja, joiden kanssa he jakavat yhteisiä tietojärjestelmiä tai käsittelevät toistensa luottamuksellisia tietoja. Suurilla yrityksillä tällaisia yhteistyökumppaneita voi olla jopa kymmeniä tuhansia. Merkittävän tästä ongelmasta tekee se, että yritykset ulkoistavat toimintoja ja ottavat samalla riskejä, joita ne eivät välttämättä voi hallita tai joiden suuruutta ne eivät voi arvioida. (Keegan 2014)

Kolmanteen osapuoleen kohdistuneista tietomurroista suurimman mediahuomion on viime vuosina saanut yhdysvaltalaiseen vähittäiskauppaketju Targetiin vuonna 2013 kohdistunut tietomurto, jossa 40 miljoonan asiakkaan maksukorttitiedot sekä 70 miljoonan asiakkaan henkilötiedot joutuivat rikollisten haltuun. Tietomurron alkuperäisenä kohteena oli Targetin pieni alihankkija, jonka heikkoa tietoturvaa hyödyntämällä rikolliset pääsivät Targetin asiakastietojärjestelmiin. Tietomurron kustannuksiksi arvioitiin noin 250 miljoonaa dollaria. (Hardy 2014, 1–5) Tietomurrot eivät koske pelkästään henkilö- ja maksukorttitietoja, vaan kohteena voivat olla mitkä tahansa salassa pidettävät tiedot, esimerkiksi yrityssalaisuudet. Kansainväliset kyberrikolliset hakkeroivat Yhdysvalloissa kolmen merkittävimmän talousalan uutistoimiston tietojärjestelmät ja saivat käsiinsä 150 000 vielä julkaisematonta lehdistötiedotetta koskien yritysten tuloksia, liikevaihtoja ja muita salassa pidettäviä tietoja. Rikolliset toimittivat salassa pidettävät tiedot sijoittajille, jotka ansaitsivat noin 30 miljoonan dollarin hyödyn salassa pidettävää tietoa käyttämällä. (U.S. Dept. of Justice 2016) Myös tässä tapauksessa varsinainen tietomurto ei kohdistunut suoraan yrityksen IT-järjestelmiin, vaan kolmanteen osapuoleen eli tässä tapauksessa uutistoimistoon.

Kolmansien osapuolten aiheuttamat kyberriskit ovat nousseet vasta muutaman viime vuoden aikana erilaisten tutkimusten ja konsulttiyhtiöiden raporteissa merkittäväksi teemaksi. Yhdysvalloissa tehdyissä riippumattomissa tutkimuksissa yritysten riskienhallintajohtajista 75 prosenttia arvioi kolmansista osapuolista muodostuvan kyberriskin vakavaksi ja 70 prosenttia heistä arvioi riskin kasvavan heidän organisaatiossaan tulevaisuudessa. Kyberhyökkäysten, uudenlaisten uhkakuvien ja teknologioiden, kuten esineiden internetin, on arvioitu muodostavan merkittävimmän haasteen kolmansien osapuolten aiheuttamissa kyberriskeissä. Kolmansiin osapuoliin liittyvän kyberriskin vakavuudesta huolimatta vain alle kolmasosa tutkimukseen vastanneista yrityksistä pitää riskienhallinnan yhtenä päätavoitteena hallita ja estää kolmansista osapuolista aiheutuvia kyberriskejä. Useimmiten syynä tähän ovat tiedon ja käytäntöjen puute. (Ponemon Institute 2016)

Kyberriskejä voidaan hallita useilla eri tavoilla, joista yksi on riskin siirtäminen vakuuttamalla. Erilaisilla omaisuus- ja vastuuvakuutuksilla on vakuutettu perinteisiä vahinkoriskejä, mutta ne kattavat useimmiten vain fyysiselle omaisuudelle, esimerkiksi tuotantolaitteille ja kiinteistöille, aiheutuneita vahinkoja. Omaisuus- ja vastuuvakuutukset eivät useimmiten kata kyberriskejä tai niissä ei ole selkeästi ilmaistu, kattavatko ne myös kyberriskejä. Viime vuosien aikana ovat yleistyneet erityisesti Yhdysvalloissa erilliset kybervakuutukset, jotka kattavat kyberriskien aiheuttamia aineettomia vahinkoja. Tällä hetkellä kybervakuutusmarkkinat ovat vielä melko pienet, koska vakuutustuotteet ovat verrattain uusia ja tuntemattomia. Kybervakuutusmarkkinat ovat Yhdysvalloissa huomattavasti suuremmat ja kehittyneemmät kuin Euroopassa. Todennäköisin syy on Yhdysvalloissa pidempään voimassa ollut sääntely, joka velvoittaa ilmoittamaan tietovuodoista, jolloin myös yritysten kiinnostus tietosuojaa ja kyberriskien hallintaa kohtaan on ollut suurempaa. (Eling & Schnell 2016)

Yhdysvaltojen osuus kansainvälisestä kybervakuutusmarkkinasta on noin 90 prosenttia. Vuonna 2015 kybervakuutusten maksutulo oli noin 1,5 miljardia dollaria. Erityisesti vähittäiskaupan, finanssialan ja terveydenhoitoalan yritykset ovat kiinnostuneita kybervakuutuksista. Edellä mainittuihin aloihin liittyy olennaisena osana asiakkaiden luottamuksellisten tietojen käsittely. Euroopassa kybervakuutusten vuosittainen maksutulo vuonna 2015 oli noin 135 miljoonaa dollaria. Euroopassa vakuutusmaksutulon odotetaan nousevan lähivuosina merkittävästi, sillä vuonna 2018 alkaa EU:n uuden tietosuoja-asetuksen soveltaminen, mikä asettaa

yrityksille tiukempia vaatimuksia noudattaa säännöksiä ja huolehtia paremmasta tietoturvasta. (Aon 2017) Vakuutusyhtiö Allianz (2015) arvioi kansainvälisten kybervakuutusmarkkinoiden kasvavan vuoteen 2025 mennessä yli 20 miljardiin dollariin vuodessa.

Kuten edellä on esitetty, kyberriskit ja erityisesti kolmansista osapuolista aiheutuvat kyberriskit on tunnistettu merkittäväksi riskiksi, mutta niiden arvioimiseen ja hallitsemiseen on kohdistettu vähän resursseja. Sen vuoksi kolmansista osapuolista aiheutuvat kyberriskit ovat mielenkiintoinen, ajankohtainen ja perusteltu tutkimuskohde. Kyberriskejä voidaan hallita useilla eri keinoilla ja kybervakuutus on vain yksi keino muiden joukossa. Kyberturvallisuuteen käytetään maailmanlaajuisesti noin 100 miljardia dollaria vuosittain, mistä kybervakuutusmarkkinat kattavat vain kaksi prosenttia. Yleisin riskienhallintakeino on riskin vähentäminen, joka tarkoittaa esimerkiksi diagnostiikkaa sekä laitteisto- ja ohjelmistoturvallisuuden parantamista. (Aon 2017) Kolmansista osapuolista aiheutuvat kyberriskit ovat tyypillisesti harvinaisia mutta kooltaan suuria. Tämän tyyppisiä riskejä on perinteisesti hallittu vakuuttamalla, minkä vuoksi tässä tutkielmassa syvennytään tarkastelemaan kybervakuutusta riskienhallintakeinona.

1.2 Tavoitteet, tutkimusongelmat ja rajaukset

Tämä tutkielma keskittyy tarkastelemaan kyberriskejä ja kybervakuuttamista. Tutkielman tavoitteena on selvittää, kuinka kolmansista osapuolista aiheutuvia kyberriskejä voidaan tunnistaa ja arvioida. Lisäksi tavoitteena on selvittää, miten pilvipalveluiden käyttäminen vaikuttaa yrityksen kyberturvallisuuteen kokonaisuutena. Tavoitteena on myös selvittää, kuinka Suomessa toimivien vahinkovakuutusyhtiöiden tarjoamat kybervakuutukset kattavat kolmansien osapuolten aiheuttamia kybervahinkoja.

Tutkielmassa selvitetään vastauksia kolmeen tutkimusongelmaan:

1) Miten kolmansista osapuolista aiheutuvia kyberriskejä voidaan tunnistaa ja arvioida?
2) Kuinka pilvipalvelut vaikuttavat yrityksen kyberturvallisuuteen?
3) Miten kybervakuutus kattaa kolmansien osapuolten aiheuttamia kybervahinkoja?

Ensimmäisen tutkimusongelman tarkoitus on selvittää, miten kolmansista osapuolista aiheutuvia kyberuhkia voidaan tunnistaa ja miten niistä muodostuvien kyberriskien suuruutta voidaan arvioida. Kolmansista osapuolista aiheutuvien kyberriskien arviointiin ei toistaiseksi ole olemassa tutkimuksellista tietoa, joten ensimmäisen tutkimusongelman tavoitteena on luoda yleiskuva, millaisilla menetelmillä kolmansista osapuolista aiheutuvia kyberriskejä voidaan arvioida ja poikkeavatko ne muiden kyberriskien arviointiin käytetyistä menetelmistä. Lisäksi ensimmäisellä tutkimusongelmalla kartoitetaan, millaisia kyberuhkia, haavoittuvuuksia ja eri toimijoita kolmansista osapuolista aiheutuvien kyberriskien taustalla on.

Toinen tutkimusongelma syventyy kolmansien osapuolien yhteen erityismuotoon, pilvipalveluihin. Niiden suosio on kasvanut viime vuosina nopeasti, ja ne aiheuttavat yrityksille uudenlaisia riskejä. Toisen tutkimusongelman tarkoituksena on selvittää, miten pilvipalveluiden käyttäminen vaikuttaa yrityksen kyberturvallisuuteen kokonaisuutena. Tutkimusongelmaa käsiteltäessä syvennytään erilaisiin tapauksiin, joissa pilvipalveluiden käyttäminen voi joko parantaa tai heikentää yrityksen kyberturvallisuutta.

Tutkielman kolmas tutkimusongelma keskittyy tarkastelemaan yhtä riskienhallintakeinoa, kybervakuutusta. Sen tarkoituksena on selvittää, miten kybervakuutukset kattavat vastuu- ja riippuvuuskeskeytysvahinkoja, kun kolmas osapuoli aiheuttaa kybervahingon. Vastuuvahinkojen korvattavuuden osalta tarkastelemme lisäksi, kuinka kybervakuutukset kattavat EU:n tietosuoja-asetuksen määrittämää korvausvelvollisuutta rekisteröidyille, kun vahingon on aiheuttanut rekisterinpitäjän lukuun henkilötietojen käsittelyä tekevä organisaation ulkopuolinen henkilötietojen käsittelijä. EU:n tietosuoja-asetuksen velvoitteiden laiminlyömisestä voi seurata taloudellisia seuraamusmaksuja eli sanktioita, joiden korvattavuutta kybervakuutuksesta tarkastellaan tässä yhteydessä.

Tutkielman nimi ja tutkimusongelmat rajaavat tutkittavaa ilmiötä itsessään. Tutkielma keskittyy tarkastelemaan kolmansista osapuolista aiheutuvien kyberriskien arvioimista ja riskin siirtämistä kybervakuutuksella. Kyberriskien hallinta keskittyy pääasiassa riskin vähentämiseen, joka tapahtuu esimerkiksi kyberturvallisuutta parantamalla. Riskin siirtäminen kybervakuutuksella on tällä hetkellä vielä pieni osa kyberriskien hallintaa, mutta sen osuuden odotetaan kasvavan tulevaisuudessa. Tässä tutkielmassa keskitytään riskienhallintakeinoista tarkastele-

maan vain kybervakuutusta, koska kolmansista osapuolista aiheutuvat kyberriskit ovat useimmiten yrityksen riskienhallinnan ulottumattomissa, ja ne aiheuttavat toteutuessaan usein suuria vahingonkorvauksia tai keskeytysvahinkoja. Tällaiset vahingot ovat tyypillisesti vakavuudeltaan suuria ja todennäköisyydeltään pieniä, joihin varaudutaan tavallisesti vakuuttamalla.

Tutkielmassa on kaksi keskeistä rajausta: tarkasteltava kohderyhmä ja maantieteellinen alue. Tutkielmassa tarkasteltavaksi kohderyhmäksi on valittu yritykset, koska ne hallinnoivat suuria määriä henkilötietoja ja muita salassa pidettäviä tietoja, joiden väärinkäytöstä ne ovat vastuussa. Kyberriskit ovat luonteeltaan globaaleja; ne voivat aiheutua mistä päin tahansa ja leviävät nopeasti verkon välityksellä, joten kyberriskien lähteitä ei rajata maantieteellisesti. Sitä vastoin lainsäädännöllisestä näkökulmasta käsittely rajataan Euroopan unioniin. Eri alueilla on voimassa erilainen lainsäädäntö, joten käsittelyn yksinkertaisuuden vuoksi tässä tutkielmassa tarkastellaan koko Euroopan unionin alueella voimassa olevaa tietosuoja-asetusta.

1.3 Keskeiset käsitteet

Kyberriski on mikä tahansa riski, joka aiheuttaa taloudellista vahinkoa, häiriöitä tai mainehaittoja informaatioteknologian toimimattomuuden vuoksi. Kyberriski voi aiheutua esimerkiksi tahallisen tietomurron, tahattoman tietovuodon tai tietojärjestelmiin liittyvän operatiivisen riskin seurauksena. Kyberriski ei välttämättä kohdistu suoraan organisaatioon itseensä, vaan se voi kohdistua myös kolmanteen osapuoleen, esimerkiksi yrityksen toimitusketjuun. (Institute of Risk Management 2014)

Kyberturvallisuus on kyberavaruuden, sähköisen tiedon, informaatio- ja kommunikaatioteknologian sekä sen käyttäjien suojaamista. Se kattaa sekä yksityishenkilöiden että yhteiskuntien aineettoman ja aineellisen omaisuuden, joka on haavoittuva kyberavaruudesta tuleville uhille. Kyberturvallisuus on käsitteenä laajempi kuin tietoturvallisuus, joka kattaa vain tietoon liittyvän luottamuksellisuuden, eheyden ja saatavuuden turvaamisen. Kyberturvallisuus laajentuu tieto-omaisuuden lisäksi käsittämään myös kyberavaruuden, informaatio- ja kommunikaatioteknologian, sen käyttäjät ja muun kuin tietoon liittyvän omaisuuden. (von Solms & van Niekerk 2013)

Uhka on jokin mahdollisesti toteutuva vahingollinen asia, joka uhkaa tiettyä organisaatiota tai sen osaa. Kyberturvallisuutta koskeville uhille on ominaista niiden abstrakti ja vaikeasti hahmotettava luonne. Kyberturvallisuutta vaarantavat uhat voivat olla organisaation ulkopuolisia tai niiden sisäisiä. (Limnéll, Majewski & Salminen 2014, 105–108)

Haavoittuvuus tarkoittaa heikkoutta, joka antaa mahdollisuuden heikentää tietyn järjestelmän tietoturvallisuutta tai toimintavarmuutta. Jotta haavoittuvuus voi muodostua, pitää järjestelmässä olla vika tai heikkous, toimijalla tai hyökkääjällä pitää olla pääsy kyseiseen järjestelmään ja lisäksi sillä pitää olla kyky käyttää kyseistä vikaa tai heikkoutta hyväkseen. (Limnéll ym. 2014, 110–111)

Kolmas osapuoli on mikä tahansa yritys, organisaatio tai yksityishenkilö, jonka kanssa yritys tekee liiketoimintaa. Kolmannet osapuolet voivat olla esimerkiksi tavarantoimittajia, alihankkijoita, yhteistyökumppaneita, välittäjiä, jälleenmyyjiä ja asiakkaita. Kolmannet osapuolet voivat olla yrityksen arvoketjussa heitä ennen ja heidän jälkeen. (OCC 2013)

Kybervakuutus on yksi riskienhallinnan keino, jolla riski voidaan siirtää. Kybervakuutus kattaa menetyksiä tietovuotojen ja kyberavaruudesta tulevien uhkien varalta. Kybervakuutus kattaa yleensä ensimmäiselle ja kolmannelle osapuolelle aiheutuneita vahinkoja. Ensimmäiselle osapuolelle eli vakuutuksenottajalle korvataan taloudellisia vahinkoja esimerkiksi tietomurron tai palvelunestohyökkäyksen seurauksena. Kolmansille osapuolille korvataan kuluja vastuuvahinkona, kun yritys on korvausvelvollinen asiakkailleen heidän luottamuksellisten tietojen joutuessa ulkopuolisten haltuun. (Gordon, Loeb & Sohail 2003)

Vastuuvahinko on toiselle aiheutunut vahinko, josta yritys on voimassa olevan oikeuden mukaan korvausvelvollinen. Vastuuvakuutuksella voidaan vakuuttaa toiselle aiheutunutta vahinkoa. Vastuuvakuutus kattaa vain toiselle aiheutetun vahingon, eikä siitä korvata vakuutuksenottajalle itselleen aiheutunutta vahinkoa. (Rantala & Kivisaari 2014, 565)

Riippuvuuskeskeytysvahinko voi aiheuttaa liiketoiminnan keskeytymisen yrityksen sopimuskumppania kohdanneen vahingon seurauksena. Riippuvuuskeskeytysvakuutuksella voidaan vakuuttaa suorassa liikesuhteessa olevan asiakkaan tai alihankkijan toiminnasta aiheutuneen vahingon aiheuttama riippuvuuskeskeytysriski. (Rantala & Kivisaari 2014, 575)

1.4 Tutkimusmenetelmät ja -aineisto

Tämä tutkielma on kvalitatiivinen eli laadullinen tutkimus, jossa aineistoa tarkastellaan kokonaisvaltaisesti. Laadullinen tutkimus lähtee liikkeelle ajatuksesta, jonka tarkoituksena on kuvata todellista elämää ja johon sisältyy ajatus todellisuuden moninaisuudesta ja monisuuntaisista suhteista. Laadullisessa tutkimuksessa ilmiöitä pyritään tutkimaan mahdollisimman kokonaisvaltaisesti ja tavoitteena on löytää tai paljastaa tosiasioita eikä niinkään todentaa jo olemassa olevia väittämiä. Laadullisessa tutkimuksessa on tunnistettavissa useita piirteitä, joita ovat muun muassa tutkimuksen kokonaisvaltainen ja luonnollisissa tilanteissa tehtävä tiedonhankinta, ihmisen suosiminen tiedon keruun instrumenttina, induktiivinen analyysi eli lähtökohtana ei ole teorian tai hypoteesien testaaminen vaan aineiston monitahoinen ja yksityiskohtainen tarkastelu, laadullisten metodien käyttö aineiston hankinnassa, kohdejoukon tarkoituksenmukainen valinta, tutkimussuunnitelman muotoutuminen tutkimuksen edetessä ja tapauksien käsittely ainutlaatuisina. (Hirsjärvi, Remes & Sajavaara 2009, 160–164)

Tutkimusmenetelmän valinnan tulisi seurata tutkimusongelmasta. Laadullisessa tutkimuksessa tutkimusongelma saattaa muuttua tutkimuksen edetessä ja sen vuoksi tutkimusongelmasta käytetään laadullisessa tutkimuksessa usein nimitystä tutkimustehtävä, joka asetetaan yleisellä tasolla. (Hirsjärvi ym. 2009, 125–126) Tämän tutkielman aihepiireistä kyberriskit ja erityisesti kolmansien osapuolien aiheuttamat kyberriskit ovat vielä melko tuntematon tieteenala, minkä vuoksi tutkimusongelmat muotoiltiin avoimiksi ja niille annettiin mahdollisuus muuttua tutkimuksen edetessä. Lisäksi uusien teemojen nouseminen esille on mahdollista, sillä laadullinen tutkimusmenetelmä mahdollistaa tutkijan paljastaa odottamattomia seikkoja, ja tutkittavien näkökulmat sekä mielipiteet pääsevät esille (Hirsjärvi ym. 2009, 164). Edellä esitettyjen seikkojen vuoksi on perusteltua, että tämän tutkielman tutkimusmenetelmäksi on valittu laadullinen tutkimus.

Tutkimuksen tarkoitusta luonnehditaan yleensä neljän piirteen perusteella, joita ovat kartoittava, selittävä, kuvaileva ja ennustava. Yhteen tutkimukseen voi sisältyä useampi kuin yksi tarkoitus ja se voi myös muuttua tutkimuksen edetessä. Tämän tutkimuksen tarkoitus on kartoittava, missä selvitetään vähän tunnettuja ilmiöitä ja etsitään uusia näkökulmia. (Hirsjärvi ym. 2009, 138–139) Koska aihepiiriä ei ole aiemmin tutkittu, voidaan kartoittavalla tutkimuksella

löytää uusia näkökulmia kolmansista osapuolista aiheutuviin kyberriskeihin ja niiden arvioimiseen.

Hirsjärvi ym. (2009, 191–192) jakavat tutkimuksen aineistonkeruun menetelmät neljään perusmenetelmään: kyselyyn, haastatteluun, havainnointiin ja dokumentteihin. Tutkimuksessa voidaan käyttää yhtä tai useampaa aineistonkeruun perusmenetelmää. Aineistonkeruun perusmenetelmän tulisi soveltua mahdollisimman hyvin tutkittavaan ilmiöön ja tutkimusongelmaan. Haastattelu on soveltuva menetelmä, kun kyseessä on vähän kartoitettu ja tuntematon alue, tutkimuksen aihe tuottaa monitahoisesti ja moniin suuntiin viittaavia vastauksia ja kun halutaan syventää saatavia tietoja sekä pyytää esitettyjen mielipiteiden perusteluja. Haastattelu on joustava menetelmä, ja se luo mahdollisuuden suunnata tiedonhankintaa haastattelutilanteessa. (Hirsjärvi & Hurme 2008, 34–35) Kuten aiemmin tässä luvussa on todettu, tämän tutkielman aihepiiri on vähän kartoitettu, minkä vuoksi aineistonkeruun menetelmäksi on valittu haastattelu.

Tutkimushaastattelun lajit jaetaan yleensä kolmeen ryhmään: strukturoituun eli lomakehaastatteluun, puolistrukturoituun eli teemahaastatteluun ja strukturoimattomaan eli avoimeen haastatteluun. Teemahaastattelulle on ominaista, että haastattelun aihe ja näkökulma on määritelty ennalta. Myös kysymykset on määritelty ennalta, mutta haastattelija voi vaihdella niiden sanamuotoja sekä järjestystä. Vastausvaihtoehtoja ei ole määritelty ennalta, vaan haastateltavat voivat vastata omin sanoin. Teemahaastattelussa on olennaista, että haastattelu etenee keskeisten teemojen varassa ja haastateltavien tulkinnat ja heidän asioille antamat merkitykset ovat keskeisiä. (Hirsjärvi & Hurme 2008, 47–48) Tässä tutkielmassa tutkimushaastattelun lajina käytetään teemahaastattelua, koska se soveltuu parhaiten tutkittavaan ilmiöön ja tutkimusongelmaan. Ilmiö on uusi ja tuntematon, mutta aihepiiri on selkeästi rajattu kolmansista osapuolista aiheutuviin kyberriskeihin ja niiden arviointiin, joten haastattelujen teema ja alustavat kysymykset voidaan määritellä ennalta. Teemahaastattelu soveltuu tutkittavaan ilmiöön paremmin kuin lomakehaastattelu, koska lomakehaastattelulla voisi jäädä olennaisia vastauksia saamatta. Haastattelun edetessä teemahaastattelu antaa mahdollisuuden tarkentaa ja syventää sekä kysymyksiä että vastauksia.

Tämän tutkielman empiirinen aineisto hankittiin asiantuntijoiden teemahaastatteluilla. Jo tutkimuskysymyksiä asetettaessa tunnistettiin, että tutkielman aihepiiri jakautuu kyberturvallisuuteen ja kybervakuuttamiseen. Toisistaan poikkeavat aihepiirit aiheuttavat sen, että haastatteluihin soveltuvilla henkilöillä ei välttämättä ole laajaa asiantuntemusta molemmista aihepiireistä. Sen vuoksi haastateltavien henkilöiden kartoittamisessa päädyttiin etsimään asiantuntijoita, joilla on laaja asiantuntemus joko kyberturvallisuudesta tai kybervakuuttamisesta. Edellä mainittujen aihepiirien painoarvo tutkimuskysymysten valossa jakautuu lähes tasan, joten tavoitteeksi asetettiin, että puolet haastateltavista ovat kyberturvallisuusasiantuntijoita ja puolet kybervakuutusasiantuntijoita. Soveltuvien haastateltavien kartoittaminen aloitettiin syksyllä 2017 ja heitä lähestyttiin sähköpostitse. Heille esiteltiin tutkielman aihe ja haastatteluissa käytävät aihepiirit. Ennen haastatteluista sopimista jokaiselta haastateltavalta varmistettiin, tuntevatko he syvällisesti kyseisen aihepiirin ja ovatko he soveltuvia henkilöitä osallistumaan haastatteluun.

Tätä tutkielmaa varten haastateltiin kuutta henkilöä: kolmea kyberturvallisuusasiantuntijaa ja kolmea kybervakuutusasiantuntijaa. Haastatteluiden kohteeksi valikoitui kyberturvallisuuden alalta henkilöitä Jyväskylän yliopiston kyberturvallisuuden ohjelmasta, kyberturvallisuuspalveluita tarjoavasta Insta DefSecistä ja yrityksen kokonaisturvallisuuden näkökulmasta Insta Groupista. Kybervakuutusalan asiantuntijoista haastatteluiden kohteeksi valikoitui henkilöitä kybervakuutusta Suomessa tarjoavista yhtiöistä OP Vakuutuksesta ja If Vahinkovakuutuksesta sekä vakuutusmeklariyhtiö Aonista. Haastateltaviksi valittiin henkilöitä, jotka työskentelevät läheisesti joko kyberturvallisuuden tai kybervakuuttamisen parissa, mikä on edellytys tutkielman luotettavuuden ja onnistumisen kannalta. Tutkielmassa ei ole käytetty haastateltavien nimiä, mutta heidän taustansa, asemansa ja edustamansa organisaatio on tuotu esille. Haastateltavan tausta ja asema voivat vaikuttaa hänen näkemyksiinsä, joten niiden tuominen esille lisää tutkielman objektiivisuutta. Haastateltaville tuotiin esille, että haastattelut eivät ole täysin anonyymejä ja käsiteltävät aihepiirit ovat sellaisia, joita voidaan käsitellä julkisesti. Tutkielman aihepiirin kannalta täydellinen anonymiteetti ei olisi tuonut lisää tietoa, koska aihepiirin luonteesta johtuen se ei yksinomaan koske yritysten luottamuksellista ja sisäistä tietoa, vaan alaa yleisesti koskevia käytäntöjä.

Laadullisessa tutkimuksessa aineiston riittävästä määrästä ei voida tehdä yksiselitteistä määritelmää. Aineiston kattavuutta tulisi tarkastella aineiston koon, kyllääntymisen, rajauksen ja yleistämisen näkökulmista. Laadullisessa tutkimuksessa tapausten määrä perustuu yleensä suhteellisen pieneen määrään, eikä aineiston koolla ole välitöntä yhteyttä tutkimuksen onnistumiseen. Aineiston voidaan katsoa olevan riittävä, kun uudet tapaukset eivät tuota tutkimuksen kannalta uutta ja olennaista tietoa. Laadullisessa tutkimuksessa pieni tapausmäärä on perusteltua, koska aineisto tulee aluksi rajata mahdollisimman tarkasti, jotta siitä voidaan rakentaa eheä tulkinta. Lisäksi aineistoa voidaan myöhemmin laajentaa ja kerätä lisää. Laadullisen tutkimuksen onnistumiselle on keskeistä sen kuvaus ja monipuolinen erittely, eikä sen tarkoituksena ole tehdä samalla tavalla empiirisesti yleistäviä johtopäätöksiä kuin määrällisessä tutkimuksessa. (Eskola & Suoranta 1998, 46–49)

Ennen aineiston hankkimista ei ollut määritelty kiinteää lukumäärää haastateltavista henkilöistä, koska aihepiiristä oli ennalta hyvin vähän tietoa ja ei ollut varmuutta, kuinka kattavia vastauksia haastatteluissa saadaan. Empiiristä aineistoa varten valittiin aluksi kuusi haastateltavaa, jonka jälkeen aineistoa analysoitiin ja oltiin tarvittaessa valmiita laajentamaan empiiristä aineistoa. Tutkielmaa varten toteutetut kuusi asiantuntijahaastattelua todettiin riittäviksi, koska haastatteluiden edetessä todettiin, että haastateltavien mielipiteet ovat pieniä poikkeuksia lukuun ottamatta samansuuntaisia. Aineisto todettiin kyllääntyneeksi, eivätkä uudet haastateltavat olisivat tuoneet tutkielman kannalta uutta ja olennaista tietoa.

Hirsjärven ym. (2009, 221) mukaan koko tutkielman kannalta olennaisinta on hankitun aineiston analyysi, tulkinta ja johtopäätösten teko, mihin tähdätään tutkimusta aloitettaessa. Aineistoa voidaan analysoida monin eri tavoin ja pääperiaate on, että valitaan sellainen analysointitapa, joka tuo parhaiten vastauksen tutkimusongelmaan. Tavallisesti laadullista aineistoa analysoidaan teemoittelun, tyypittelyn, sisällönanalyysin, diskurssianalyysin ja keskustelunanalyysin menetelmillä. (Hirsjärvi ym. 2009, 224) Tämän tutkielman empiirisen haastatteluaineiston analyysimenetelmänä käytetään sisällönanalyysiä, jolla analysoidaan dokumentteja systemaattisesti ja objektiivisesti. Sisällönanalyysillä pyritään saamaan tutkittavasta ilmiöstä kuvaus tiivistetyssä ja yleisessä muodossa kadottamatta sen sisältämää informaatiota.

(Tuomi & Sarajärvi 2018, 86, 90) Sisällönanalyysi soveltuu tässä tutkielmassa tutkittavaan ilmiöön, koska aineiston analysoinnissa keskitytään haastattelujen asiasisältöön eikä kielellisten merkityksien analysointiin.

Sisällönanalyysi voidaan jakaa aineistolähtöiseen, teoriaohjaavaan ja teorialähtöiseen analyysiin. Tässä tutkielmassa analyysimenetelmänä käytetään teoriaohjaavaa analyysiä, jossa teoria toimii analyysin apuna, mutta analyysi ei pohjaudu yksinomaan teoriaan. Teoriaohjaavassa analyysissä aikaisemman tiedon merkitys tulee tunnistaa, mutta analyysi ei ole teoriaa testaava, vaan sen tarkoitus on avata uusia ajatuksia. Teoriaohjaavassa analyysissä on usein kyse abduktiivisesta päättelystä, jossa tutkija pyrkii yhdistelemään aineistolähtöistä analyysiä ja valmiita malleja. (Tuomi & Sarajärvi 2018, 80–81) Tutkielman aihepiiriin ei ole sovellettavissa jo olemassa olevaa teoriaa, jota tässä tutkielmassa voitaisiin testata, vaan tarkoituksena on löytää uutta tietoa aiempaan teoreettiseen tietoon nojautuen. Aineistosta löydetyille havainnoille haetaan tukea esitetystä teoriasta ja ne pyritään sitomaan laajempaan kokonaisuuteen tutkittavasta ilmiöstä.

1.5 Aikaisemmat tutkimukset

Kolmansien osapuolten aiheuttamat kyberriskit ja niiden arvioiminen ovat uusi aihe, ja suoraan vastaavasta aiheesta ei ole tehty akateemisia tutkimuksia Suomessa eikä kansainvälisesti. Sen sijaan kyberriskeistä ja kybervakuuttamisesta on jo olemassa runsaasti akateemisia julkaisuja, mutta niissä ei ole erityisesti käsitelty kolmansista osapuolista aiheutuvia kyberriskejä. Aihetta käsittelevää kirjallisuutta on julkaistu 2000-luvun alusta lähtien, mutta vuodesta 2010 alkaen kirjallisuuden määrä on kasvanut moninkertaisesti. Gordon ym. (2003) tutkivat ensimmäisten joukossa kyberriskien hallintaa ja kybervakuutusta. He tutkivat ensimmäisiä kybervakuutustuotteita, niiden kattavuutta ja arvioivat kybervakuutuksen hyödyllisyyttä. He tutkivat myös, kuinka resurssit tulisi jakaa kyberturvallisuuden ja kybervakuutuksen välillä. He päätyivät lopputulokseen, että mikä tahansa kyberturvallisuuteen käytettävä rahamäärä ei voi estää kaikkia kyberriskejä, joten jäljelle jäävän riskin siirtämiselle kybervakuutuksella on perusteita.

Biener, Eling ja Wirfs (2015) ovat tutkineet kattavasti kyberriskien vakuutuskelpoisuutta. Heidän tutkimustensa mukaan kybervakuuttamisen ongelmia ovat vahingon ennustamisen vaikeus, informaation epäsymmetria ja empiirisen tiedon puute. Heidän mukaansa kybervakuutus tulee kuitenkin kehittymään tulevaisuudessa, kun poolit kasvavat suuremmiksi ja kyberriskeistä ja vahingoista saadaan enemmän dataa. Heidän mukaansa kybervakuutus lisää yritysten tietoisuutta kyberriskeistä ja lisää heidän panostuksiaan kyberturvallisuuteen.

Kolmannet osapuolet voivat olla esimerkiksi yrityksen toimitusketjun jäseniä. Windelberg (2016) on tutkinut toimitusketjuista aiheutuvia kyberriskejä ja määrittänyt tavoitteita niiden hallitsemiseksi. Hän on tuonut esille toimitusketjun osien tärkeyden, koska yksi toimitusketjun osa voi aiheuttaa merkittävän kyberriskin yritykselle, joka tarjoaa palveluitaan loppukäyttäjille. Erityisen riskin ne muodostavat kriittistä infrastruktuuria palvelevilla sektoreilla. Nishat Faisal, Banwet ja Shankar (2007) sekä Sharma ja Routroy (2016) ovat tutkineet kyberriskejä toimitusketjuissa ja rakentaneet alustavia malleja arvioida toimitusketjuista aiheutuvien kyberriskien taloudellisia vaikutuksia. Myös Boyson (2014) on tutkinut niin sanottuja kybertoimitusketjuja ja niihin liittyviä kyberriskejä. Hän on tuonut esille, että kybervakuutuksilla siirretään vakuutusyhtiöille toimitusketjuista aiheutuvia kyberriskejä, mutta vakuutusyhtiöillä ei ole vielä luotettavia menetelmiä mitata toimitusketjuista aiheutuvia kyberriskejä, joten vakuutusyhtiöiden kantamat riskit voivat olla oletettuja huomattavasti suuremmat.

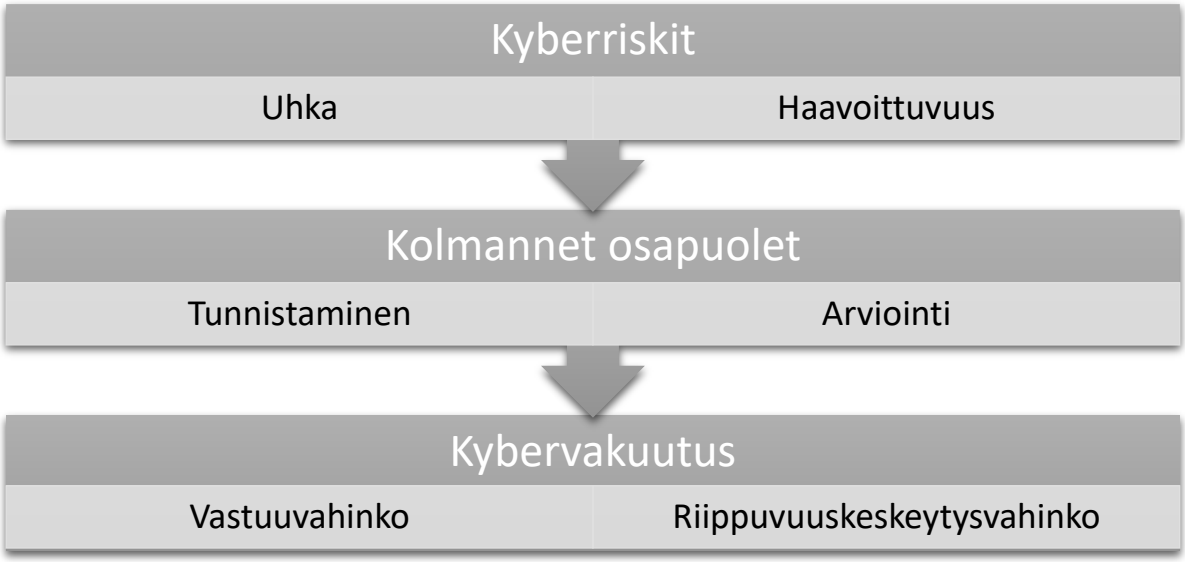
Kaiken kaikkiaan tutkimustieto tämän tutkielman aihepiiristä on varsin niukkaa, minkä vuoksi tutkielman teoreettisessa osuudessa yhdistetään aiemman tutkimustiedon eri osa-alueita soveltuvin osin. Tutkielma nojaa vahvasti empiiriseen aineistoon, koska vastaavaa tutkimusta ei ole toistaiseksi tehty.

1.6 Teoreettinen viitekehys

Perinteisesti hyvä tutkimus lähtee teoriasta ja jälleen palaa siihen. Tutkimuksen ongelmat johdetaan teoriasta, ja empirian avulla hankittujen vastausten jälkeen katsotaan, tukevatko ne teoriaa. Tutkimuksen teorialla on kaksi tehtävää: teoria keinona ja teoria päämääränä. Keinona teoria auttaa tutkimuksen tekemistä. Kun teoria on päämääränä, tutkimuksen tavoitteena on teorian kehittäminen edelleen. Empiirisessä tutkimuksessa teoriaa hyödynnetään

tavanomaisesti keinona. (Eskola & Suoranta 1998, 60) Tämä tutkielma on empiirinen, joten teoriaa hyödynnetään keinona, jolla selitetään uusia ilmiöitä.

Laadullinen tutkimus edellyttää kahdenlaisia teorioita. Ensin tarvitaan taustateoria, jota vasten aineistoa tarkastellaan. Lisäksi tarvitaan tulkintateoria, joka ohjaa tutkijan valintoja ja sitä mitä hän aineistosta etsii. (Eskola & Suoranta 1998, 60–61) Edellä mainittujen teorioiden jäsentämiseen voidaan soveltaa teoreettista viitekehystä, joka havainnollistaa tutkimuksen eksplisiittisesti määriteltyä näkökulmaa (Alasuutari 2011, 60).



Kuvio 1 Tutkielman teoreettinen viitekehys

Tämän tutkielman teoreettinen viitekehys rakentuu kolmen keskeisen käsitteen ympärille. Tutkielman aihepiirin kannalta keskeisiä ja läpi tutkielman toistuvia käsitteitä ovat kyberriskit, kolmannet osapuolet ja kybervakuutus. Tutkielman kantava teema on kyberriskit, joiden ympärille tutkielman muut tutkittavat ilmiöt rakentuvat. Kyberriskit ovat tutkielman taustateoria, jota vasten koko ilmiötä tarkastellaan. Lisäksi tutkielman taustateoriassa ovat uhat ja haavoittuvuudet, jotka kytkeytyvät keskeisesti edellä mainittuihin kyberriskeihin, kuten kuviossa 1 on esitetty. Tässä tutkielmassa keskitytään tarkastelemaan yksinomaan kolmansista osapuolista aiheutuvia kyberriskejä. Kolmannet osapuolet ovat tämän tutkielman tulkintateoria, jonka ympärille tutkielman näkökulma rakentuu. Kolmansista osapuolista aiheutuvien kyberriskien tarkastelussa keskitytään niiden tunnistamiseen ja arviointiin, jotka ovat esitetty kuviossa 1.

Lisäksi kuviossa 1 on esitetty alimmaisena kybervakuutus, jonka kattavuutta kolmansista osapuolista aiheutuvissa vastuu- ja riippuvuuskeskeytysvahingoissa tarkastellaan tässä tutkielmassa.

1.7 Tutkielman rakenne

Tämä tutkielma noudattelee vakuutuksen ja riskienhallinnan opintosuunnan konventioita tutkielman rakenteesta. Tutkielma rakentuu neljästä osasta, jotka on jaettu kuuteen päälukuun: johdantoon, kahteen teorialukuun, kahteen empirialukuun ja yhteenvetoon. Johdantoluvussa avataan lukijalle tutkielman taustaa ja luodaan tieteelliset puitteet tutkielman suorittamiselle.

Toinen pääluku esittelee tutkielman taustateorian eli tutkielman kannalta keskeisen teorian, jota vasten aineistoa tarkastellaan. Taustateorialuvussa syvennytään tarkastelemaan kyberriskejä ja kyberuhkia. Tarkasteltavan ilmiön kannalta keskeisistä teemoista syvennytään kyberriskien luokitteluun, niistä aiheutuviin kustannuksiin, erilaisiin kyberuhkiin ja haavoittuvuuksiin sekä erilaisiin toimijoihin, jotka aiheuttavat kyberuhkia.

Kolmannessa pääluvussa esitetään tulkintateoria, jossa syvennytään tarkastelemaan tutkielman näkökulman kannalta olennaisia ilmiöitä: kolmansista osapuolista aiheutuvia kyberriskejä ja kybervakuutusta riskienhallintakeinona. Tulkintateorian aluksi määritellään tarkemmin, mitä kolmansilla osapuolilla käsitetään, miten pilvipalvelut vaikuttavat kyberriskeihin ja millaista sääntelyä henkilötietojen käsittelyn ulkoistamiseen liittyy. Lisäksi tulkintateoriassa käsitellään tutkielman kannalta olennaisia ja osittain toisiaan sivuavia käsitteitä: tieto- ja kyberturvallisuutta sekä kyberriskien hallintaa, joiden yhtäläisyydet ja erot ovat oleellista tunnistaa. Tutkielman näkökulmaan on valittu riskienhallintakeinoksi kybervakuutus, josta kolmannen pääluvun lopuksi syvennytään kyberriskien vakuutuskelpoisuuteen ja kybervakuutuksen turviin.

Neljäs ja viides pääluku muodostavat tutkielman empiirisen osan, missä käsitellään ja analysoidaan haastatteluilla hankittua empiiristä aineistoa. Neljännen pääluvun aluksi kuvataan tutkimushaastatteluiden kulku ja esitellään tutkielmaan haastatellut henkilöt. Neljännessä pääluvussa käsitellään kahden ensimmäisen tutkimusongelman kannalta keskeistä aineistoa,

missä selvitetään menetelmiä kolmansista osapuolista aiheutuvien kyberriskien arviointiin ja tutkitaan, kuinka pilvipalvelut vaikuttavat yrityksen kyberturvallisuuden tasoon. Viidennessä pääluvussa syvennytään käsittelemään kolmannen tutkimusongelman kannalta olennaista aineistoa ja selvitetään, miten kybervakuutuksella voi suojautua kolmansista osapuolista aiheutuvia kyberriskejä vastaan.

Kuudennessa ja viimeisessä pääluvussa esitetään tutkielman yhteenveto. Viimeisessä luvussa vastataan tutkimusongelmiin aiemmin käsitellyn empiirisen aineiston analysoinnin pohjalta ja tehdään johtopäätökset tutkielman tuloksista. Tutkimusongelmiin vastaamisen ja johtopäätösten jälkeen arvioidaan tutkielmaa ja sen luotettavuutta tieteellisten konventioiden mukaisesti. Yhteenvedon lopuksi käännetään katse tulevaisuuteen ja arvioidaan toimintaympäristön kehityssuuntia sekä pohditaan mahdollisia jatkotutkimuskohteita.

2 KYBERRISKIT JA KYBERUHAT

2.1 Kyberriskit

Kyberriskillä tarkoitetaan mitä tahansa riskiä, joka aiheuttaa taloudellista vahinkoa, häiriöitä tai mainehaittoja informaatioteknologiaan liittyvän vian vuoksi. Kyberriski voi aiheutua esimerkiksi tahallisen tietomurron, tahattoman tietovuodon tai tietojärjestelmiin liittyvän operatiivisen riskin seurauksena. Kyberriski ei välttämättä kohdistu suoraan organisaatioon itseensä, vaan se voi kohdistua myös kolmanteen osapuoleen, esimerkiksi yrityksen toimitusketjuun tai IT-palveluita tuottavaan yritykseen. (Institute of Risk Management 2014) Kyberriski voidaan määritellä hieman eri tavoilla ja sille ei ole olemassa yhtä vakiintunutta määritelmää. Esimerkiksi Biener ym. (2015) määrittelevät kyberriskin operatiiviseksi riskiksi, joka vaikuttaa tiedon tai tietojärjestelmien luottamuksellisuuteen, eheyteen tai saatavuuteen. Luottamuksellisuus tarkoittaa, että tiedot ovat vain niihin oikeutettujen henkilöiden saatavilla ja tietojen luvaton käyttö on estetty. Eheys tarkoittaa, että tiedot pysyvät alkuperäisessä muodossaan virheettöminä ja kokonaisina, eivätkä ne altistu tuhoutumiselle. Saatavuudella tarkoitetaan,

että tietoihin oikeutetuilla henkilöillä on aina häiriötön pääsy kyseisiin tietoihin ja että ne ovat vaaditussa muodossa. (Straub, Goodman & Seymour 2008, 124)

Kyberriskit voidaan luokitella toiminnan, kyberhyökkäyksen lajin ja lähteen mukaan. Toiminta voi olla esimerkiksi rikollista tai ei-rikollista, kyberhyökkäyksen laji voi olla esimerkiksi haitta-ohjelma tai palvelunestohyökkäys ja lähteenä voivat olla esimerkiksi kyberrikolliset tai toiset valtiot. Kyberriskien lähteet luokitellaan tarkemmin luvussa 2.1.1. Kyberhyökkäykset ovat pääasiassa rikollista toimintaa ja ne toteutetaan esimerkiksi haittaohjelmia tai tietokoneviruksia hyödyntämällä. Kyberhyökkäyksen onnistuminen riippuu siitä, pystyvätkö kyberhyökkäyksen tekijät hyödyntämään organisaation haavoittuvuutta. (Eling & Schnell 2016) Haavoittuvuudella tarkoitetaan heikkoutta tietyn järjestelmän tieto- ja/tai toimintavarmuudessa, jota esimerkiksi kyberrikollinen voi heikentää (Limnéll ym. 2014, 110–111). Haavoittuvuuksille on ominaista idiosynkraattinen eli yksittäiselle organisaatiolle ominainen riski, mihin vaikuttavat muun muassa laitteet ja järjestelmät, liiketoimintaprosessit ja ihmisten toiminta. Lisäksi haavoittuvuuksiin ja kyberturvallisuuden tasoon vaikuttavat kolmansien osapuolten, esimerkiksi toimitusketjun jäsenten, toimenpiteet kyberturvallisuuden edistämiseksi. (Eling & Schnell 2016)

Suomen kielessä kyber-sana on melko uusi, ja käsitteenä se on vakiintunut hallinnolliseen käyttöön ja tullut suuren yleisön tietoisuuteen vuonna 2013 esitellyn Suomen Kyberturvallisuusstrategian myötä. Kyber-sanaa käytetään suomen kielessä harvoin erikseen ja useimmiten se esiintyy yhdyssanan osana. (Limnéll 2014) Kyber-käsite yhdistyy kahteen elementtiin: virtuaalitodellisuuteen ja tietoverkkoihin. Virtuaalitodellisuus painottaa kyberriskien abstraktia ja aineetonta luonnetta, minkä vuoksi kyberriskejä on haastava arvioida. Tietoverkot liittyvät läheisesti kyberavaruus-käsitteeseen, jota käytetään usein synonyyminä internetille. Kyberavaruudella tarkoitetaan mitä tahansa verkkoa, joka yhdistää eri IT-järjestelmiä, kun taas internet käsittää vain julkiset tietoverkot. Internetin julkisesta luonteesta johtuen se on merkittävin kanava erilaisille kyberuhille. (Eling & Schnell 2016)

Perinteisille vahinkoriskeille on tyypillistä, että ne eivät ole vahvasti toisistaan riippuvaisia, sillä esimerkiksi maantieteelliset erot rajoittavat vahinkojen leviämistä. Sitä vastoin kyberriskeille on ominaista korrelaatio eli niiden riippuvuus toisistaan. (Öğüt, Raghunathan & Menon 2011)

Koska laitteet ja järjestelmät ovat yhteydessä toisiinsa internetin välityksellä, eivät maantieteelliset erot rajoita kyberriskien leviämistä, vaan ne voivat levitä maailmanlaajuisesti hyvin nopeasti. IT-järjestelmä- ja ohjelmistomarkkinoita hallitsee muutama suuri yritys, minkä vuoksi monet niiden käyttäjistä altistuvat samoille haavoittuvuuksille. Se lisää kyberriskien korrelaatiota, koska kyberrikolliset voivat hyödyntää samaa haavoittuvuutta suurelle määrälle käyttäjiä maantieteellisistä rajoista riippumatta. (Eling & Schnell 2016)

2.1.1 Luokittelu

Taulukko 1 Kyberriskien lähteiden luokittelu (mukaillen Cebula & Young 2010)

1. Ihmisten toimenpiteet	2. Järjestelmävirheet	3. Sisäisten prosessien epäonnistuminen	4. Ulkoiset tapahtumat
1.1 Tahaton	**2.1 Laitteisto**	**3.1 Prosessien suunnittelu ja toimeenpano**	**4.1 Katastrofit**
Vahinko	Kapasiteetti	Prosessien eteneminen	Sääilmiö
Virhe	Suorituskyky	Prosessien dokumentointi	Tuli
Laiminlyönti	Ylläpito	Roolit ja vastuut	Tulva
	Vanhentuneisuus	Ilmoitukset ja hälytykset	Maanjäristys
1.2 Tahallinen		Tiedonkulku	Levottomuus
Petos	**2.2 Ohjelmisto**	Ongelmien laajentuminen	Pandemia
Vahingonteko	Yhteensopivuus	Palvelutasosopimus	
Varkaus	Kokoonpanon hallinta	Tehtävien siirtäminen	**4.2 Lainsäädännölliset ongelmat**
Ilkivalta	Muutosten hallinta		Lakien noudattaminen
	Turvallisuusasetukset	**3.2 Prosessien hallinta**	Uusi lainsäädäntö
1.3 Toteuttamatta jättäminen	Ohjelmointikäytännöt	Valvonta	Oikeudenkäynnit
Taidot	Testaus	Mittarit	
Tiedot		Kausiarviointi	**4.3 Liiketoiminnalliset ongelmat**
Ohjeistus	**2.3 Järjestelmät**	Prosessin omistajuus	
Resurssien saatavuus	Suunnittelu		Toimittajan estyminen tarjota palveluita
	Vaatimukset	**3.3 Tukiprosessit**	Markkinatilanteet
	Integrointi	Rekrytointi	Taloustilanteet
	Monimutkaisuus	Rahoitus	
		Koulutus	**4.4 Riippuvuus ulkoisista palveluista**
		Hankinta	Sähkö, tietoliikenne
			Palo- ja pelastustoimi
			Varavoima
			Kuljetus

Kyberriskejä ja niiden eri tyyppejä on olemassa lukematon määrä. Uusia uhkia syntyy ja vanhoja poistuu koko ajan, minkä vuoksi niitä ei ole mahdollista luokitella aukottomasti. Yksi vakiintunut tapa luokitella kyberriskejä on jakaa ne riskien lähteiden mukaan neljään pääluokkaan: ihmisten toimenpiteisiin, järjestelmävirheisiin, sisäisten prosessien epäonnistumiseen ja ulkoisiin tapahtumiin. Taulukossa 1 on kuvattu kyberriskien luokittelu lähteiden mukaan neljään pääluokkaan, joista jokainen pääluokka on jaettu alaluokkiin. Lisäksi jokainen alaluokka on jaettu elementteihin, jotka kuvaavat jokaisen alaluokan mahdollisia riskien aiheuttajia. Kyberriskien lähteitä tarkastellessa on tärkeää huomioida kyberriskien moniulotteisuus; kyberriskit voivat levitä nopeasti ja ne voivat aiheuttaa muiden riskien toteutumisen. Lisäksi yhden kyberriskin tarkastelu yllä kuvatun taulukon mukaisesti voi vaatia useamman eri pää- ja alaluokan elementtien arvioimista. (Cebula & Young 2010)

Taulukossa 1 kyberriskien lähteistä ensimmäinen pääluokka on ihmisten toimenpiteet, jotka kuvaavat ihmisten tekemiä tai tekemättä jättämiä toimenpiteitä. Ihmisten aiheuttamat kyberriskit sisältävät organisaation sekä sisäiset että ulkopuoliset henkilöt. Ensimmäinen pääluokka on jaettu kolmeen alaluokkaan: tahattomiin ja tahallisiin toimenpiteisiin sekä toteuttamatta jättämiseen. Ihmisten aiheuttamat tahattomat kyberriskit ovat useimmiten organisaation sisäisten henkilöiden aiheuttamia ja ne voivat aiheutua vahingoista, virheistä ja laiminlyönneistä. Ihmisten aiheuttamat tahalliset toimenpiteet ovat tarkoituksellisia ja niiden tavoitteena on aiheuttaa vahinkoa. Tahallisia vahinkoja voivat aiheuttaa organisaation sekä sisäiset että ulkopuoliset henkilöt. Tahallisesti aiheutettuja kyberriskejä ovat petos, vahingonteko, varkaus ja ilkivalta. Viimeinen alaluokka on toteuttamatta jätetyt toimenpiteet, jotka kuvaavat tilanteita, joissa henkilö ei ole suorittanut tilanteen vaatimia toimenpiteitä. Viimeisen alaluokan kyberriskit aiheutuvat useimmiten organisaation sisäisten henkilöiden toiminnasta. Ne voivat johtua tietojen, taitojen, ohjeistuksen ja resurssien saatavuuden puutteesta. (Cebula & Young 2010)

Taulukossa 1 kyberriskien lähteistä toisen pääluokan muodostavat järjestelmävirheet, jotka johtuvat tietojärjestelmien ja ohjelmistojen epänormaalista tai odottamattomasta toiminnasta. Järjestelmävirheiden pääluokka on jaettu kolmeen alaluokkaan: laitteistoihin, ohjelmistoihin ja järjestelmiin. Laitteistoista aiheutuvat kyberriskit ovat fyysisistä laitteista aiheutuvia

riskejä, joita ovat kapasiteetin, suorituskyvyn ja ylläpidon puute sekä laitteistojen vanhentuneisuus. Ohjelmistoista aiheutuvat kyberriskit sisältävät ohjelmistoihin, sovelluksiin ja käyttöjärjestelmiin liittyvät riskit, joita ovat esimerkiksi yhteensopivuuden, muutosten hallinnan ja turvallisuusasetusten puutteellisuus. Järjestelmiin liittyvät kyberriskit aiheutuvat eri osista koottujen laitteistojen ja ohjelmistojen muodostamien järjestelmien odottamattomasta toiminnasta. Ne voivat johtua esimerkiksi suunnittelun, vaatimuksien ja integroinnin puutteellisuudesta. (Cebula & Young 2010)

Sisäisten prosessien epäonnistuminen kuvaa operatiivisia riskejä, joiden vuoksi organisaation sisäiset prosessit eivät toimi kuten niiden vaaditaan tai odotetaan toimivan. Ne voidaan jakaa taulukon 1 mukaisesti prosessien suunnittelusta ja toimeenpanosta, prosessien hallinnasta sekä tukitoiminnoista johtuviin riskeihin. Prosessien suunnitteluun ja toimeenpanoon liittyvät kyberriskit sisältävät prosesseja, jotka eivät saavuta niille asetettuja tavoitteita. Ne voivat johtua huonosti suunnitelluista prosesseista tai niiden huonosta toteutuksesta. Prosessien suunnitteluun ja toimeenpanoon vaikuttavia yksittäisiä tekijöitä ovat esimerkiksi vastuisiin ja tiedonkulkuun liittyvät puutteellisuudet. Prosessien hallinnasta aiheutuvat riskit ovat prosessien riittämätöntä johtamista ja hallintaa, mikä voi johtua valvonnan, mittareiden, kausiarvioinnin ja prosessien omistajien puutteellisuudesta. Sisäisten prosessien epäonnistumisten kolmas alaluokka on tukitoimintojen epäonnistuminen, mikä tarkoittaa, että ne eivät kykene tarjoamaan muiden liiketoimintaprosessien tarvitsemia toimintoja tai palveluita. Ne voivat johtua rekrytoinnin, rahoituksen, koulutuksen ja tarvittavien palveluiden tai tuotteiden hankinnan puutteista. (Cebula & Young 2010)

Kyberriskien lähteistä neljäs pääluokka on ulkoiset tapahtumat, joita organisaatio ei voi itse hallita ja joiden ajoitusta tai lopputulosta ei useimmiten voida ennustaa. Ulkoiset tapahtumat jaetaan neljään alaluokkaan: katastrofeihin, lainsäädännöllisiin ongelmiin, liiketoiminnallisiin ongelmiin ja riippuvuuteen ulkoisista palveluista. Katastrofit ovat luonnon tai ihmisen aiheuttamia ja niitä ovat esimerkiksi äärimmäiset sääilmiöt, maanjäristykset ja levottomuudet. Lainsäädäntöön liittyvät ongelmat aiheutuvat lakien noudattamisen epäonnistumisesta, uudesta lainsäädännöstä ja oikeudenkäynneistä yritystä vastaan. Liiketoiminnalliset ongelmat voivat aiheutua toimittajan kyvyttömyydestä toimittaa palveluita tai tuotteita, markkinatilanteiden

heikentymisestä ja yrityksen rahoituksen puutteesta. Viimeinen alaluokka on riippuvuus ulkoisista palveluista, kuten energiasta ja tietoliikennepalveluista, palo- ja pelastustoimesta, varavoimasta ja kuljetuspalveluista. (Cebula & Young 2010)

2.1.2 Vahinkojen kustannukset

Kyberriskien kustannusten arviointi on haastavaa ja erilaiset arviot vaihtelevat huomattavasti, koska kyberriskeihin liittyy keskeisesti epävarmuus. Sen vuoksi ei ole olemassa yleisesti hyväksyttyä tietolähdettä kyberriskien kustannusten arvioimiseksi. Osa kyberriskeistä ei aiheuta kustannuksia lainkaan ja tiettyjä vahinkoja ei välttämättä ole mahdollista mitata taloudellisesti. Esimerkiksi rasismin levittämistä ja kybermaailmassa tapahtuvan henkisen väkivallan kustannuksia ei ole mahdollista määrittää rahallisesti. (Eling & Schnell 2016)

Kyberriskeistä aiheutuvat vahingot jaetaan yritykselle itselleen ja kolmansille osapuolille aiheutuneisiin vahinkoihin. Yritykselle aiheutuvia vahinkoja ovat digitaalisen omaisuuden katoaminen tai vahingoittuminen, liiketoiminnan keskeytyminen, kiristys ja digitaalisen omaisuuden sekä rahan varastaminen. (Marotta ym. 2017) Kustannuksia edellä mainituista vahingoista voi aiheutua esimerkiksi toimintakyvyn palauttamisesta, tuottojen ja liikevaihdon pienentymisestä, asiantuntijoiden palkkaamisesta ja kiristyksen vuoksi maksetuista kuluista (Biener ym. 2015).

Kolmansille osapuolille aiheutuneet vahingot ovat luonteeltaan vastuuvahinkoja, joista yritys on korvausvelvollinen vahingon tapahduttua. Kolmansille osapuolille aiheutuvat vahingot voivat syntyä esimerkiksi asiakkaiden salassa pidettävien tietojen, kuten henkilö- ja maksukorttitietojen, vuotamisesta ulkopuolisille sekä asiakkaille aiheutuneista vahingoista, jos yrityksen palveluiden tai järjestelmien kautta asiakas on altistunut haittaohjelmille. Vastuuvahingoissa kustannuksia syntyy yleensä myös mahdollisista oikeudenkäynneistä ja tietosuojaan liittyvistä sanktioista. (Biener ym. 2015) Tässä yhteydessä on olennaista huomioida ero kolmansille osapuolille *aiheutetuissa* vahingoissa ja tämän tutkielman keskeisessä teemassa eli kolmansista osapuolista *aiheutuvissa* kyberriskeissä. Kolmansia osapuolia käsitellään laajemmin kolmannessa pääluvussa.

Vaikka kyberriskien kustannuksia on haastava arvioida ja alalla ei ole olemassa yleisesti hyväksyttyä tietolähdettä, ovat useat tietoturvayhtiöt, tutkijat ja alaa tutkivat organisaatiot esittäneet omia arvioitaan kyberriskien kustannuksista. Kyberriskien kustannuksia voidaan arvioida yhtä vuotanutta tietuetta tai yhtä tietomurtoa kohden tai kuinka paljon tietomurrot aiheuttavat kokonaisuudessaan kustannuksia vuodessa. Tietomurroissa tietueella käsitetään yhtä kirjausta, joka voi sisältää esimerkiksi henkilötietoja tai maksukorttitietoja. (Eling & Schnell 2016)

Kyberriskien maailmanlaajuisten kustannusten arvioidaan vuosittain olevan yli 100 miljardia dollaria. Arviot vaihtelevat merkittävästi, koska osa arvioista ottaa huomioon vain suorat kustannukset, ja toiset arviot huomioivat myös epäsuorat kustannukset, kuten maineen heikkenemisen. Maailmanlaajuisten kustannusten arviot vaihtelevat yleisesti 100 ja 1000 miljardin dollarin välillä, mikä ilmentää suurta vaihtelua ja epävarmuutta arvioissa. Suuren vaihtelun vuoksi kyberriskien maailmanlaajuisten kustannusten arvioihin tulee suhtautua varauksella. (Eling & Schnell 2016)

Kun kyberriskien kustannuksia tarkastellaan yhtä tietomurtoa tai yhtä paljastunutta tietuetta kohden, eri arvioiden välinen vaihtelu pienenee. Yleisesti yhden tietomurron kustannuksiksi on arvioitu 2,1–3,8 miljoonaa dollaria. (Eling & Schnell 2016) Ponemon Instituten (2017) tutkimuksen mukaan vuonna 2017 yhden tietomurron keskimääräinen kustannus on 3,62 miljoonaa dollaria. Heidän arvionsa mukaan yhden tietomurrossa paljastuneen tietueen kustannus on 141 dollaria. Kyseisessä tutkimuksessa on kartoitettu tietomurtojen kustannuksia 13 eri maassa tai maantieteellisellä alueella ja kustannusten arvioinnissa on otettu huomioon sekä suorat että epäsuorat kustannukset. Tietomurtojen kustannukset vaihtelevat maantieteellisten alueiden välillä. Yhtä tietuetta kohden tietomurron kustannukset Yhdysvalloissa ovat 225 dollaria, kun Intiassa vastaava luku on 64 dollaria. Eri maiden väliset erot selittyvät esimerkiksi lainsäädäntöön ja tietosuojaan liittyvien vaatimusten eroilla. Myös eri toimialojen välillä on eroja tietomurtojen kustannuksissa. Terveydenhuoltoalalla yhden paljastuneen tietueen kustannukset ovat lähes kaksinkertaiset yhden tietomurron keskimääräisiin kustannuksiin verrattuna. (Ponemon Institute 2017)

Eling ja Schnell (2016) huomauttavat, että arvioihin kyberriskien kustannuksista on suhtauduttava varauksella, koska useimmat arvioista on tehty tietoturva- ja konsultointialan yrityksien toimesta, joten heidän näkemyksensä ei välttämättä ole täysin objektiivinen. Tietomurtojen

kustannuksista on esitetty myös poikkeavia arvioita. Romanosky (2016) on tutkinut 12 000 tietomurron otosta ja hänen mukaansa yhden tietomurron keskimääräinen kustannus on noin 200 000 dollaria, joka on merkittävästi alhaisempi kuin usein esitetyt arviot muutamista miljoonista dollareista. Tässä tutkimuksessa tyypillisen tietomurron kustannus on laskettu koko aineiston mediaanilukuna. Esimerkiksi Ponemon Instituten tekemissä arvioissa on käytetty tilastollista keskiarvoa, mikä voi olla harhaanjohtavaa. Tietomurroille on ominaista, että lukumääräisesti harvemmilla tietomurroilla on erittäin korkeat kustannukset ja usein tapahtuvilla tietomurroilla on verrattain alhaiset kustannukset, mikä johtaa jakauman vinoutumiseen. (Romanosky 2016)

2.2 Kyberuhat

Kyberuhka on digitaalisessa maailmassa tahallisesti tai tahattomasti tapahtuva turvattavan kohteen turvallisuutta heikentävä tekijä. Uhkaan liittyy keskeisesti jonkin tapahtuman mahdollisuus eli se voi olla mitä tahansa toimintaa, joka saattaa aiheuttaa vahinkoa tai muilla tavoin estää tai vaikeuttaa toimintaa. Kyberuhat mielletään usein rikolliseksi toiminnaksi ja kyberhyökkäyksiksi, mutta merkittävä osa toteutuvista kyberuhista on muita kuin tahallisesti aiheutettuja. Esimerkiksi ohjelmistovirheet, laitteiden tekniset viat tai luonnonkatastrofit ja sääilmiöt ovat usein vahinkojen taustalla. (Limnéll ym. 2014, 37)

Aina uhka ei johdu suoraan tietystä toimijasta, vaan se voi olla jokin mahdollisesti toteutuva epämiellyttävä tai vahingollinen tapahtuma, joka uhkaa tai jonka voidaan ajatella olevan uhkaava. Tästä luonteesta johtuen kyberuhat ovat abstrakteja, minkä vuoksi niitä on vaikea arvioida objektiivisin perustein. Koska kyberuhkia on haastava arvioida ja niistä tiedetään vähän, voidaan kyberuhkia helposti liioitella ja keskittyä vain tiettyihin kyberuhkiin. Kyberuhat voivat aiheutua yrityksen ulkopuolisista tekijöistä tai ne voivat tulla yrityksen sisältä. Sisäisten kyberuhkien lähteenä ovat esimerkiksi tyytymättömät työntekijät, alihankkijat tai yhteistyökumppanit. Sisäiset kyberuhat voivat olla myös tahattomia. Esimerkiksi työntekijä voi tietämättään tuoda haittaohjelman organisaation järjestelmiin. Ulkopuolisia kyberuhkia muodostavat esimerkiksi kyberrikolliset ja aktivistit, jotka käyttävät välineinään esimerkiksi haittaohjelmia ja palvelunestohyökkäyksiä. (Limnéll ym. 2014, 106–107, 113)

Teknologia kehittyy nopeasti, minkä mukana muodostuu jatkuvasti uusia ja yhä kehittyneempiä kyberuhkia, joita voi olla haastava jäljittää (Bendovschi 2015). Euroopan unionin verkko- ja tietoturvavirasto ENISA:n (2017) mukaan vuonna 2016 merkittävimmät kyberuhat olivat: 1) haittaohjelmat, 2) verkkohyökkäykset, 3) verkkosovellushyökkäykset, 4) palvelunestohyökkäykset, 5) bottiverkot, 6) verkkourkinta, 7) roskaposti, 8) kiristysohjelmat, 9) sisäpiiriuhat (tahalliset ja tahattomat), 10) fyysinen manipulointi, vahingoittaminen, varkaus ja katoaminen, 11) haittaohjelmapaketit, 12) tietomurrot, 13) identiteettivarkaudet, 14) tietovuodot ja 15) kybervakoilu.

Edellä esitetyt 15 merkittävintä kyberuhkaa eivät ole kaikki toisistaan erillisiä ja erilaisia kyberuhkia, vaan ne kuuluvat 12 erilaiseen kyberuhkien tyyppien mukaan jaettuihin luokkiin. Tietyillä kyberuhilla on samankaltaisia ominaisuuksia, riippuvuuksia ja torjuntamenetelmiä, minkä vuoksi osa edellä esitetyistä kyberuhista kuuluu samaan luokkaan. Esimerkiksi kiristysohjelma on yksi haittaohjelman tyyppi, mutta sillä on tiettyjä erityisominaisuuksia, joita käytetään sen torjumiseen. (ENISA 2017)

Seuraavassa avataan viittä tärkeintä kyberuhkaa, jotka vaativat tarkemman määrittelyn. Muita kyberuhkia ei käsitellä tässä tutkielmassa laajemmin, ja niiden käsitteet ovat itseään selittäviä, joten niitä ei määritellä tässä yhteydessä erikseen. *Haittaohjelmat* ovat kaikista yleisin kyberuhka. Se on mikä tahansa ohjelma, jonka tarkoituksena on tehdä ei-toivottuja ja vahingollisia toimenpiteitä tietojärjestelmissä. Haittaohjelmia ovat esimerkiksi madot, virukset, troijalaiset ja vakoiluohjelmat. (Wangen 2015; ENISA 2017) *Verkkohyökkäykset* ja *verkkosovellushyökkäykset* ovat osittain päällekkäisiä käsitteitä. Molemmat käyttävät alustanaan palvelimia, selaimien sisällönhallintajärjestelmiä ja selainlaajennuksia, joiden tarkoituksena on hyödyntää selaimien ja niiden lisäosien haavoittuvuuksia. Verkkohyökkäykset ja verkkosovellushyökkäykset voivat levittää haittaohjelmia laitteille pelkästään sillä, että käyttäjä vierailee haitallisella verkkosivustolla. (ENISA 2017) *Palvelunestohyökkäyksen* tavoitteena on pyrkiä estämään tietyn verkkosivuston käyttö jumittamalla se, jolloin siihen kohdistetaan niin paljon verkkoliikennettä, että sivusto ei toimi normaalisti. Hajautetulla palvelunestohyökkäyksellä tarkoitetaan verkkohyökkäystä, jossa useat tahot hyökkäävät samaan kohteeseen samanaikaisesti. *Bottiverkoilla* tarkoitetaan yhteen kytkettyjen ja kaapattujen tietokoneiden verkkoa,

jota hyökkääjä voi hyödyntää esimerkiksi palvelunestohyökkäyksen tekemiseen tai haittaohjelmien levittämiseen. (Limnéll ym. 2014, 112)

2.2.1 Haavoittuvuudet

Tietotekniikassa haavoittuvuudella tarkoitetaan heikkoutta, joka antaa mahdollisuuden heikentää tietyn järjestelmän tietoturvallisuutta tai toimintavarmuutta. Jotta haavoittuvuus voi syntyä, pitää järjestelmässä olla vika tai heikkous, toimijalla tai hyökkääjällä pitää olla pääsy kyseiseen järjestelmään ja lisäksi sillä pitää olla kyky käyttää kyseistä vikaa tai heikkoutta hyväkseen. (Limnéll ym. 2014, 110–111) Edellisessä luvussa kuvatut kyberuhat käyttävät hyväkseen haavoittuvuuksia, joita hyödyntämällä toimijat voivat vaikuttaa organisaatioiden aineelliseen ja aineettomaan omaisuuteen. Esimerkiksi tieto-omaisuus on yksi organisaatioiden omaisuuseristä, joka voi olla vahingoittamisen tai varkauden kohteena. Perinteisesti tieto-omaisuus ja tietotekniikka ovat aiheuttaneet haavoittuvuuksia, mutta yhä useammin ihmiset, esimerkiksi huolimattomuuttaan, aiheuttavat haavoittuvuuksia. Lisäksi ihmiset voivat olla myös kyberuhan kohteena, minkä vuoksi ihmiset ovat yksi suojattava kohde kyberavaruudesta tulevia uhkia vastaan. (von Solms & van Niekerk 2013)

Haavoittuvuudet voidaan jakaa sen mukaan, mihin organisaation omaisuuserään ne liittyvät. International Organization for Standardization on jakanut ISO 27005 -standardissaan (2008) haavoittuvuudet kuuteen luokkaan: laitteistoihin, ohjelmistoihin, verkkoihin, henkilöstöön, fyysiseen sijaintiin ja organisaatioon. Laitteistoihin liittyvät haavoittuvuudet voivat johtua esimerkiksi puutteellisesta ylläpidosta ja niiden vanhentuneisuudesta. Ohjelmistoista aiheutuvat haavoittuvuudet voivat syntyä esimerkiksi puutteellisesta käyttöoikeuksien todentamisesta, heikosta salasanojen hallinnasta ja suunnitteluvirheistä. Verkkoihin liittyvät haavoittuvuudet voivat johtua esimerkiksi suojaamattomista viestintäyhteyksistä ja luottamuksellisten tietojen välittämisestä alhaisen suojaustason viestintävälineillä. Organisaation henkilöstö voi aiheuttaa haavoittuvuuksia, jos heitä ei ole koulutettu riittävästi tai he käyttävät ohjelmistoja ja laitteita virheellisesti. Fyysisestä sijainnista aiheutuvat haavoittuvuudet voivat syntyä, jos esimerkiksi organisaation tiloissa ei ole riittävää kulunvalvontaa ja se mahdollistaa asiattomien henkilöiden pääsyn tiloihin. Koko organisaatioon liittyvät haavoittuvuudet voivat syntyä esimerkiksi sisäisen valvonnan, riskien arvioinnin tai jatkuvuussuunnitelmien puutteista. (ISO 2008)

Ohjelmistoihin liittyviä haavoittuvuuksia löydetään päivittäin ja ne ovat yleisin syy uhkien toteutumisille. Erityisen vakavia ovat tuntemattomat haavoittuvuudet eli niin sanotut nollapäivähaavoittuvuudet. Yhä useampi kyberuhka hyödyntää nollapäivähaavoittuvuuksia ja niiden vaikutus kestää ajallisesti pitkään. (Zhang, Cheng & Boutaba 2015) Nollapäivähaavoittuvuus on ohjelmistossa oleva haavoittuvuus, joka on löydetty ja jolle on olemassa hyväksikäyttömenetelmä, mutta sille ei ole olemassa korjausta (Wolf & Fresco 2016).

2.2.2 Toimijat ja motiivit

Taulukko 2 Toimijat ja motiivit (mukaillen Limnéll ym. 2014, 113)

	MOTIVAATIO	TOIMIJAT	KOHDE
KYBERSOTA	Poliittinen / sotilaallinen hallinta	Valtiot	Kriittinen infra ja muut strategiset kohteet
KYBERTERRORISMI	Poliittinen muutos, pelko	Terroristit	Infra, voimavarat ja julkiset kohteet
KYBERVAKOILU	Tiedon varastaminen	Valtiot ja yritykset	Hallitukset, yritykset ja yksilöt
KYBERRIKOLLISUUS	Taloudellinen hyötyminen	Rikolliset	Yritykset ja yksilöt
HAKTIVISMI, HAKKEROINTI	Poliittinen muutos, egoismi	Aktivistit, haktivistit ja yksilöt	Hallitukset, yritykset ja yksilöt

Luvussa 2.2 kyberuhat on jaettu teknisellä tasolla, mutta ne voidaan jakaa myös strategisesta näkökulmasta taulukon 2 mukaisesti uhan muodostajien ja motiivien perusteella. Strategisella tasolla uhat voivat olla kybersodankäyntiä, kyberterrorismia, kybervakoilua, kyberrikollisuutta sekä haktivismia ja hakkerointia. (Limnéll ym. 2014, 113–114)

Kybersodasta keskustellaan yleisesti mediassa ja usein erilaisia palvelunestohyökkäyksiä ja tietomurtoja nimitetään kybersodaksi. Kaikkia kybermaailman tapahtumia ei pidä ymmärtää sodankäynniksi. (Limnéll ym. 2014, 138–139) Ridin (2012) mukaan kybersotaa ei tule tapahtumaan nyt eikä tulevaisuudessa. Hänen mukaansa kybersota ei ole sodankäyntiä, koska sodan

tuntomerkkien tulee sisältää väkivaltaisen luonteen, vastustajan saamisen puolustuskyvyttömäksi ja lisäksi sillä tulee olla poliittinen luonne. Myös Limnéll ym. (2014, 141–142) tarkentavat, että kybersota, jossa sotatoimet tapahtuvat vain kyberavaruudessa, ei ole todennäköinen tulevaisuudessa. Kybersodankäynti tulisi nähdä yhtenä sodankäynnin ulottuvuutena, missä kyberhyökkäyksellä voidaan esimerkiksi lamaannuttaa vihollisen johtamisjärjestelmiä, viestintäverkkoja ja kriittistä infrastruktuuria. Kybertoimet ovat siten vain osa sodankäynnin strategiaa, jossa yhdistetään kyberhyökkäyksiä ja fyysisiä toimenpiteitä. (Limnéll ym. 2014, 140–147)

Kyberterrorismille ei ole yksiselitteistä määritelmää, mutta taulukon 2 mukaisesti sen voidaan katsoa olevan terroristien aiheuttamia tietoteknologiaa hyödyntäviä toimia infrastruktuuria ja julkisia kohteita vastaan, joilla on tavoitteena saada aikaan poliittista muutosta tai pelkoa. Mikä tahansa kyberhyökkäys valtionhallintoa vastaan ei ole kyberterrorismia, sillä olennaista kyberterrorismille ovat poliittiset ja ideologiset tavoitteet, joilla yritetään vaikuttaa väestöön ja päätöksentekijöihin tai kiinnittää huomiota tiettyyn asiaan. Kyberterrorismin taustalla ovat useimmiten yksilöt tai pienet ryhmittymät. (Limnéll ym. 2014, 131–136)

Vakoilussa on kyse vanhasta ilmiöstä, jolla yritetään hankkia tietoa kaikin mahdollisin keinoin. Koska nykyisin valtaosa tiedosta on digitaalisessa muodossa, kutsutaan digitaaliseen tietoon kohdistuvaa vakoilua kybervakoiluksi. Taulukosta 2 ilmenee, että vakoilua suorittavat sekä yritykset että valtiot ja vakoilun kohteena ovat hallitukset, yritykset ja yksilöt. Kybervakoilulla tarkoitetaan salaisen tiedon luvatta hankkimista, jolla tavoitellaan kilpailuetua, tiedustelutietoa tai toisen valtion turvallisuuteen ja talouteen liittyviä tietoja. Tiedon siirtyminen kybermaailmaan on poistanut vakoilun maantieteellisiä rajoja ja sitä voidaan suorittaa kaukana vakoiltavasta kohteesta. Kybervakoilusta on tullut yleistä erityisesti valtioiden välillä, mutta myös yritysten keskuudessa kybervakoilu on yhä yleisempää. Esille on tullut tapauksia, joissa yritykset ovat palkanneet hakkereita hankkimaan salaista tietoa toisista yrityksistä. Kybervakoilua pidetään yhtenä merkittävimmistä kyberuhista, jonka seuraukset voivat esimerkiksi kahden suurvallan välillä eskaloitua vakaviksi. (Limnéll ym. 2014, 128–130)

Kyberrikollisuus on kyberuhista yleisin ja se voi taulukon 2 mukaisesti kohdistua yksilöön, yritykseen tai valtioon. Kyberrikollisuudelle ei ole vielä olemassa oikeustermiä ja sen käyttö ei ole vakiintunut. Kyberrikollisuus on kuitenkin rikollista toimintaa ja siihen sovelletaan muuta

olemassa olevaa lainsäädäntöä. Kyberrikollisuudella tarkoitetaan yleensä laitonta toimintaa, joka kohdistuu tietokoneisiin, digitaaliseen tietoon, tietojärjestelmiin ja tietoverkkoihin. Kyberrikollisuus on moniulotteinen ilmiö ja rajaa perinteisen rikollisuuden ja kyberrikollisuuden välille ei voida yksiselitteisesti tehdä. Kyberrikollisuuden yleisyyttä kuvaa se, että kybermaailmassa rikoksen uhriksi joutumisen todennäköisyys on suurempi kuin fyysisen rikollisuuden uhriksi joutumisessa. (Limnéll ym. 2014, 119–122)

Kyberrikollisuudessa pääasialliset toimijat ovat rikolliset, kuten taulukosta 2 ilmenee. Rikolliset voivat olla yksittäisiä tekijöitä, joita voi olla vaikea tunnistaa ja saada kiinni. Kyberrikollisuudesta on kuitenkin tullut yhä systemaattisempaa ja arvioiden mukaan noin 80 prosenttia kyberrikollisuudesta on järjestäytynyttä rikollisuutta. Motiivina kyberrikollisuudessa on useimmiten taloudellinen hyötyminen, mitä voidaan saavuttaa esimerkiksi identiteettivarkauksilla, teollisella vakoilulla sekä pankki- ja luottokorttitietoja kalastelemalla. Kyberrikollisuuden edistynyttä luonnetta kuvaa, että kyberhyökkäyksen toteuttamisen apuvälineitä on mahdollista ostaa palveluna (Crime-as-a-Service, CaaS), joita kyberrikolliset myyvät saadakseen taloudellista hyötyä. (Limnéll ym. 2014, 122–124)

Haktivismi muodostuu aktivismin ja hakkeroinnin yhdistämisestä, millä viitataan poliittisesti, ideologisesti tai sosiaalisesti motivoituneeseen toimintaan. Sekä kyberterrorismilla että haktivismilla on poliittiset tai ideologiset tavoitteet, mutta kyberterrorismista haktivismin erottaa se, että haktivismin tavoitteena ei ole aiheuttaa yhtä suurta vahinkoa kuin kyberterrorismilla. (Quigley, Burns & Stallard 2015) Hakkeroinnilla viitataan laittomaan toimintaan, jonka tarkoituksena on päästä suojattuihin tietojärjestelmiin käyttämällä esimerkiksi haittaohjelmia tai muita sovelluksia. Taulukon 2 mukaisesti haktivismin taustalla voivat olla yksilöt, aktivistit tai haktivistit. Aktivismi on laillista ja häiriötä aiheuttamatonta toimintaa jonkin tietyn päämäärän saavuttamiseksi kybermaailmaa käyttämällä. Haktivismi on sitä vastoin laitonta toimintaa ja siinä käytetään erilaisia hakkerointimenetelmiä esimerkiksi jonkin palvelun lamaannuttamiseksi. Haktivismin tavoitteena on aiheuttaa häiriötä mutta ei merkittäviä vahinkoja. (Denning 2001, 241, 263)

ENISA:n (2017) raportin mukaan vuonna 2016 kyberrikollisuus oli merkittävin kyberuhka ja se kattaa noin kaksi kolmasosaa kaikista kybertapahtumista. Kyberrikollisuuden jälkeen toiseksi

merkittävin uhka ovat organisaation sisäiset henkilöt, jotka voivat aiheuttaa uhkia tarkoituksellisesti, huolimattomuudella tai virheen seurauksena. Lisäksi haktivismi ja kybervakoilu ovat vuonna 2016 olleet merkittäviä kyberuhkia. Kyberterrorismi on kasvattanut painoarvoaan kyberuhkana, mutta se ei silti ole vielä vakavimpien kyberuhkien joukossa. (ENISA 2017) Vaikka kyberuhkien luokittelussa korostuvat tarkoituksellinen ja rikollinen toiminta, on olennaista huomioida, että kyberriskien aiheuttajista ei-rikollinen toiminta muodostaa yhtä tärkeän osa-alueen kyberriskeistä (Eling & Schnell 2016).

3 KOLMANNET OSAPUOLET KYBERRISKIEN LÄHTEENÄ JA KYBERVAKUUTUS RISKIENHALLINTAKEINONA

Kolmannet osapuolet ja niistä aiheutuvat kyberriskit ovat tämän tutkielman keskiössä. Tässä pääluvussa kuvataan ensin, mitä kolmansilla osapuolilla tarkoitetaan ja mitä erityispiirteitä niihin liittyy. Luvussa myöhemmin käsiteltävät teemat – kyberturvallisuus, kyberriskien hallinta ja kybervakuuttaminen – kytkeytyvät kaikki ensin käsiteltyihin kolmansiin osapuoliin. Myös kolmansista osapuolista aiheutuviin kyberriskeihin pätevät samat lainalaisuudet kuin yritykseen suoraan kohdistuviin kyberriskeihin.

3.1 Kolmannet osapuolet kyberriskien lähteenä

Kolmannella osapuolella viitataan tässä tutkielmassa mihin tahansa yritykseen, organisaatioon tai yksityishenkilöön, jonka kanssa yritys tekee liiketoimintaa. Kolmannet osapuolet voivat olla esimerkiksi tavarantoimittajia, alihankkijoita, yhteistyökumppaneita, välittäjiä, jälleenmyyjiä ja asiakkaita. Kolmannet osapuolet voivat olla yrityksen arvoketjussa heitä ennen ja heidän jälkeen. (OCC 2013)

Sekä pienet että suuret yritykset käyttävät liiketoiminnassaan lukuisia yhteistyökumppaneita, niin sanottuja kolmansia osapuolia, joita suurilla yrityksillä voi olla jopa tuhansia. Kolmannet osapuolet voivat olla mukana yritysten liiketoiminnassa vain satunnaisesti ja yksinkertaisissa

toiminnoissa, mutta monilla yrityksillä kolmannet osapuolet ovat keskeisessä osassa liiketoimintaa ja niiden kanssa jaetaan salassa pidettäviä tietoja. (Ulsch 2014, 145)

Kolmansia osapuolia pidetään yhtenä vakavimmista kyberriskien aiheuttajista, ja ne voivat toimia ikään kuin takaovena, jossa hyökkääjille on vähemmän esteitä ja jonka turvallisuuden taso on alhaisempi. Kun hyökkääjien kohteena olevan suuremman yrityksen kyberturvallisuuden taso on korkea, hyökkääjät siirtyvät etsimään tietoturva-aukkoja kolmansista osapuolista, joiden kautta he pääsevät murtautumaan kohdeyrityksen järjestelmiin. (Ulsch 2014, 145–146)

Ulkoistaminen ja kasvanut yhteistyö eri osa-alueilla on tuonut kiistattomia strategisia ja taloudellisia hyötyjä, joiden tärkeyttä kuvastaa se, että yritykset pitävät yhteistyökumppaneitaan toiseksi arvokkaimpana voimavaranaan. Jotta eri yrityksistä muodostuva verkosto voi toimia mahdollisimman tehokkaasti, täytyy jokaisen jakaa omasta toiminnastaan tietoa yrityksen ulkopuolelle. Kasvaneen tehokkuuden ja parantuneen taloudellisen tuloksen kääntöpuolena ovat kuitenkin kasvaneet ja kokonaan uudenlaiset riskit, jotka aiheutuvat kolmansista osapuolista. Yrityksen riskienhallinnassa on tärkeä ymmärtää, että ulkoistaessaan palveluita yritys on edelleen itse vastuussa varsinaisesta tuotteesta tai palvelusta ja siihen mahdollisesti liittyvistä lainsäädännön aiheuttamista velvoitteista. Uudentyyppisiä riskejä muodostuu jatkuvasti, minkä vuoksi niihin tulee varautua ennakoiden. (Park, Sen & Griffiths 2015)

3.1.1 Pilvipalvelut

Tässä tutkielmassa pilvipalveluntarjoajia käsitellään yhtenä keskeisenä muotona yritysten käyttämistä kolmansista osapuolista, jotka käsittelevät tietoja toimeksiantajansa lukuun. Pilvipalvelut voidaan määritellä lukuisilla eri tavoilla. Yleisesti käytetyn National Institute of Standards and Technologyn määritelmän mukaan pilvipalveluilla tarkoitetaan toimintamallia, joka mahdollistaa helpon pääsyn kaikkialta jaettuihin ja konfiguroitaviin tietotekniikkaresursseihin, esimerkiksi verkkoihin, palvelimiin ja tallennusvälineisiin, jotka voidaan ottaa käyttöön tai pois käytöstä nopeasti ja helposti. Pilvipalveluille tyypillisiä ominaispiirteitä ovat itsepalvelullisuus, laaja päätelaiteyhteensopivuus, resurssien yhteiskäyttö, nopea joustavuus sekä tarkka resurssien käyttö ja valvonta. (Mell & Grance 2011)

Pilvipalvelut voidaan luokitella esimerkiksi palvelu- ja hankintamallien mukaan. Palvelumallit jaetaan ohjelmisto-, alusta- ja infrastruktuuriresursseihin. Ohjelmistoresurssi-palvelumalli on yksinkertaisin ja siinä asiakkaan käyttöön annetaan verkon yli käytettäviä palveluita, esimerkiksi verkkoselaimen kautta käytettävä sähköposti. Käyttäjällä ei ole kontrollia pilvipalvelun turvallisuuteen eikä infrastruktuuriin, kuten verkkoihin, palvelimiin ja tallennusvälineisiin. Alustaresurssi-palvelumallissa palveluntarjoaja tuottaa sovelluskehitysympäristön, johon asiakas rakentaa omat ohjelmistonsa. Tässä palvelumallissa asiakkaalla ei ole kontrollia pilvipalvelun infrastruktuuriin, mutta se voi hallita omia ohjelmistojaan. Infrastruktuuriresurssi-palvelumallissa palveluntuottaja tarjoaa asiakkaansa käyttöön tietoverkkoja, tallennustilaa ja laskentatehoa, mutta asiakas saa itse valita ja toteuttaa käyttöjärjestelmänsä ja ohjelmistonsa. Käyttäjällä ei ole kontrollia pilvipalvelun infrastruktuuriin, mutta se hallitsee itse käyttöjärjestelmiään, ohjelmistojaan ja tallennustilaansa. (Mell & Grance 2011)

Pilvipalveluiden hankintamallit jaetaan neljään pääluokkaan: yksityiseen, yhteisölliseen, julkiseen ja hybridiin. Yksityinen pilvipalvelu on vain yhden organisaation omaan käyttöön tarkoitettu pilvipalvelu. Sen voi omistaa yritys itse tai palvelun voi tuottaa ulkopuolinen palveluntarjoaja mutta yksinomaan tilaajayrityksen käyttöön. Yhteisöllinen pilvipalvelu on tietyn ja rajatun yritysryhmän omaan käyttöön tarkoitettu pilvipalvelu, joka voidaan tuottaa yritysten itsensä tai ulkopuolisen palveluntarjoajan toimesta. Julkinen pilvipalvelu on tarkoitettu yleiseen ja käyttäjäryhmältään ennalta rajoittamattomaan käyttöön, minkä voi tuottaa jokin yritys tai valtiollinen organisaatio. Hybridipilvipalvelussa yhdistetään edellä esitettyjä malleja. Esimerkiksi yksityinen pilvipalvelu voi ylikuormittuessa ottaa käyttöön lisäkapasiteettia julkisesta pilvipalvelusta. (Mell & Grance 2011)

Pilvipalveluiden etuina nähdään alhaiset käyttökustannukset, korkea skaalautuvuus, helppo pääsy tietoresursseihin, alhaisemmat huoltokustannukset, laitteistoihin liittyvien riskien väheneminen ja toiminnan laajentaminen ilman tarvetta investoida IT-järjestelmiin (Zhang ym. 2010). Pilvipalvelut tuovat mukanaan kuitenkin ennestään tuntemattomia riskejä, joita vastaan perinteiset riskienhallintamenetelmät ovat tehottomia. Pilvipalveluiden turvallisuuden keskeinen haaste on luottamus. Luottamus pilvipalveluihin riippuu käytetyistä hankintamalleista. Esimerkiksi julkisessa tai yhteisöllisessä pilvipalvelussa tiedon ja ohjelmistojen hallinta

on ulkoistettu, ja tiedon omistajalla ei ole välitöntä kontrollia omiin tietoihinsa ja ohjelmistoihinsa. Tällaisissa hankintamalleissa luottamuksen merkitys pilvipalveluntarjoajan kykyyn taata turvallisuus korostuu. (Zissis & Lekkas 2012)

Luottamuksen lisäksi pilvipalveluiden toinen merkittävä haaste on uhkien tunnistaminen. Tietojärjestelmien turvallisuus on pohjimmiltaan uhkien tunnistamista ja niiden hallitsemista riittävillä riskienhallintatoimenpiteillä. Pilvipalveluiden turvallisuushaasteissa nousevat esille tietoturvallisuuden keskeiset osa-alueet: luottamuksellisuus, eheys ja saatavuus. Luottamuksellisuus korostaa, että vain tietoon ja järjestelmiin oikeutetuilla henkilöillä on niihin pääsy. Pilvipalvelut lisäävät tietovuodon uhkaa, koska pilvipalveluita käyttävät useammat käyttäjät erilaisilla laitteilla ja sovelluksilla. Se lisää kirjautumisten määrää pilvipalveluun eri laitteilta ja käyttäjiltä, ja tuo tiedon saataville useammille osapuolille. Koska pilvipalveluita pääsevät käyttämään useat eri käyttäjät, on valtuuksien määrittely tärkeää tiedon eheyden suojaamisessa, jotta vain tietoon oikeutetut henkilöt pääsevät muokkaamaan ja poistamaan tietoja. Vastuu tiedon eheydestä on pilvipalveluntarjoajalla. Tiedon ja tietojärjestelmien saatavuus on pilvipalveluissa keskeistä, koska resurssien on oltava käyttäjien saatavilla, vaikka jokin toiminto pilvipalveluissa ei ole toimintakunnossa tai pilvipalveluun tehdään tietomurto. Lisäksi verkkoyhteyksien toimivuuden takaaminen pilvipalveluita käytettäessä on keskeistä, jotta tiedot ja tietojärjestelmät ovat aina saatavilla ja käytettävissä. (Zissis & Lekkas 2012)

Pilvipalveluita kansainvälisesti tarjoavilla yrityksillä palvelimet, eli tietojen fyysiset säilytyspaikat, voivat sijaita eri puolilla maailmaa, joten asiakkaat eivät voi olla täysin varmoja, missä heidän tietojaan säilytetään. Palvelimien maantieteellinen sijainti altistaa tiedot kyseisen valtion lainsäädännön alaisuuteen, ja joidenkin valtioiden alueella tietoihin voi olla helpompi päästä käsiksi. Esimerkiksi Yhdysvalloissa terrorismin estämiseksi tarkoitetun asetuksen nojalla voidaan päästä pilvipalveluissa salassa pidettäviin tietoihin käsiksi, minkä vuoksi esimerkiksi eurooppalaiset yritykset eivät ole halukkaita käyttämään yhdysvaltalaisia palvelimia salaisten tietojen käsittelyssä. (Ulsch 2014, 166–167)

Koska pilvipalveluntarjoajia on lukuisia erilaisia ja eri tasoisia, ja myös ulkoistavien yritysten kyberturvallisuuden taso voi olla hyvin vaihteleva, ei ole olemassa yksiselitteistä vastausta, parantaako vai heikentääkö pilvipalveluiden käyttäminen yrityksen kyberturvallisuutta. Kyberturvallisuuteen sijoittaminen on kallista, minkä vuoksi kaikilla yrityksillä kyberturvallisuuden

taso ei ole korkealla. Tällaisessa tapauksessa ulkoisten pilvipalveluiden käyttäminen voi parantaa yrityksen kyberturvallisuuden tasoa, koska pilvipalveluntarjoajalla on korkeampi kyberturvallisuuden taso. Pilvipalveluiden käyttäminen voi siten lisätä tai vähentää yritykseen kohdistuvia kyberriskejä. (Ulsch 2014, 168) Pilvipalvelun kokonaisturvallisuus muodostuu sekä pilvipalveluntarjoajan että asiakkaan tietoturvakäytännöistä ja pilvipalveluun siirrettävän sovelluksen tietoturvasta. Pilvipalveluntarjoajan kyberturvallisuutta arvioitaessa tulisi kiinnittää huomiota palveluntarjoajan tekniseen, henkilöstön ja fyysiseen turvallisuuteen. Jos asiakkaalla ei ole mahdollista auditoida pilvipalveluntarjoajaa, voi palveluntarjoajaa arvioida teknisten ratkaisujen, sertifikaattien ja kolmansien osapuolten tekemien auditointien perusteella. (Kyberturvallisuuskeskus 2014)

3.1.2 Sääntely

Kun tietojenkäsittelyä ja -säilytystä ulkoistetaan kolmansille osapuolille, voivat ne sisältää henkilötietoja, joiden käsittelyä säännellään laeilla. Tämän tutkielman keskiössä ei ole tarkastella lainsäädännön vaikutusta henkilötietojenkäsittelyn ulkoistamisessa, mutta lainsäädännöllinen viitekehys on tärkeää tuoda tutkielman teoreettisessa osuudessa esille, ja sitä tullaan sivuamaan tutkielman empiirisessä osiossa. Tämän tutkielman kannalta keskeisin lainsäädäntö on EU:n tietosuoja-asetus, jota käsitellään tässä alaluvussa lyhyesti. EU:n tietosuoja-asetus on laaja sääntelykokonaisuus, josta keskitymme sen vaatimuksiin erityisesti henkilötietojen käsittelyn ulkoistamisessa. Lisäksi Suomessa on lukuisia eri toimialoja sääntteleviä erityislakeja, kuten sosiaali- ja terveydenhuollossa, joita ei tulla käsittelemään tässä tutkielmassa (Andreasson, Riikonen & Ylipartanen 2017, 29).

Euroopan parlamentin ja neuvoston asetus luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (2016/679) eli EU:n tietosuoja-asetus hyväksyttiin Euroopan parlamentissa 14.4.2016 ja se astuu voimaan kahden vuoden siirtymäajalla 25.5.2018. EU:n tietosuoja-asetus on suoraan jäsenvaltioissa sovellettavaa lainsäädäntöä. Tietosuoja-asetuksella on tarkoitus yhdenmukaistaa henkilötietojen käsittelyä ja tietosuojaa koskeva lainsäädäntö sekä luoda ajanmukainen sääntelykehikko vastaamaan nykyaikaisen tietoyhteiskunnan vaatimuksiin. EU:n tietosuoja-asetus koskee sekä julkista että

yksityistä sektoria ja se sisältää tarkat puitteet henkilötietojen käsittelylle, rekisteröityjen oikeuksille ja rekisterinpitäjän velvollisuuksille. EU:n tietosuoja-asetus kumoaa voimaan tullessaan henkilötietodirektiivin 95/46/EY, joka on Suomessa saatettu voimaan henkilötietolailla 22.4.1999/523. Henkilötietolaki kumoutuu vuonna 2018 ja voimaan astuu EU:n uusi tietosuoja-asetus. (Valtiovarainministeriö 2016)

EU:n tietosuoja-asetus ottaa huomioon nopeasti kasvavan suuntauksen, jossa palveluita ulkoistetaan muille palveluntuottajille tai rekisteritietoja pääsee käyttämään yrityksen ulkopuoliset käsittelijät. Aiemmin henkilötietolaissa ei ole erikseen määritelty tilanteista, joissa ulkopuolinen palveluntarjoaja tuottaa palveluita tai käsittelee rekisterinpitäjän henkilötietoja. EU:n tietosuoja-asetus erottaa toisistaan rekisterinpitäjän ja henkilötietojen käsittelijän. Tietosuoja-asetuksen 4 artiklan mukaan rekisterinpitäjällä tarkoitetaan tahoa, joka yksin tai yhdessä määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. 4 artiklan mukaan henkilötietojen käsittelijällä tarkoitetaan tahoa, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.

EU:n tietosuoja-asetuksen 28 artikla määrittelee rekisterinpitäjän ja henkilötietojen käsittelijän välisistä velvoitteista ja edellyttää esimerkiksi, että niiden välinen sopimus on tehtävä kirjallisena. Vastuu henkilötietojen käsittelystä säilyy edelleen rekisterinpitäjällä, mutta tietosuoja-asetus määrittelee rekisterinpitäjän ja henkilötietojen käsittelijän välisen sopimuksen sisältöä tarkemmin, mikä selkeyttää aiemmin melko laajaa sopimuksellista liikkumavaraa. EU:n tietosuoja-asetuksen puitteissa samat velvoitteet koskevat henkilötietojen käsittelijää kuin myös rekisterinpitäjää, koska tietosuoja-asetus edellyttää 28 artiklan mukaan rekisterinpitäjää käyttämään vain sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät suojatoimet ja täyttävät kaikki tietosuoja-asetuksen vaatimukset. Lisäksi tietosuoja-asetuksen 33 artiklan mukaan henkilötietojen käsittelijän on ilmoitettava rekisterinpitäjälle tietoturvaloukkauksista ilman aiheetonta viivytystä. Jos henkilötietojen käsittelyä tekee yrityksen ulkopuolinen taho, esimerkiksi pilvipalveluntarjoaja, myös tällaiset alihankkijat vastaavat sanktioiden uhalla tietosuoja-asetuksen vaatimusten noudattamisesta (Andreasson ym. 2017, 33).

Tietosuoja-asetuksen merkittävänä uudistuksena ovat hallinnolliset seuraamukset, joita valvontaviranomainen voi langettaa tietosuoja-asetuksen noudattamatta jättämisestä 83 artiklan mukaisesti. Valvontaviranomaisen langettamat seuraamukset ovat taloudellisia sanktioita,

jotka voivat olla enimmillään 20 miljoonaa euroa tai neljä prosenttia yrityksen kokonaisliikevaihdosta, jos sen osuus on suurempi kuin 20 miljoonaa euroa.

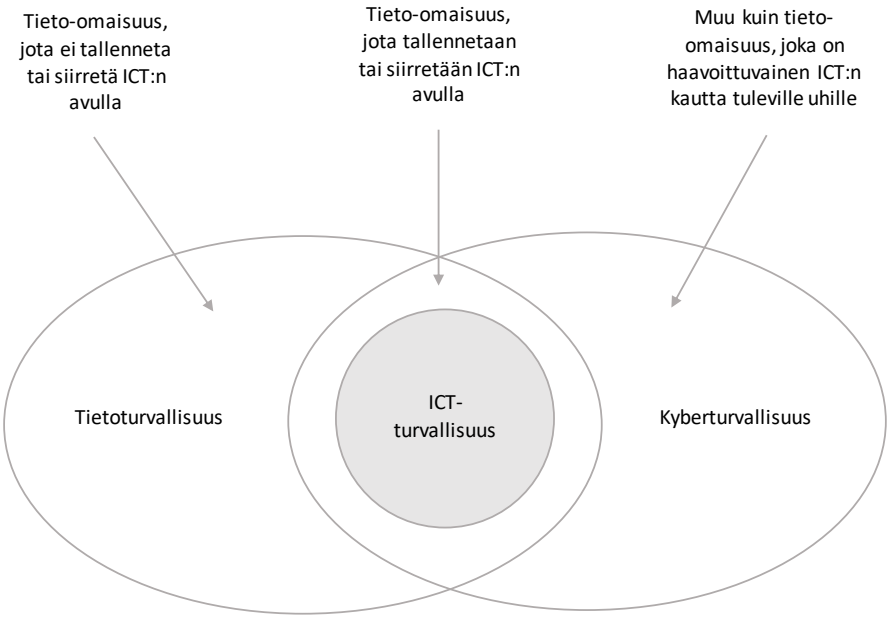
3.2 Kyberturvallisuutta vai tietoturvallisuutta?

Kyberturvallisuus on keskeinen osa kyberriskien hallintaa, joten tarkastelemme ensin kyberturvallisuuden merkitystä ennen siirtymistä kyberriskien hallintaan ja kybervakuuttamiseen. Limnéllin ym. (2014, 39) määritelmän mukaan: “Kyberturvallisuus tarkoittaa digitaalisen maailman tilaa, jossa vallitsee sekä ymmärryksen myötä tuotettu luottamuksen tunne että käytännön toimenpitein saavutettu kyky ennakoitavasti hallita sekä sietää kyberuhkia ja niiden vaikutuksia.” Kyberturvallisuudessa on hyvin keskeistä luottamus kybertoimintaympäristön toimivuuteen ja turvallisuuteen, samalla tavoin kuin luottamus esimerkiksi sähkönsaantiin ja yleiseen turvallisuuteen. Kyberturvallisuudella pyritään siihen, että käyttäjät voivat luottaa kybermaailman toimivuuteen ja että salassa pidettävät tiedot säilyvät luottamuksellisina ja vain niihin oikeutettujen henkilöiden saatavilla. Kyberturvallisuus mielletään helposti teknologiseksi asiaksi, mutta todellisuudessa kyberturvallisuudesta kaksi kolmasosaa on muuta kuin teknologiaa tai teknologisia ratkaisuja. Kyberturvallisuudessa keskeistä on luottamus ja sen määrittelee suurimmaksi osaksi ihmisten tekemät toimenpiteet. (Limnéll ym. 2014, 40, 47)

Kuten useille kybermaailman käsitteille, myös kyberturvallisuudelle ei ole olemassa yhtä vakiintunutta määritelmää. Edellä esitetyn määritelmän lisäksi kyberturvallisuus voidaan määritellä kyberavaruuden, sähköisen tiedon, informaatio- ja kommunikaatioteknologian sekä sen käyttäjien suojaamiseksi. Se kattaa sekä yksityishenkilöiden että yhteiskuntien aineettoman ja aineellisen omaisuuden, joka on haavoittuva kyberavaruudesta tuleville uhille. Kyberturvallisuus laajentuu tieto-omaisuuden lisäksi käsittämään myös kyberavaruuden, informaatio- ja kommunikaatioteknologian, sen käyttäjät ja muun kuin tietoon liittyvän omaisuuden. (von Solms & van Niekerk 2013) Molemmissa edellä esitetyissä määritelmissä on yhteistä näkemys kybermaailmasta laajana ympäristönä, jonka toimintavarmuutta ja luotettavuutta pyritään turvaamaan.

Kyberturvallisuutta ja tietoturvallisuutta käytetään usein virheellisesti toistensa synonyymeinä. Ne ovat toisistaan poikkeavia käsitteitä, vaikka niillä on myös selkeitä yhtäläisyyksiä.

Tietoturvallisuudella tarkoitetaan tiedon luottamuksellisuuden, eheyden ja saatavuuden turvaamista. Tietoturvallisuudelle on ominaista, että se keskittyy vain tieto-omaisuuden turvaamiseen, eikä siinä oteta huomioon muuta aineetonta tai aineellista omaisuutta ja käyttäjiä. Kyberturvallisuus laajentaa tietoturvallisuuden käsitettä kattamaan tieto-omaisuuden lisäksi myös muun omaisuuden ja suojaamaan käyttäjiä mahdollisilta kyberhyökkäyksiltä. (von Solms & van Niekerk 2013)



Kuvio 2 Kyberturvallisuuden ja tietoturvallisuuden välinen suhde (mukaillen von Solms & van Niekerk 2013)

Kuvio 2 havainnollistaa kyberturvallisuuden ja tietoturvallisuuden välistä suhdetta. Kyberturvallisuuden ja tietoturvallisuuden yhteinen osuus käsittää digitaalisessa muodossa olevan tiedon, esimerkiksi maksukorttitiedot, joita turvataan sekä kyberturvallisuudessa että tietoturvallisuudessa. Kuvion 2 vasemmassa laidassa oleva tietoturvallisuuden osuus kattaa tieto-omaisuuden, joka ei ole digitaalisessa muodossa, jolloin se sisältyy vain tietoturvallisuudessa määritellyksi suojattavaksi omaisuudeksi mutta ei kuulu kyberturvallisuuden piiriin. Kuvion 2 oikeassa laidassa oleva kyberturvallisuuden alue kattaa muun kuin tietoon liittyvän omaisuuden, joka ei kuulu perinteiseen tietoturvallisuuteen. Kyberturvallisuus sisältää sellaisia uhkia, jotka eivät toteutuessaan vaaranna tietoturvallisuudessa määriteltyjä tiedon luottamuksellisuutta, eheyttä ja saatavuutta. Esimerkkejä tällaisista tapauksista voivat olla kyberrikollisten tai kyberterroristien hyökkäykset kriittistä infrastruktuuria vastaan, jolloin he voivat häiritä

sähkön- tai vedenjakelua. Tällaisessa tapauksessa tiedon luottamuksellisuus, eheys tai saatavuus ei vaarannu, mutta rikolliset voivat aiheuttaa muuta vahinkoa. (von Solms & van Niekerk 2013)

3.3 Kyberriskien hallinta

Edellisessä luvussa esitelty kyberturvallisuus liittyy keskeisesti riskienhallintaan. Ne ovat osittain päällekkäisiä käsitteitä, sillä kyberturvallisuudella suojaudutaan negatiivisilta tekijöiltä, ennaltaehkäistään tai torjutaan niitä sekä lievennetään niiden vaikutuksia. (Limnéll ym. 2014, 105) Kyberturvallisuus on pääasiassa riskienhallintaa, jonka tavoitteena on minimoida riskit varmistamalla, että järjestelmät on hyvin konfiguroitu, päivitetty ja tarkastettu sekä henkilöstö on koulutettu ja säännöllisesti testattu (Touhill & Touhill 2014, 37). Kyberriskien hallinnassa yksi tärkeimmistä näkökulmista on, että se ei ole pelkästään IT-osastojen vastuulla, vaan sen tulee ulottua jokaisen osaston toimintaan. Oleellista on koko organisaation sitoutuminen kyberturvallisuuteen, ja organisaatioissa tulisi olla henkilö, joka on vastuussa tieto- tai kyberturvallisuudesta. (Eling & Schnell 2016) Yrityksillä, joilla on nimitetty tietoturvajohtaja tai vastaavassa asemassa oleva henkilö, on todettu olevan noin 30 prosenttia alhaisemmat kustannukset tietomurrosta kuin yrityksillä, joilla tietoturvan johtaminen ei kuuluu kokonaisvaltaiseen riskienhallintaan (Shackelford 2012).

Perinteinen riskienhallinta on jaettu viiteen vaiheeseen: lähtötilanteen määrittelyyn ja riskienhallinnan tavoitteisiin, riskien tunnistamiseen, riskien arvioimiseen, riskienhallintatoimenpiteisiin ja seurantaan. Riskien tunnistamista, arvioimista ja riskienhallintakeinoja käsitellään tarkemmin seuraavissa alaluvuissa. Riskienhallintaprosessin viimeinen vaihe eli seuranta on yksi tärkeimmistä vaiheista riskienhallintaprosessissa, sillä kyberriskit ja erilaiset kyberuhat muuttuvat nopeasti, joten riskienhallintaa pitää parantaa ja päivittää jatkuvasti. Huolellinen kommunikointi ja tiedon jakaminen on tärkeää, jotta koko yrityksen osaamista ja tietoisuutta kyberriskeistä voidaan vahvistaa. (Eling & Schnell 2016)

3.3.1 Tunnistaminen ja arviointi

Riskienhallintaprosessissa kyberriskien tunnistamisen tavoitteena on tunnistaa kyberriskien kohteena olevia omaisuuseriä, esimerkiksi aineetonta omaisuutta, ja niihin liittyviä liiketoimintaprosesseja. Kyberriskien kohteena olevan omaisuuden tunnistamisen jälkeen määritetään potentiaaliset kyberuhat ja niiden lähteet. (Eling & Schnell 2016) Riskien tunnistamisessa listataan ja luonnehditaan riskin elementtejä: uhkia, haavoittuvuuksia ja vaikutusta (Marotta ym. 2017).

Riskien arvioinnissa tavoitteena on arvioida riskien seurauksia ja todennäköisyyksiä. Kyberriskien arvioinnissa voidaan käyttää vaikutusanalyysiä, jolla arvioidaan yksittäisen vahinkoskenaarion kokonaiskustannuksia. Kokonaiskustannuksissa otetaan huomioon vahingon suorien kustannusten lisäksi epäsuorat kustannukset, kuten mainehaitat. Koska kyberriskit ovat verrattain uusi riskiluokka, niistä on olemassa vielä niukasti dataa. Sen vuoksi kyberriskien todennäköisyyksien arviointi on yksi suurimmista haasteista kyberriskien hallinnassa. Lisäksi kyberriskit muuttuvat nopeasti, minkä vuoksi tulevaisuuden ennakointiin historiallisen datan perusteella on suhtauduttava varauksella. (Eling & Schnell 2016)

Kyberriskien arviointi voi olla kvantitatiivista tai kvalitatiivista. Kvantitatiivisessa riskien arvioinnissa käytetään todellisia lukuja ja arvioita riskielementtien arvioinnissa. Kvalitatiivisessa riskien arvioinnissa ei sitä vastoin käytetä matemaattisia laskelmia, vaan riskien arviointi perustuu erilaisten skenaarioiden analysointiin. (Touhill & Touhill 2014, 55)

Kvantitatiivinen riskien arviointi on matemaattisesti monitahoinen menetelmä, jota käytetään perinteisten riskien arvioinnissa. Kvantitatiivista menetelmää käytetään harvemmin kyberriskien arvioinnissa, koska kyberriskien kohteena olevan tiedon tai muun omaisuuden arvoa on vaikea määrittää. Vielä haastavampaa on arvioida kyberriskien todennäköisyyttä. Kvantitatiivista menetelmää on kuitenkin mahdollista soveltaa kyberriskien arvioimiseen, kun aineettoman omaisuuden arvon määrittämisessä käytetään harkittuja arvioita. Tapahtumien todennäköisyyksistä on mahdollista tehdä valistuneita arvioita analysoimalla erilaisia uhkia ja tilastotietoja. (Touhill & Touhill 2014, 55)

Aineettomalle omaisuudelle, esimerkiksi tiedolle ja liikesalaisuuksille, on mahdollista määrittää taloudellinen arvo laskemalla, kuinka paljon aineeton omaisuus voi tuottaa tulosta, kuinka paljon sen hankkiminen tai kehittäminen maksaa, kuinka paljon sen ylläpito maksaa, paljonko sen korvaaminen maksaa, kuinka paljon syntyy kuluja, jos se ei ole saatavilla ja kuinka paljon kuluja voi syntyä vastuusta, jos tiedot vuotavat ulkopuolisille. Aineettoman omaisuuden arvon lisäksi tulee määrittää arvo mahdolliselle vahingolle, eli kuinka suuri osa aineettomasta omaisuudesta altistuu tuhoutumiselle vahingon sattuessa. Vahingon suuruus lasketaan omaisuuden arvon ja riskille altistumisen suhteena. Riskille altistuminen kuvaa suhteellista osuutta koko omaisuuden määrästä, mikä tuhoutuisi tai vahingoittuisi mahdollisen vahingon yhteydessä. (Touhill & Touhill 2014, 55–61)

Kyberriskin todennäköisyyttä voidaan arvioida tilastojen perusteella yrityksen toimialaan ja kyberturvallisuuden tasoon perustuvilla tekijöillä eli arvioidaan, kuinka usein vastaavanlainen yritys joutuisi tietomurron kohteeksi. Tilastollisista arvioista huolimatta kyberriskin todennäköisyyttä, yleisyyttä ja vakavuutta yhden yrityksen kohdalla on lähes mahdotonta ennakoida tarkasti. Kvantitatiivisessa riskin arvioinnissa riskin suuruus saadaan kertomalla vahingon suuruus tapahtuman todennäköisyydellä. Aiemmin esitetyistä ongelmakohdista johtuen kvantitatiivinen riskien arviointi ei ole kyberriskejä arvioitaessa tarkka, minkä vuoksi sitä käytetään melko vähän kyberriskien arvioinnissa. (Touhill & Touhill 2014, 62–63)

Kyberriskien arvioinnissa kvalitatiivinen menetelmä on yleisempi, sillä siinä ei käytetä yksityiskohtaisia laskelmia riskin rahallisen arvon määrittämiseksi. Se on myös menetelmänä yksinkertaisempi, nopeampi ja edullisempi kuin edellä esitelty kvantitatiivinen menetelmä. Kvalitatiivisessa riskien arvioinnissa käytetään suhteellisia arvoja riskistä ja omaisuuden arvosta, jotka luokitellaan vakavuuden mukaan esimerkiksi korkeaan, keskivertoon ja matalaan riskiin. (Touhill & Touhill 2014, 63)

Kvalitatiivinen arviointimenetelmä lähtee liikkeelle uhkien ja niiden lähteiden tunnistamisesta. Lähteinä voivat olla esimerkiksi ihmiset, luonnonkatastrofit ja ympäristöstä aiheutuvat riskit. Yksittäisiä kyberuhkia voivat olla esimerkiksi hakkerointi, tietokonevirus tai maanjäristys. Kyberuhkien tunnistamisen jälkeen riskien arvioinnissa kartoitetaan yrityksen haavoittuvuuksia. Haavoittuvuuksia voidaan kartoittaa muun muassa tekemällä haavoittuvuusskannauksia ja testaamalla tietoverkkoon tunkeutumista, jolla ammattilaiset yrittävät tunkeutua

yrityksen tietoverkkoon. Tavoitteena on löytää haavoittuvuuksia ennen kuin joku ulkopuolinen löytää ne ja kykenee hyödyntämään niitä. Myös sisäisellä tarkastuksella on haavoittuvuuksien havaitsemisessa merkittävä rooli koko organisaation tasolla. Uhkien ja haavoittuvuuksien arvioinnissa on tärkeää kohdistaa haavoittuvuudet ja niitä vastaavat uhat, koska haavoittuvuus ilman uhkaa ei vielä muodosta riskiä. Vastaavasti uhka ilman haavoittuvuutta ei muodosta riskiä. Kun uhka kohdistetaan tiettyyn haavoittuvuuteen, muodostaa se todellisen kyberriskin. (Touhill & Touhill 2014, 64–66)

Taulukko 3 Riskimatriisi (mukaillen Touhill & Touhill 2014, 71)

↓ Todennäköisyys / Vakavuus →	Matala	Kohtalainen	Korkea
Matala	Matala	Matala	Kohtalainen
Kohtalainen	Matala	Kohtalainen	Korkea
Korkea	Kohtalainen	Korkea	Korkea

Kyberriskien kvalitatiivisessa arvioinnissa on olennaista luokitella riskin eri tekijöitä sen vakavuuden mukaan. Riskin todennäköisyys voidaan luokitella esimerkiksi kolmeen luokkaan: matalaan, keskivertoon ja korkeaan. Luokat jaetaan todennäköisyyden mukaan tasavälein tai käyttämällä muunlaista luokitusta; esimerkiksi korkeaan todennäköisyyteen voidaan sisällyttää vain tapaukset, jotka sattuvat 90–100 prosentin todennäköisyydellä. Todennäköisyyden lisäksi riskikomponenteista arvioidaan tapahtuman vakavuutta yritykselle. Myös riskin vakavuus luokitellaan esimerkiksi kolmeen luokkaan, joiden arvioinnissa voidaan käyttää taloudellisia kustannuksia, liiketoiminnan keskeytymistä ja oikeudenkäyntien todennäköisyyttä. Todennäköisyyden ja vakavuuden luokittelun jälkeen muodostetaan taulukon 3 mukainen riskimatriisi, jossa yhdistetään tapahtuman todennäköisyys ja vakavuus, mistä voidaan arvioida yritykselle aiheutuvan riskin suuruutta. (Touhill & Touhill 2014, 69–71)

3.3.2 Riskienhallintakeinot

Kyberriskien hallinnassa sovelletaan samoja riskienhallintakeinoja kuin perinteisessä riskienhallinnassa. Kyberriskejä voidaan hallita välttämällä, vähentämällä, pitämällä omalla vastuulla tai siirtämällä. Riskien välttäminen tarkoittaa riskiä aiheuttavasta liiketoiminnasta luopumista, tässä tapauksessa tietotekniikan käyttämisestä luopumista, mikä ei useimmilla yrityksillä ole

mahdollista. (Eling & Schnell 2016) Kyberriskien hallinnassa riskin välttäminen voidaan ymmärtää myös toisella tavalla. Kybertoimintaympäristössä riskejä voidaan välttää poistamalla käytöstä vanhentuneita ja haavoittuvuuksille alttiita laitteita sekä järjestelmiä korvaamalla ne uusilla. Tässä tapauksessa riskin välttäminen onnistuu ilman, että tietotekniikan käyttämisestä luovutaan kokonaan. (Touhill & Touhill 2014, 73)

Riskien vähentäminen on kyberriskien hallintakeinoista yleisin. Kyberriskien todennäköisyyttä voidaan vähentää käyttämällä virustorjuntaohjelmia ja palomuureja. Vahinkojen suuruutta voidaan vähentää määrittämällä ohjeistuksia ja toimintatapoja tietomurron sattuessa, jotta vahinko voidaan rajata nopeasti. (Eling & Schnell 2016) Rakes, Deane ja Rees (2012) nostavat esille, että useimmilla yrityksillä ei ole luotettavaa menetelmää, jolla optimaalisia riskienhallintakeinoja valitaan, koska kyberriskien mittaaminen ja niihin soveltuvien riskienhallintakeinojen sovittaminen on haastavaa. He ovat esittäneet viitekehystä, jossa erilaisia riskienhallintakeinoja verrataan niiden soveltuvuudella kyberuhkien vähentämiseen. Viitekehyksen tarkoituksena on auttaa valitsemaan käytettävissä olevista keinoista tehokkain menetelmä. Viitekehys on muotoiltu optimointiongelmaksi, joka ottaa huomioon kustannukset, soveltuvuuden ja budjettirajoitteen. (Rakes ym. 2012)

Riskin hyväksyminen tai pitäminen omalla vastuulla tarkoittaa tunnistetun riskin hyväksymistä, jolloin sitä ei pyritä pienentämään, siirtämään tai välttämään. Riskin hyväksyminen voi tulla kyseeseen, kun suojattavan omaisuuden arvo on alhaisempi kuin sitä vaarantavan haavoittuvuuden korjaamisesta aiheutuvat kustannukset. Riskin hyväksyminen voi myös olla välttämätöntä, jos haavoittuvuuden korjaamiseen ei ole tarvittavia resursseja. (Touhill & Touhill 2014, 72–73) Riskin siirtäminen toteutetaan normaalisti siirtämällä riski vakuutusyhtiölle. Myös kyberriskien hallinnassa siirtäminen on mahdollista vakuuttamalla. (Eling & Schnell 2016) Kyberriskien hallintakeinoista kybervakuutus on tämän tutkielman keskiössä, ja sitä käsitellään seuraavassa luvussa.

3.4 Kybervakuutus

Yrityksille suunnatut omaisuus- ja vastuuvakuutukset ovat saatavilla useimmilla vakuutusmarkkinoilla maailmanlaajuisesti. Tyypillisesti omaisuusvakuutukset korvaavat vain omaisuudelle esimerkiksi tulipalon seurauksena aiheutuneita vahinkoja, mutta kyberriskit on usein rajattu ulkopuolelle. Myös vastuuvakuutuksissa kyberriskit on useimmiten rajattu korvauspiirin ulkopuolelle. Jo tapahtuneet kybervahingot ovat osoittaneet yritysten päätöksentekijöille, että nykyiset vakuutukset eivät tarjoa riittävää suojaa kyberriskien varalta. Tämän vuoksi erityisesti kyberriskien vakuuttamiseen erikoistunut markkina on kasvanut viime vuosina erityisesti Yhdysvalloissa, josta se on laajentunut myös Eurooppaan. (Biener ym. 2015)

Tavallisesti yritysvakuutuksissa ei ole erikseen määritelty, kuuluvatko kybervahingot omaisuus- ja vastuuvakuutusten korvauspiiriin, minkä vuoksi se on aiheuttanut epäselvyyksiä asiakkaiden ja vakuutusyhtiöiden välillä. Asiakkaat ovat voineet mieltää, että kybervahingot korvataan heidän vakuutuksestaan, kun taas vakuutusyhtiöt ovat mieltäneet, että kybervahingot eivät kuulu korvauspiiriin. Epäselvyyden vähentämiseksi vakuutusyhtiöt ovat muuttaneet ehtojaan, joissa selkeästi määritetään, kuuluvatko kybervahingot omaisuus- ja vastuuvakuutuksista korvattaviin vahinkoihin. Kun kybervahinkoja on rajattu perinteisten yritysvakuutusten ulkopuolelle, ovat vakuutusyhtiöt tuoneet markkinoille erillisiä kybervakuutuksia. Tähän mennessä kybervakuutusmarkkinat eivät ole kuitenkaan kehittyneet laajalti. Esimerkiksi Euroopassa useimmat yritykset eivät välttämättä ole tietoisia, että on olemassa erillinen vakuutus kybervahinkojen varalle. (Eling & Schnell 2016) Kybervakuutusmarkkinan uuden ja kehittyvän luonteen vuoksi haasteena markkinoilla ovat kybervakuutustuotteiden nopea muutos sekä vakuutusehtojen ja rajoitusten erot eri vakuuttajien välillä. Lisäksi yrityksiä uhkaavat kyberriskit ovat usein yksilöllisiä heidän toimialalleen tai jopa yksittäiselle yritykselle, minkä vuoksi kybervakuuttaminen on vaatinut paljon asiakaskohtaista muokkaamista. (Biener ym. 2015)

Kybervakuutusmarkkinat ovat Yhdysvalloissa huomattavasti suuremmat ja kehittyneemmät kuin Euroopassa. Todennäköisin syy on Yhdysvalloissa pidempään voimassa ollut sääntely, joka velvoittaa ilmoittamaan tietovuodoista, jolloin myös yritysten kiinnostus tietosuojaa ja kyberriskien hallintaa kohtaan on ollut suurempaa. (Eling & Schnell 2016) Vuonna 2015 kybervakuutusten maksutulo oli noin 1,5 miljardia dollaria, josta Yhdysvaltojen osuus oli noin 90

prosenttia. Erityisesti vähittäiskaupan, finanssialan ja terveydenhoitoalan yritykset ovat kiinnostuneita kybervakuutuksista. Edellä mainittuihin aloihin liittyy olennaisena osana asiakkaiden luottamuksellisten tietojen käsittely. Euroopassa kybervakuutusten vuosittainen maksutulo vuonna 2015 oli noin 135 miljoonaa dollaria. Euroopassa vakuutusmaksutulon odotetaan nousevan lähivuosina huomattavasti, sillä vuonna 2018 alkaa EU:n uuden tietosuoja-asetuksen soveltaminen, mikä asettaa yrityksille tiukempia vaatimuksia noudattaa säännöksiä ja huolehtia paremmasta kyberturvallisuudesta. (Aon 2017) Vakuutusyhtiö Allianz (2015) arvioi maailmanlaajuisten kybervakuutusmarkkinoiden kasvavan vuoteen 2025 mennessä yli 20 miljardiin dollariin vuodessa.

3.4.1 Kyberriskien vakuutuskelpoisuus

Taulukko 4 Vakuutuskelpoisuuden kriteerit (mukaillen Berliner 1985; Biener ym. 2015)

Vakuutuskelpoisuuden kriteerit		**Vaatimukset**
Vakuutusmatemaattinen	1) Vahingon sattumanvaraisuus	Riippumattomuus ja ennustettavuus
	2) Maksimivahingon määrä	Hallittavissa
	3) Keskimääräinen vahinko	Kohtuullinen
	4) Vahinkojen määrä	Suuri
	5) Epäsymmetrinen informaatio	Ei liiallinen
Markkinat	6) Vakuutusmaksu	Riittävä vakuuttajalle
	7) Maksimikorvaus	Hyväksyttävä asiakkaalle
Yhteiskunnallinen	8) Yhteiskunnallinen toimintatapa	Yhteiskunnallisten arvojen mukainen
	9) Lainsäädännön rajoitteet	Sallivat vakuutuskorvauksen

Taulukossa 4 on kuvattu Berlinerin (1985) esittämä yksinkertainen ja kattava mutta tiukka viitekehys, jolla arvioidaan riskin vakuutuskelpoisuutta. Hänen esittämää viitekehystä käytetään usein arvioitaessa vakuutusmarkkinoita ja -tuotteita. Viitekehys koostuu yhdeksästä vakuutuskelpoisuuden kriteeristä, jotka jaetaan kolmeen kategoriaan: vakuutusmatemaattisiin, markkinoihin liittyviin ja yhteiskunnallisiin tekijöihin. (Biener ym. 2015)

Taulukossa 4 ensimmäinen kategoria on vakuutusmatemaattiset tekijät, joista ensimmäinen kriteeri on vahingon sattumanvaraisuus. Sattumanvaraisuudella tarkoitetaan vahinkojen riip-

pumattomuutta toisistaan ja samalla myös vahinkojen määrän ennustettavuutta tietyllä ajanjaksolla. Lisäksi vakuutusmatemaattisesta näkökulmasta vakuutettavan riskin maksimivahingon tulee olla vakuutusyhtiön kantokyvyn kannalta hallittavissa, keskimääräisen vahingon suuruus tulee olla kohtuullinen ja vahinkojen määrän vuodessa tulee olla riittävän suuri. Lisäksi epäsymmetrinen informaatio eli haitallinen valikoituminen tai moraalikato eivät saa olla liian suuria. Vakuutusmatemaattisille kriteereille, kuten vakuutustaloudessa yleensä, on keskeistä suurten lukujen laki, sillä toisistaan erilliset ja hajautetut riskit alentavat vakuutuspoolin vahinkojen hajontaa. (Biener ym. 2015)

Taulukon 4 mukaisesti markkinoihin liittyvistä kriteereistä vakuutusmaksun tulee olla vakuuttajan liiketoiminnan kannalta riittävä, jotta se kattaa riskin, riskilisän ja liiketoiminnan kulut. Samaan aikaan vakuutusmaksun tulee olla kohderyhmälle edullinen. Myös vakuutuksen maksimikorvausmäärien tulee olla hyväksyttäviä kohderyhmälle. Maksimikorvausmäärät ovat toisinaan välttämättömiä, jotta riskistä tulee vakuutuskelpoinen. (Biener ym. 2015)

Taulukon 4 vakuutuskelpoisuuden kriteerien kolmas kategoria on yhteiskunnalliset kriteerit, joiden mukaan vakuutettavan riskin tulee olla yhteiskunnan toimintatapojen ja arvojen mukaista. Lisäksi yhteiskunta asettaa lainsäädännöllisiä rajoitteita, joten voimassaolevan lainsäädännön tulee sallia vakuutettavan riskin korvaus vakuutuksesta. Vakuutussopimukset eivät saa aiheuttaa kannustimia rikolliseen toimintaan, ja lainsäädäntö kieltääkin tietyntyyppisten riskien vakuuttamisen. (Biener ym. 2015)

Kun kyberriskejä arvioidaan edellä esitetyn Berlinerin vakuutuskelpoisuuden viitekehyksen puitteissa, nousee kyberriskien vakuutuskelpoisuudessa esille kolme keskeistä ongelmaa. Ensimmäinen haaste kyberriskien vakuutuskelpoisuudessa on, että vahingot eivät välttämättä ole sattumanvaraisia ja niiden ennustettavuus on heikko, minkä vuoksi riskin jakaminen ei toimi tarkoituksenmukaisesti. (Eling & Schnell 2016) Bienerin ym. (2015) mukaan vahinkojen sattumanvaraisuuden ja ennustettavuuden ongelmia ovat riskin tehokasta jakamista estävä riskien keskinäinen korrelaatio, poolien pienen koon aiheuttama hajauttamisen vähyys, riittävän jälleenvakuuttamisen vähyys, datan puute ja kyberriskien muuttuva luonne.

Kyberriskien vakuutuskelpoisuuden toinen keskeinen ongelma on epäsymmetrinen informaatio, joka aiheuttaa moraalikatoa ja haitallista valikoitumista. Moraalikato tarkoittaa vakuutetun käytöksen muutosta riskialttiimmaksi vakuutuksen ottamisen jälkeen. Kybervakuuttamisen tapauksessa moraalikato voi vähentää kannustimia sijoittaa yrityksen kyberturvallisuuden parantamiseen, kun vakuutus tarjoaa taloudellista turvaa vahingon tapahduttua. Vakuuttajat vähentävät moraalikatoa auditoimalla asiakkaitaan ja sisällyttämällä vakuutuksiin maksimikorvausmääriä sekä suurempia omavastuita. Moraalikadon lisäksi haitallinen valikoituminen aiheuttaa ongelmia kybervakuuttamisessa. Haitallista valikoitumista pyritään vähentämään esimerkiksi vakuutettavien etukäteisarvioinneilla, asiakasvalinnalla tai edellyttämällä asiakkailta näyttöä IT-järjestelmien käytön ja kokoonpanon ohjeidenmukaisuudesta. (Eling & Schnell 2016) Kybervakuuttamisessa haitallinen valikoituminen ilmenee esimerkiksi siten, että kyberhyökkäyksen kohteeksi joutuneet yritykset hankkivat kybervakuutuksen todennäköisemmin kuin sellaiset yritykset, jotka eivät ole joutuneet kyberhyökkäyksen kohteeksi (Shackelford 2012).

Kolmas keskeinen ongelma kyberriskien vakuutuskelpoisuudessa on vakuutuksen maksimikorvausmäärien verrattain alhainen taso, jonka lisäksi niissä on tyypillisesti useita rajoituksia korvauspiirin ulkopuolelle jäävistä vahinkotyypeistä. Rajoitusehtojen ja riskin muuttuvan luonteen vuoksi kybervakuutukset ovat usein monimutkaisia ja aiheuttavat epäselvyyksiä siitä, mitä vakuutuksesta todella korvataan. Kyberriskeistä aiheutuu usein epäsuoria vahinkoja, kuten mainehaittoja, joita on vaikea mitata ja sen vuoksi ne usein rajataan vakuutuksen ulkopuolelle. (Biener ym. 2015) Kybervakuutusten alhainen maksimikorvausmäärä johtaa tilanteisiin, joissa vakuutus ei korvaa kokonaan mahdollisia suurvahinkoja. Kybervakuutukset eivät siten täysin vastaa asiakkaiden tarpeita, koska vakuutetut hakevat kybervakuutuksilla usein suojaa suurten vahinkojen varalle, eikä niinkään usein tapahtuville pienemmille vahingoille. (Eling & Schnell 2016) Vaikka kyberriskien vakuutuskelpoisuudesta on edellä esitetty ongelmia, ovat ne kuitenkin vakuutuskelpoisia riskejä. Kyberriskien vakuutuskelpoisuus paranee tulevaisuudessa, kun markkinat kehittyvät ja laajentuvat, ja enemmän dataa tulee saataville kybervakuuttamisen kehittämiseksi. (Biener ym. 2015)

3.4.2 Kybervakuutusten turvat

Kybervakuutustuotteet ja niiden tarjoamat turvat poikkeavat toisistaan eri vakuuttajien ja markkina-alueiden välillä, mutta yleisesti kybervakuutuksen korvaukset voidaan jakaa kahteen luokkaan: vakuutetulle itselleen aiheutuneisiin vahinkoihin ja kolmansille osapuolille aiheutuneisiin vahinkoihin, joista vakuutuksenottaja on korvausvelvollinen (Marotta ym. 2017). Vakuutetulle itselleen maksettavat korvaukset voivat olla esimerkiksi kriisinhallinnasta, liiketoiminnan keskeytymisestä, tieto-omaisuuden suojaamisesta tai palauttamisesta sekä kiristyksestä aiheutuvia kustannuksia. Kriisinhallinnan aiheuttamia kustannuksia korvataan esimerkiksi asiantuntija-avun käyttämisestä yrityksen maineen palauttamiseksi ja tiedotuskuluja yrityksen sidosryhmille. Kybervahingon aiheuttama keskeytysvahinko aiheuttaa katteen menetystä, jota voidaan korvata kybervakuutuksesta. Sen lisäksi korvataan myös kuluja liiketoiminnan palauttamisesta normaaliksi. Tieto-omaisuudelle aiheutuneiden vahinkojen seurauksena voidaan korvata niiden palauttamisesta tai korvaamisesta aiheutuneita kuluja sekä muita aineettomalle omaisuudelle aiheutuneita vahinkoja. Kiristysvahingot kuuluvat keskeisesti kybertoimintaympäristöön, ja kybervakuutuksesta voidaan korvata kiristysmaksuja tai kiristyksen välttämiseksi aiheutuneita kuluja sen selvittämisestä. (Biener ym. 2015)

Kolmannelle osapuolelle aiheutuneet vahingot ovat kybervahingon seurauksena jollekin muulle kuin yritykselle itselleen aiheutuneita vahinkoja, joista yritys on korvausvelvollinen. Kolmansille osapuolille aiheutuneista vahingoista kybervakuutus tarjoaa suojaa yksityisyydensuojan loukkauksista, tietoverkon turvallisuuspuutteista, immateriaalioikeuksien loukkauksista ja mediavahingoista. Yksityisyydensuojan loukkauksista aiheutuvia kustannuksia voi syntyä, kun yrityksellä on salassa pidettäviä asiakastietoja, jotka joutuvat ulkopuolisille esimerkiksi tietomurron tai huolimattomuuden vuoksi. Kybervakuutuksesta korvattavia kuluja ovat esimerkiksi oikeudenkäynti- ja kriisinhallintakulut, kuten tiedotuskulut asiakkaille ja asiantuntija-avun käyttö tietomurron selvittämiseksi. Lisäksi kybervakuutus voi korvata yksityisyydensuojan loukkauksia toissijaisen vastuun periaatteella eli kybervakuutuksesta korvataan kuluja, vaikka tietojenkäsittely olisi ulkoistettu. (Biener ym. 2015)

Kolmansille osapuolille aiheutuneita vahinkoja voi syntyä tietoverkon turvallisuuspuutteiden vuoksi, jotka johtavat kolmansien osapuolien IT-järjestelmien vahingoittumiseen. Yrityksen IT-

järjestelmistä voi tahattomasti levitä haittaohjelmia asiakkaiden järjestelmiin, jokin ulkopuolinen taho voi päästä vakuutetun yrityksen järjestelmien kautta vahingoittamaan kolmannen osapuolen järjestelmiä tai kolmansien osapuolten immateriaalioikeuksia kavalletaan. Edellä mainitut tapaukset sisältyvät usein kybervakuutusten korvauspiiriin. Lisäksi kybervakuutus voi kattaa immateriaalioikeuksien loukkauksia ja mediavahinkoja. Mediavahingoilla tarkoitetaan esimerkiksi kunnianloukkausta, johon liittyviä oikeudenkäyntikuluja voidaan korvata kybervakuutuksesta. (Biener ym. 2015)

4 KOLMANSISTA OSAPUOLISTA AIHEUTUVIEN KYBERRISKIEN ARVIOINTI JA PILVIPALVELUIDEN VAIKUTUS KYBERTURVALLISUUTEEN

4.1 Aineiston kuvaus

Tutkielman empiirisen aineiston hankintamenetelmäksi valittiin tutkimuksen alkuvaiheessa laadullinen teemahaastattelu, jotta laajasta ja osin tuntemattomasta aihepiiristä saadaan mahdollisimman monipuolinen kuva. Lisäksi teemahaastattelu mahdollistaa uusien ja ennalta odottamattomien seikkojen nousemisen esille haastattelun edetessä. Haastatteluiden kannalta tunnistettiin kaksi toisistaan poikkeavaa asiantuntijuusaluetta – kyberturvallisuus ja kybervakuuttaminen – minkä perusteella päädyttiin valitsemaan haastateltavat henkilöt. Ensisijainen kriteeri haastateltavan henkilön valinnassa oli, että henkilöllä on vankka osaaminen joko kyberturvallisuudesta tai kybervakuuttamisesta. Soveltuviksi henkilöiksi tunnistettiin vakuutusyhtiöiden underwritingista ja tuotteistamisesta vastaavat henkilöt, kyberturvallisuuden tekniset asiantuntijat sekä yrityksen riskienhallinnasta vastaavat henkilöt. Useimmilla alalla työskentelevillä henkilöillä ei ole vankkaa osaamista sekä kyberturvallisuudesta että kybervakuuttamisesta, minkä vuoksi haastatteluihin pyrittiin valitsemaan tasapuolinen edustus molempien asiantuntijuusalueiden henkilöistä. Tutkielmaa varten haastateltiin kuutta henkilöä, joista kolme henkilöä on kyberturvallisuuden ja toiset kolme kybervakuuttamisen asiantuntijoita. Haastateltavien henkilöiden soveltuvuus pyrittiin varmistamaan selvittämällä etukäteen

haastateltavien kokemusta ja asiantuntijuusalueita sekä taustoittamalla heille tutkielman aihepiiriä.

Haastattelut toteutettiin marraskuussa 2017 ja tammikuussa 2018. Haastattelut toteutettiin pääsääntöisesti vakuutusyhtiöiden ja asiantuntijoiden edustamien yritysten toimitiloissa, joiden lisäksi yksi haastattelu suoritettiin Jyväskylän yliopistolla ja yksi haastattelu Tampereen yliopistolla. Haastattelut kestivät noin tunnin ja jokainen haastattelu suoritettiin yksitellen eli haastattelutilanteessa oli paikalla vain haastateltava ja tutkija.

Haastatteluita varten laadittiin ennalta erilliset haastattelurungot sekä kyberturvallisuus- että kybervakuutusasiantuntijoille. Kyberturvallisuusasiantuntijoiden haastattelussa käytettiin apuna liitteen 1 mukaista haastattelurunkoa ja kybervakuutusasiantuntijoiden haastattelussa käytettiin liitteen 2 mukaista haastattelurunkoa. Molemmissa haastattelurungoissa on yhteisenä osiona kyberriskien tunnistamista ja arviointia koskevat kysymykset, mutta kybervakuutusasiantuntijoille on liitteen 2 haastattelurungossa laajemmat kysymykset koskien kybervakuutusta. Kyberturvallisuusasiantuntijoiden haastattelurungossa pääpaino on kyberriskien tunnistamisessa ja arvioinnissa, kun taas kybervakuutusasiantuntijoiden haastattelurungossa kybervakuuttamista koskevat kysymykset saavat suuremman painoarvon. Tutkittavan aiheen monitahoisuudesta ja teemahaastattelun verrattain avoimesta luonteesta huolimatta keskustelut eivät juurikaan ajautuneet aihepiirien ulkopuolelle, ja haastattelijan oli mahdollista tarkentavilla kysymyksillä ohjata keskustelua oikeaan suuntaan.

Yhtä haastattelua lukuun ottamatta kaikki haastattelut taltioitiin äänitallenteena haastateltavien suostumuksella, jotta tutkija pystyi keskittymään täysipainoisesti haastatteluun ja esittämään täydentäviä kysymyksiä. Haastattelutallenteiden litterointi eli haastattelun puhtaaksikirjoittaminen suoritettiin pääsääntöisesti kahden päivän kuluessa haastattelusta, jotta voidaan varmistua siitä, että tutkija ei tulkitse haastateltavien vastauksia väärin. Yksi haastateltava halusi, että haastattelua ei taltioida äänitallenteena tietoturvasyistä. Tästä haastattelusta tehtiin kattavat muistiinpanot ja puhtaaksikirjoittaminen suoritettiin välittömästi haastattelun jälkeen, jotta väärinymmärrykset voitiin minimoida. Litteroitu haastattelumateriaali lähetettiin kaikille haastateltaville sähköpostitse tarkistettavaksi, jotta he pystyivät halutessaan tekemään korjauksia ja täydennyksiä vastauksiinsa. Tutkielman lopulliseen versioon käytetyt referoidut osiot haastatteluista sekä suorat lainaukset lähetettiin haastateltaville tarkistettavaksi,

jotta heillä oli mahdollisuus tehdä muutoksia ja korjauksia omista haastatteluistaan käytettyihin osuuksiin.

Tutkielman tarkoituksena on tehdä yrityskenttään kohdistuva yleiskatsaus, joten haastattelujen sisältö pidettiin yleistasoisena ja koko yrityskenttään kohdistuvana. Koska haastateltavat eivät tuoneet ilmi yrityskohtaisia ja salassa pidettäviä tietoja, käytetään tässä tutkielmassa haastateltavien suostumuksella heidän tehtävänimikettään ja edustamansa työnantajan nimeä. Haastateltavien aseman ja edustamansa yrityksen käyttäminen lisää tutkielman luotettavuutta ja luettavuutta, koska lukija voi vaivatta varmistua haastateltavan henkilön asiantuntemuksesta käsiteltävään aihepiiriin. Haastateltujen henkilöiden yksityisyyden vuoksi heidän nimiään ei ole mainittu ja heihin viitataan tutkielmassa kirjainten A–F tai heidän edustamansa yrityksen ja tehtävänimikkeen avulla.

Haastateltavat henkilöt on jaettu tutkielman teemojen mukaan kahteen ryhmään: kyberturvallisuuden ja kybervakuuttamisen asiantuntijoihin. Kyberturvallisuuden teemasta haastateltiin kolmea henkilöä:

- Asiantuntija A työskentelee Jyväskylän yliopistossa kyberturvallisuuden professorina, missä hän vastaa kyberturvallisuuden koulutusohjelmasta, tekee omaa tutkimusta ja ohjaa maisteriksi valmistuvia sekä tohtorikoulutettavia. Hän on tullut Jyväskylän yliopistoon rakentamaan kyberturvallisuuden koulutusohjelmaa vuonna 2009, minkä lisäksi hänellä on 30 vuoden kokemus puolustusvoimissa tiedustelun, valvonnan, johtamisen ja kyberturvallisuuden tehtävissä. Hän on väitellyt sotatieteiden tohtoriksi vuonna 2012. Asiantuntija A:n kyberturvallisuusosaaminen keskittyy kyberturvallisuusstrategioihin, sen johtamiseen ja sotilastaustan vuoksi myös kybersodankäyntiin.
- Asiantuntija B työskentelee Insta Group Oy:ssä turvallisuusjohtajana, missä hän vastaa konsernitasolla kokonaisturvallisuudesta, joka kattaa henkilöstö-, toimitila-, tieto- ja kyber-, ympäristö-, pelastus- ja työturvallisuuden sekä valmius- ja varautumissuunnittelun. Hänen vastuullaan ei ole Insta Groupin tuotteiden tieto- ja kyberturvallisuus, mutta hän on mukana eri foorumeissa, missä niitä kehitetään.
- Asiantuntija C työskentelee Insta DefSec Oy:ssä teknologiajohtajana, missä hän vastaa teknologiaratkaisuista ja tulevaisuuden tuotetarjoaman suunnittelusta kyberturvalli-

suuspalveluissa sekä yhteiskunnan kannalta kriittisille toimialoille suunnatuissa palveluissa. Haastateltava on koulutukseltaan filosofian maisteri ja tekee parhaillaan väitöskirjatutkimusta. Hänellä on vajaan 20 vuoden kokemus tietoturvasta ja hän on työskennellyt tietoturvan teknisten ratkaisujen ja identiteetinhallinnan asiantuntijana.

Kybervakuuttamisen asiantuntijoita haastateltiin kolme henkilöä:

- Asiantuntija D työskentelee Aon Finland Oy:ssä asiakaspäällikkönä ja kybervakuuttamisen asiantuntijana. Aon Finland tarjoaa palveluita sekä kyberriskien hallintaan että kybervakuuttamiseen, joista hän on erikoistunut kybervakuuttamiseen. Koulutukseltaan hän on diplomi-insinööri.
- Asiantuntija E työskentelee OP Vakuutus Oy:ssä Senior Underwriterina, missä hän toimii kybervakuutuksen tuotepäällikkönä. Haastateltavalla on kokemusta vakuutusalalta 1990-luvun lopulta saakka ja hän on ollut vuodesta 2013 lähtien mukana kybervakuutustehtävissä. Koulutukseltaan hän on yhteiskuntatieteiden maisteri.
- Asiantuntija F työskentelee If Vahinkovakuutus Oyj:ssä yritysten vastuuvakuutuksen tuotepäällikkönä, missä hänen vastuullaan on myös kybervakuuttaminen. Hän on ollut alusta lähtien mukana kehittämässä If Vahinkovakuutuksen Tietoturvavakuutusta, sen hinnoittelua ja ratkaisuja. Koulutukseltaan hän on juristi.

Tutkielman empiirinen aineisto koostuu edellä esiteltyjen haastateltavien näkemyksistä. Aineiston käsittely tehdään teemoittain, jonka avulla haastateltavien näkemykset voidaan koota yhteen ja jäsentää lukijan kannalta helposti luettavaan muotoon. Pääluvussa 4 keskitymme kyberriskien tunnistamiseen, arviointiin ja pilvipalveluiden vaikutukseen kyberturvallisuuteen, jossa empiirisen aineiston muodostavat pääasiassa kyberturvallisuusasiantuntijoiden haastattelut. Pääluvussa 5 käsittelemme kybervakuutusta, jossa kybervakuutusasiantuntijoiden haastattelut saavat suuremman painoarvon.

4.2 Kyberriskien tunnistaminen ja arviointi

Haastattelujen alussa haastateltavilta asiantuntijoilta kysyttiin, kuinka vakavana uhkana he pitävät kolmansia osapuolia kyberriskien aiheuttajina. Jo haastatteluiden alussa kävi selväksi,

että kaikki asiantuntijat pitävät juuri kolmansista osapuolista aiheutuvia kyberriskejä hyvin vakavana uhkana, mihin on herätty vasta viime aikoina. Useissa haastatteluissa nostettiin esille, että yritysten näkökulmasta toimintojen ulkoistaminen ja yhteistyökumppaneiden käyttäminen ei poista yrityksen riskejä, vaan se saattaa jopa kasvattaa niitä. Yritykset eivät välttämättä pääse tarkasti seuraamaan, mitä tietoja heidän yhteistyökumppaneillaan on ja kuinka ne käsittelevät niitä. Kyberturvallisuuden professorina toimiva asiantuntija A kuvailee kolmansista osapuolista aiheutuvien kyberriskien ydinongelmaa näkymän puutteeksi:

> *”Perusongelma liittyy kysymykseen siitä, kuinka hyvin yritys näkee omat IT-resurssinsa. Se tarkoittaa sitä, että kuinka hyvin on yrityksen tiedossa, missä sen softa ja hardware ovat olemassa. Siellä ääripäässä on pilvipalvelut, johon on siirretty kaikki yrityksen tiedot ja joku muu pyörittää sitä sinun puolesta. Peruskysymys on se, että kuinka hyvin sinä näet niihin palveluihin ja mikä on sinun todellinen näkymäsi. – – Riskienhallinnan näkökulmasta ongelma on, että silloin kun kaikki on sinun omissa käsissä, niin pystyt määrittelemään ja näkemään paljon helpommin minkälaisia riskejä näihin liittyy. Heti kun olet antanut palvelun jonkun kolmannen osapuolen käyttöön, niin se näkymä heikkenee.”*

Vaikka näkymän puute tunnistetaan keskeiseksi ongelmaksi kolmansista osapuolista aiheutuvissa kyberriskeissä, pyritään tässä tutkielmassa juuri sen vuoksi pureutumaan ongelmaan, miten niistä aiheutuvia kyberriskejä voidaan arvioida. Riskienhallintaprosessin ensimmäinen vaihe on riskien tunnistaminen, mikä kolmansien osapuolten kohdalla voi olla haastavaa. Insta DefSecin teknologiajohtajana toimivan asiantuntija C:n mukaan kyberriskien tunnistamisessa kartoitetaan ensin yrityksen omaisuuserät eli suojattavat kohteet, kuten aineettomat omaisuudet ja IT-järjestelmät. Suojattavien kohteiden tunnistamisen jälkeen tarkastellaan, missä järjestelmissä ne ovat ja mitkä kolmannet osapuolet pääsevät käyttämään kyseisiä tietoja. Kolmansien osapuolten osalta tutkitaan, miten niiden pääsyä ja järjestelmien käyttöä valvotaan ja ovatko kyseiset tahot luotettavia kyberturvallisuuden näkökulmasta. Kyberriskien tunnistamisessa olennaista on tiedon arvo. Yrityksen kannalta arvokkaimpiin omaisuuseriin tulee kohdistaa vahvimmat suojaustoimenpiteet, ja vähempiarvoiset kohteet jätetään kevyemmälle huomiolle, jotta koko yrityksen riskienhallinnasta ei tule liian raskasta.

Kolmansista osapuolista aiheutuvien kyberriskien tunnistaminen nähtiin prosessina hyvin samanlaisena kuin muidenkin riskien tunnistaminen. Aonin asiakaspäällikkönä ja kybervakuutusasiantuntijana toimivan asiantuntija D:n mukaan kolmansista osapuolista aiheutuvien kyberriskien tunnistaminen on normaalia riskienhallintatyötä eli ulkopuolisille yhteistyökumppaneille tehdään samanlaista auditointia kuin yritys tekee myös omille järjestelmilleen ja toimintatavoilleen. Asiantuntija A nostaa yhteistyökumppaneiden auditoinnista esille, että tilaajan ja tuottajan välinen suhde perustuu usein luottamukselle ja palvelutasosopimuksille, mutta varsinkin pienemmät yritykset pääsevät harvoin näkemään palveluntuottajalle, hoitavatko he tehtävänsä tilaajan haluamalla tavalla.

Kyberriskien – kuten muidenkin riskien – arvioinnissa riskien tunnistamisen jälkeen arvioidaan riskin suuruutta. Kaikki haastateltavat olivat yksimielisiä siitä, että kolmansista osapuolista aiheutuvien kyberriskien suuruuden arviointiin ei ole olemassa vakiintunutta menetelmää, jolla kyberriskille saataisiin määriteltyä rahamääräinen arvio. Kuten teorialuvussa 3.3.1 tuotiin esille, voidaan kyberriskien arviointiin käyttää kvantitatiivisia menetelmiä tai kvalitatiivisia asiantuntija-arvioon pohjautuvia menetelmiä. Insta Groupin turvallisuusjohtajana työskentelevä asiantuntija B sanoo, että he käyttävät sekä kvantitatiivisia että kvalitatiivisia menetelmiä kyberriskien suuruuden arviointiin. Hän huomauttaa, että menetelmästä riippumatta vahingon suuruuden arviointi on haastavaa ja joissakin tapauksissa jopa mahdotonta. Esimerkiksi maineen menettämisestä aiheutuvien kustannusten arvioiminen on hänen mukaansa haastavaa, koska heidän toimialallaan luottamuksen menettäminen tarkoittaisi pitkäaikaisia haittoja ja johtavan lopulta henkilöstövähennyksiin.

Asiantuntija C tuo esille, että he arvioivat kolmansista osapuolista aiheutuvia kyberriskejä hyvin yksinkertaisella menetelmällä, jolla riskin todennäköisyyttä ja vaikututusta arvioidaan. Riskin todennäköisyydestä ja vaikutuksesta muodostetaan riskimatriisi, jollainen esiteltiin luvussa 3.3.1 kvalitatiivisen riskien arvioinnin yhteydessä. Heillä riskimatriisia sovelletaan alihankkijoista aiheutuvissa kyberriskeissä siten, että ne riskit ovat hallittavissa ja niitä tarkkaillaan, jos ne ovat todennäköisiä mutta vaikutukseltaan mitättömiä tai todennäköisyys on mitätön mutta vaikutus on suuri. Jos riskit arvioidaan vakavaksi ja todennäköiseksi, pyrkivät he silloin vähentämään alihankkijoista aiheutuvia kyberriskejä. Asiantuntija C edustaa organisaa-

tiota, joka tuottaa palveluita kriittisen infrastruktuurin sektorille, joten heillä mahdollinen palveluiden ulkoistaminen toteutetaan hyvin tiukkojen kriteerien perusteella. Kolmansista osapuolista aiheutuvat kyberriskit ovat hänen mukaansa heillä lähtökohtaisesti epätodennäköisiä.

Sekä kvalitatiivisessa että kvantitatiivisessa kyberriskien arvioinnissa todennäköisyyden arvioiminen on haastavaa, kun arvioidaan nimenomaan kolmansista osapuolista aiheutuvia kyberriskejä. Teknologiajohtajana toimivan asiantuntija C:n mukaan kolmansista osapuolista aiheutuvien kyberriskien todennäköisyyden määrittäminen pohjautuu hyvin pitkälti asiantuntija-arvioon. Asiantuntija-arviota voidaan pohjata osittain esimerkiksi tietyntyyppisten tietomurtojen tai palvelunestohyökkäysten yleisyysasteella, koska tietojärjestelmien osalta haavoittuvuudet on luokiteltu melko kattavasti ja niistä on olemassa tilastotietoa. Hänen mukaansa keskeinen ongelma todennäköisyyden määrittämisessä on, että vaikka tilastotietoa verkkohyökkäyksistä on olemassa, ei todennäköisyyden määrittäminen niiden pohjalta ole mahdollista. Hän havainnollistaa esimerkillä, että maailmanlaajuisesti alihankkijoiden kautta aiheutuvia tietomurtoja voi tapahtua vuodessa esimerkiksi 100 000 tapausta, mutta siitä ei voida päätellä onko se paljon vai vähän ja mikä on sen riskin todennäköisyys tiettyä yritystä kohden. Asiantuntija-arvioissa tilastotietoa voidaan käyttää apuna, kun suhteutetaan kolmansien osapuolten kautta aiheutuneita tietomurtoja kaikkiin muihin vuoden aikana toteutuneisiin tietomurtoihin.

Vakuutusmeklariyhtiötä edustavan asiantuntija D:n mukaan he käyttävät kvantitatiivisia arvioita kyberriskien suuruudesta, kun he arvioivat asiakkaan kanssa kybervakuutuksen tarvetta ja mahdollisia kyberriskeistä aiheutuvia vahinkoja. Tällaisissa arvioissa he määrittelevät tiettyjä euromääräisiä arvioita esimerkiksi kolmannen osapuolen aiheuttamalle keskeytysvahingolle tai henkilötietojen vuotamiselle ulkopuolisille.

Kaikissa haastatteluissa nousi esille, että juuri kolmansista osapuolista aiheutuvien kyberriskien suuruuden arviointiin ei toistaiseksi ole erillistä menetelmää eli niiden vaikutusten arviointiin käytetään samankaltaisia menetelmiä kuin muidenkin kyberriskien arviointiin. Asiantuntija A nostaa esille, että hänen tiedossaan ei ole, että juuri kolmansista osapuolista aiheutuvien kyberriskien mittaamiseen olisi olemassa jotakin tiettyä menetelmää. Hänen mukaansa perinteiset riskimatriisit ovat yleisesti käytössä olevia riskien arviointimenetelmiä, ja samat

lainalaisuudet pätevät kolmansista osapuolista aiheutuvien kyberriskien arviointiin kuin muidenkin kyberriskien arviointiin.

Kuten tässä luvussa on aiemmin mainittu, asiantuntija C:n mukaan kyberriskien arvioinnissa kartoitetaan ensin yrityksen kannalta keskeiset omaisuuserät eli suojattavat kohteet. Myös asiantuntija A on samoilla linjoilla, eli toimialasta riippumatta ensin tulee kartoittaa yrityksen kannalta kriittiset prosessit. Usein tällaisille toiminnoille voidaan asettaa esimerkiksi tiettyjä vasteaikoja, joissa niiden tulee olla takaisin toiminnassa. Kriittisten prosessien ja niihin kohdistuvien kyberriskien arvioinnin osalta asiantuntija C nostaa esille tärkeän seikan; usein kaikista tärkeimmät prosessit tunnistetaan hyvin ja niiden suojaamiseen käytetään jopa liikaa resursseja. Hänen mukaansa kaikista tärkeimpien prosessien ja omaisuuserien ohella yrityksissä voi olla suuri määrä vähemmälle huomiolle jääneitä toimintoja, joihin sitoutuu kuitenkin runsaasti tietoa tai yritys on niiden toiminnasta riippuvainen. Se voi johtaa tilanteeseen, että kaikista kriittisimmät mutta määrältään suhteellisen pieni osa tiedoista on hyvin suojattu, mutta niiden alle jäävä suuri tietomassa on vailla riittävää suojausta.

Yhteenvetona kolmansista osapuolista aiheutuvien kyberriskien arviointiin voidaan todeta, että kolmansista osapuolista aiheutuvia kyberriskejä voidaan parhaiten tunnistaa yrityksen kannalta kriittisten prosessien ja omaisuuserien tunnistamisella. Samalla kartoitetaan, mitä tietoa kolmansilla osapuolilla on, ketkä niitä pääsevät käsittelemään ja päästäänkö heidän toimintaansa auditoimaan. Kolmansista osapuolista aiheutuvien kyberriskien suuruuden arvioinnissa oli vastauksissa hajontaa eli niiden arviointiin käytetään sekä kvantitatiivisia että kvalitatiivisia menetelmiä. Vastausten perusteella kvalitatiiviset arviointimenetelmät ovat yleisempiä niiden yksinkertaisemmasta luonteesta johtuen, mikä vahvistaa luvussa 3.3.1 esitettyä näkemystä kvalitatiivisten menetelmien ja erityisesti riskimatriisien yleisyydestä. Vastauksista käy myös ilmi, että kolmansista osapuolista aiheutuvien kyberriskien suuruuden arviointiin ei ole olemassa erityistä menetelmää, vaan niitä arvioidaan samankaltaisilla menetelmillä kuin muitakin kyberriskejä ja niihin pätevät samat lainalaisuudet.

4.3 Tyypilliset kyberuhat ja haavoittuvuudet

Luvussa 2.2 käsittelimme kyberuhkia, haavoittuvuuksia ja erilaisia toimijoita kyberuhkien taustalla. Erityisesti kyberturvallisuusasiantuntijoiden haastatteluissa nousi esille, että kolmansista osapuolista aiheutuvat kyberuhat voivat olla hyvin erilaisia riippuen yrityksen toimialasta. Asiantuntija B:n mukaan heidän konsernilleen tyypillisiä kyberuhkia ovat sähköpostien mukana tulevat haittaohjelmalinkit, jotka ovat heille arkipäiväisiä uhkia. Haittaohjelmalinkkien lisäksi yleisiä ovat toimitusjohtajahuijaukset, jotka pyrkivät suorittamaan tilisiirron yrityksen johdon nimissä. Näiden lisäksi heille yleinen kyberuhka on verkkourkinta.

Erityisesti kolmansien osapuolten aiheuttamista kyberuhista asiantuntija D nostaa esille pilvipalvelut ja muut vastaavat tietojenkäsittelyä ulkoistavat palvelut, joiden kautta aiheutuu uhka tietovuodoista. Hänen mukaansa toinen merkittävä kolmansista osapuolista aiheutuva kyberuhka on keskeytysvahingon aiheuttava tapahtuma, jos kolmannen osapuolen tarjoamat järjestelmät eivät toimi odotetulla tavalla, esimerkiksi palvelunestohyökkäyksen seurauksena.

Haastatteluissa nousi verrattain vähän esille erilaiset kyberuhat, mutta sitäkin korostuneemmin esillä olivat erilaiset haavoittuvuudet. Asiantuntija A:n mukaan suurin osa kyberhyökkäyksistä, riippumatta mitä kautta ne tulevat, johtuu ohjelmistohaavoittuvuuksista. Arvioiden mukaan noin 10 prosenttia ohjelmistokoodeista sisältää ohjelmointivirheitä, minkä seurauksena ne aiheuttavat haavoittuvuuksia ja avaavat mahdollisuuksia verkkohyökkäyksille. Kolmansista osapuolista puhuttaessa hän huomauttaa, että alihankkijat osana tuotantoketjua käyttävät lukuisia erilaisia ohjelmistoja, jotka sisältävät erilaisia haavoittuvuuksia. Tuotantoketjussa olevat alihankkijat ja niiden haavoittuvuudet mahdollistavat verkkohyökkäyksen läpipääsyn, jolloin hyökkääjät pääsevät kohdeyrityksen tietoihin ja järjestelmiin käsiksi.

Myös vakuutusyhtiöiden näkökulmasta yrityksen ja alihankkijan välinen suhde nähdään ongelmallisena, koska se voi aiheuttaa haavoittuvuuksia. If Vahinkovakuutuksen kyber- ja vastuuvakuutuksen tuotepäällikkönä toimiva asiantuntija F tuo esille, että kybervakuuttaminen on suhteellisen uusi vakuutus, minkä vuoksi heidän omasta vakuutuskannasta ei voi vielä tunnistaa keskeisiä haavoittuvuuksia. Hänen mielestään yrityksen ja alihankkijan välisessä suhteessa haasteita aiheuttaa tunnuksien, tunnistautumisen ja valtuuksien määrittely. Yrityksellä

ei välttämättä ole tietoa, ketkä pääsevät yrityksen tietoihin ja järjestelmiin käsiksi, mikä voi aiheuttaa vakavia haavoittuvuuksia. Sen lisäksi hän mainitsee, että yrityksen ja alihankkijan välinen yhteys voi olla heikommin suojattu kuin yrityksen sisäisissä järjestelmissä, mikä voi tarjota verkkohyökkääjille mahdollisuuden hyödyntää kyseisiä haavoittuvuuksia.

Asiantuntija A:n mukaan ohjelmistohaavoittuvuuksien lisäksi esimerkiksi yritysten turvallisuusprosessit voivat sisältää haavoittuvuuksia. Hän tuo esille tutkimuksia, joiden mukaan alle 10 prosentilla yrityksistä on erittäin nopea reagointi kyberhyökkäyksiin, 20 prosentilla se on nopea ja noin 70 prosentilla yrityksistä ei välttämättä ole kykyä havaita, onko joku tehnyt heille kyberhyökkäyksen. Keskimääräisesti yrityksiltä kestää havaita kyberhyökkäys, pois lukien palvelunestohyökkäys, noin puoli vuotta. Kun yrityksillä on useita alihankkijoita, eikä niillä ole kattavaa näkymää alihankkijoidensa turvallisuusprosesseihin, aiheuttavat alihankkijoiden ohjelmistohaavoittuvuudet yhdessä yrityksen omien turvallisuusprosessien heikkouksien kanssa vakavia haavoittuvuuksia. Tietojärjestelmä- ja ohjelmistohaavoittuvuuksista asiantuntija C nostaa esille, että kun järjestelmissä on haavoittuvuus ja se on julkista tietoa, sitä ei käytä enää kukaan. Haavoittuvuus on olemassa, kun sitä ei vielä tiedetä. Sen vuoksi heidän pitää olla valmistautuneita, että järjestelmissä ja ohjelmistoissa on koko ajan haavoittuvuuksia. Hän painottaa, että heidän pitää pystyä havaitsemaan, kun murto tapahtuu. Tästä hän käyttää reaktiivisen suojauksen käsitettä, mikä tarkoittaa yrityksen havainnointikyvykkyyttä, kun tietomurto tapahtuu. Sen lisäksi käytetään myös proaktiivista suojausta, joka tarkoittaa perinteisiä menetelmiä eli esimerkiksi palomuureja.

Asiantuntija C mainitsee henkilöstön merkityksen haavoittuvuutena, jota käsiteltiin muiden haavoittuvuuksien ohella luvussa 2.2.1. Hän ottaa esimerkikseen tilanteen, jossa kolmansia osapuolia eli yrityksen ulkopuolisia tahoja tulee luvallisesti heidän tiloihinsa tai heidät päästetään yrityksen järjestelmiin suorittamaan toimenpiteitä. Tällaisissa tilanteissa suurin haavoittuvuus on yrityksen henkilöstö, jota voidaan yrittää manipuloida eli saada paljastamaan tietoja tai antamaan pääsy salassa pidettäviin tietoihin. Myös asiantuntija D mainitsee, että henkilöstöön ja inhimillisiin virheisiin liittyvät haavoittuvuudet ovat saaneet merkittävän painoarvon.

Henkilöstön lisäksi erilaiset kyberuhat voivat olla hyvin arkipäiväisiä, joihin yritykset eivät ole välttämättä osanneet kiinnittää huomiota. Asiantuntija C:n edustama yritys tarjoaa kyberturvallisuuspalveluita asiakkailleen, jolloin he ensin pyytävät asiakkaitaan kuvaamaan liiketoimintansa. Hänen mukaansa tällaisissa tilanteissa asiakkaat voivat keskittyä kertomaan tärkeät yksityiskohdat ydintoiminnoistaan, mutta voivat unohtaa vähemmälle huomiolle jäävät kolmannet osapuolet, kuten aulatyöntekijät, siivoojat ja muut alihankkijat, jotka tulevat heidän tiloihinsa tekemään esimerkiksi huolto- ja asennustöitä. Myös tällaiset hyvin yksinkertaisilta vaikuttavat tekijät voivat olla haavoittuvuus yritykselle.

Vaikka kyberriskit voivat aiheutua muusta kuin rikollisesta toiminnasta, esimerkiksi inhimillisistä virheistä, nousi haastatteluissa rikollinen toiminta korostuneesti esille. Kyberrikollisuuden lisäksi kyberturvallisuusasiantuntijoiden haastatteluissa nousivat esille yritysten ja valtioiden suorittama kybervakoilu, haktivismi ja kybervaikuttaminen. Asiantuntija A:n haastattelussa tuli esille kyberrikollisuuden suuri mittakaava. Kyberrikollisuudessa liikkuu vuosittain noin 400 miljardia dollaria ja sen taustalla on lukematon määrä erilaisia toimijoita, esimerkiksi järjestäytynyttä rikollisuutta ja pienempiä yksittäisiä tahoja, joiden kaikkien motiivina on hankkia rahaa. Hän tuo esille, että kyberrikollisuus on järjestäytynyttä, kuten moni muukin rikollisuus. Rikollisista osa tuottaa hyökkäysohjelmia, etsii haavoittuvuuksia ja myy niitä eteenpäin. Näiden lisäksi on hyökkäyksiä tekevät tahot ja rikollisella toiminnalla saatujen varoja käsittelevät tahot. Kybervakoilussa on myös järjestäytynyttä toimintaa eli on olemassa organisaatioita, jotka hankkivat esimerkiksi kilpailijayrityksistä salaista tietoa.

Sekä Insta Groupin turvallisuusjohtajan että Insta DefSecin teknologiajohtajan mukaan heidän toimialalleen on kyberrikollisuuden ohella tyypillistä valtiollinen kybervakoilu ja haktivismi, jossa jokin aktivistijärjestö yrittää lamauttaa heidän toimintaansa. Insta DefSec toimii puolustusteknologiaa tarjoavalla alalla ja on mukana suurissa projekteissa, minkä vuoksi valtiollinen kybervakoilu on heille todellinen uhka. Kybertoimintaympäristössä on lukuisia erilaisia toimijoita eri motiiveilla, mutta kyberturvallisuusasiantuntijoiden haastatteluista voidaan päätellä, että rikollinen toiminta ja rahan ansaitseminen motiivina ovat vakavin ongelma.

Oman toimialansa ulkopuolelta asiantuntija C mainitsee, että tietyillä toimialoilla haktivismi ja julkisuutta tavoitteleva toiminta voivat olla yleisiä. Hän vertaa, että pienenkin yrityksen asiakas- ja henkilötiedoilla haktivistit voivat saada huomattavaa mediajulkisuutta, mutta vastaavasti pienemmän yrityksen internetsivujen kaatamisella hakkerit eivät saisi julkisuutta.

Haastattelujen perusteella voidaan yhteenvetona todeta, että kyberuhat saivat haastatteluissa verrattain vähän huomiota. Niistä tärkeimmiksi nousivat haittaohjelmat ja mahdolliset tietovuodot kolmansien osapuolten kautta. Haittaohjelmien ja tietovuotojen nouseminen esille vakavimpina kyberuhkina tukivat teoriaosuudessa esitettyä näkemystä vakavimmista kyberuhista. Haastatteluissa erilaiset haavoittuvuudet saivat suuremman painoarvon. Suurimmassa osassa haastatteluita ohjelmistoihin ja tietojärjestelmiin liittyvät haavoittuvuudet nostettiin vakavimmiksi haavoittuvuuksiksi. Myös yrityksen ja alihankkijan välinen suhde nähtiin ongelmallisena, ja merkittävänä uhkana nähtiin kyberhyökkääjien mahdollisuus hyödyntää jonkin alihankkijan heikompaa tietoturvaa tai haavoittuvuutta, jonka avulla ne pääsevät murtautumaan toimitusketjussa olevien muiden yritysten tietoihin tai järjestelmiin. Jo edellisessä alaluvussa mainittu näkymän puuttuminen alihankkijaverkostoon tuli esille myös haavoittuvuuksia käsiteltäessä, koska yrityksellä ei ole kykyä havaita riittävän nopeasti tietomurtoja, jos sillä ei ole näkymää alihankkijoidensa tietojärjestelmiin ja sitä kautta mahdollisuutta seurata mahdollisia tietomurtoja.

Erilaisten kyberriskien taustalla olevista toimijoista ja motiiveista kaikilla haastateltavilla oli hyvin samansuuntainen kuva. Kyberrikollisuus ja nopea rahan ansaitseminen mainittiin lähes poikkeuksetta ensimmäisenä, mikä vahvistaa kuvaa kyberrikollisuuden suuresta mittakaavasta. Haastattelujen perusteella kyberriskien taustalla olevat toimijat ovat samoja riippumatta siitä, kohdistuuko hyökkäys suoraan yritykseen vai tuleeko se esimerkiksi jonkin alihankkijan tai yhteistyökumppanin kautta sen heikomman kyberturvallisuuden seurauksena. Kyberrikollisia motivoi raha ja he etsivät heikoimman kohdan yrityksen tai sen toimitusketjun jäsenten järjestelmistä ja prosesseista. Kyberrikollisuuden yleisyys tuki teoriaosuudessa esitettyä näkemystä kyberriskien aiheuttajista, mutta inhimillisten virheiden merkitys jäi haastatteluissa oletettua vähemmälle huomiolle.

4.4 Pilvipalveluiden vaikutus kyberturvallisuuteen

Haastattelujen edetessä kysymys pilvipalveluiden vaikutuksesta yritysten kyberturvallisuuteen sai aikaan vilkasta ja pohdiskelevaa keskustelua, ja se todettiin myös hyvin ajankohtaiseksi aiheeksi. Kaikissa haastatteluissa kävi ilmi, että ei ole yksiselitteistä vastausta, parantaako vai heikentääkö pilvipalveluiden käyttäminen yrityksen kyberturvallisuuden tasoa. Joissakin tapauksissa pilvipalveluiden käyttäminen voi merkittävästi parantaa kyberturvallisuuden tasoa, mutta toisaalta korkean turvaluokituksen tietoja käsiteltäessä pilvipalveluiden voidaan katsoa heikentävän sitä. Haastateltavien mukaan voidaan yleisesti nähdä, että erityisesti pienten yritysten kohdalla pilvipalveluiden ja ammattimaisten IT-palveluita tarjoavien yritysten palveluiden käyttäminen parantaa kokonaiskyberturvallisuutta. Siitä huolimatta ei voida tehdä johtopäätöstä yrityksen koon ja kyberturvallisuuden välillä olevasta yhteydestä, koska kyberturvallisuuteen vaikuttavat myös monet muut tekijät. Yleisesti ottaen suuremmilla yrityksillä kyberturvallisuus on otettu paremmin huomioon, mutta eräs haastateltavista totesi myös suurissa yrityksissä olevan tunnettuja tapauksia, joilla kyberturvallisuus on heikolla tasolla.

Kyberturvallisuusasiantuntijat suhtautuivat pilvipalveluihin hieman kriittisemmin kuin kybervakuutusasiantuntijat, mutta molemmat näkivät niiden käyttämisessä kuitenkin selkeitä etuja yleisellä tasolla. Asiantuntija A ottaa esille pilvipalveluiden hyviä ja huonoja puolia: fyysisen turvallisuuden osalta pilvipalveluiden käyttäminen poistaa esimerkiksi tulipalo- ja vesivahinkoriskin sekä omiin palvelimiin suoraan kohdistuvan kyberhyökkäysriskin, joiden voidaan yleisesti katsoa lisäävän kyberturvallisuutta. Toisaalta suuren tietomäärän kasautuminen yhteen pilvipalveluun tekee siitä houkuttelevan kohteen kyberrikollisille, koska he voivat saada yhdestä paikasta suuren määrän arvokasta tietoa. Sen lisäksi suuren tietomäärän keskittyminen yhteen palveluun lisää riskiä häiriöille eli häiriö yhdellä palveluntarjoajalla vaikuttaa suureen määrään sitä käyttäviä asiakkaita.

Asiantuntija A kertoo yhteistyössä Aalto yliopiston kanssa tekemästään kansallista kyberturvallisuutta koskevasta raportista, josta ilmeni viimeaikainen suuntaus kriittisempään suhtautumiseen pilvipalveluiden hyödyntämisessä. Hänen mukaansa osa kriittisen infrastruktuurin

toimijoista, jotka ovat aiemmin ulkoistaneet ydintoimintojensa tietojenkäsittelyä ja varastointia pilvipalveluihin, ovat sittemmin päätyneet siirtämään kriittisimpien toimintojensa osalta näitä osia takaisin itselleen. Yritykset pohtivat kaikkein kriittisimpien prosessiensa osalta, ovatko ne turvallisempi pitää omassa kontrollissa. Vastaavasti sellaiset toiminnot, jotka eivät yrityksen kannalta ole kriittisiä, voidaan ulkoistaa erilaisiin pilvipalveluihin, jolloin niiden edut tulevat esille. Erityisesti suuremmilla yrityksillä, joilla on resursseja omiin ja tarpeeksi turvallisiin IT-järjestelmiin, on kriittisimpien toimintojen pitäminen itsellään perusteltua ja järkevää.

Myös muut haastatellut kyberturvallisuusasiantuntijat suhtautuivat hieman varauksella pilvipalveluihin, mutta samalla myös tunnistivat niistä saatavat hyödyt. Osaltaan varauksellisen suhtautumiseen vaikuttaa heidän toimialansa, koska he tuottavat muun muassa puolustusteknologian palveluita, joka aiheuttaa heille rajoitteita tietojen salassapidosta. Lisäksi rajoitteena voi olla, että tietoja ei saa fyysisesti säilyttää Suomen tai Euroopan unionin ulkopuolella, mitä voi olla vaikea valvoa pilvipalveluissa. Tämä näkemys tukee teoriaosuudessa esitettyä ongelmakohtaa pilvipalveluiden käyttämien palvelimien fyysisestä sijainnista, koska asiakkaat eivät välttämättä tiedä, missä heidän tietonsa fyysisesti sijaitsevat ja minkä valtion lainsäädännön alaisuudessa ne ovat.

Asiantuntija C mainitsee pilvipalveluntarjoajista näkymän puuttumisen, mikä tuli esille aiemmin luvussa 4.2. Yritykset käyttävät paljon pilvipalveluita, mutta se on tällä hetkellä vielä tavallaan hallitsematon riski, koska ulkoistavilla yrityksillä ei ole näkymää, miten pilvipalveluntarjoajat käsittelevät ja säilyttävät heidän tietojaan. Hän tuo esille, että pilvipalveluita tarjoavat usein suuret monikansalliset yritykset, ja Suomessakin verrattain suurilla yrityksillä ei ole mahdollisuutta päästä auditoimaan tällaisia pilvipalveluntarjoajia. Suurten palveluntarjoajien kohdalla auditointimahdollisuuden puuttuessa yritysten on luotettava siihen, mitä palveluntarjoajat raportoivat omasta toiminnastaan ja käytännöistään. Vaikka pilvipalveluntarjoajilla ensisijaisena intressinä on turvallisuus oman maineriskinsä vuoksi, eivät asiakkaat voi olla täysin varmoja heidän toimintatavoistaan. Asiantuntija C:n näkemys on, että pienemmissä toiminnoissa pilvipalveluita käytetään yhä enemmän, koska se pienentää yritysten kiinteitä investointeja IT-järjestelmiin, mutta kääntöpuolena omat resurssit ja niiden kontrolli on ulkoistettu.

Asiantuntija C:n kanssa samassa konsernissa turvallisuusjohtajana työskentelevällä asiantuntija B:llä on samankaltainen suhtautuminen pilvipalveluihin. He käyttävät ulkoisen palveluntarjoajan tuottamia ICT-järjestelmiä, joiden lisäksi heillä on käytössä pilvipalveluita automaatioliiketoiminnassaan. Parhaillaan he ovat hankkimassa laajempaan käyttöön pilvipalvelupalvelujärjestelmää asiakastiedon hallintaan. Ongelmalliseksi hän näkee sen, että pilvipalveluista aiheutuvia riskejä on vaikea arvioida ja millä perusteilla sellainen järjestelmä voidaan ottaa käyttöön. Ulkoisista ICT-palveluista ja pilvipalveluista aiheutuvia riskejä hallitakseen he ovat tehneet turvallisuussopimuksia, palvelutasosopimuksia ja vaitiolositoumuksia. Lisäksi he edellyttävät palveluntuottajalta kriteerien mukaista turvallisuudenhallintajärjestelmää ja henkilöiden taustat tarkistetaan. Pilvipalveluiden ja ulkoisen ICT:n riskiksi hän näkee sen, että sitä käyttävillä henkilöillä on pääsy sellaiseen tietoon, johon heillä ei ole oikeutta. Sitä he pyrkivät hallitsemaan niin, että he näkevät koko ajan, mitä eri henkilöt tekevät heidän tiedoillaan.

Yleisesti ottaen kybervakuutusasiantuntijat suhtautuivat pilvipalveluihin avoimemmin kuin kyberturvallisuusasiantuntijat. He näkivät pilvipalveluiden useimmiten parantavan kyberturvallisuutta, mutta myös he tunnistivat, että tietyissä tilanteissa pilvipalveluiden käyttäminen voi lisätä kyberriskien mahdollisuutta. OP Vakuutuksessa kybervakuuttamisen Senior Underwriterina työskentelevä asiantuntija E toteaa pilvipalveluista:

> *”Yleisesti peukalosääntönä voi sanoa, että tällaisten ammattimaisten palveluiden käyttäminen vähentää sitä riskiä, koska aika harvoilla yrityksillä – isot yritykset mukaan lukien – se oman tietoturvan taso on niin korkea. Ainakin mitä me keskustelemme meidän tietoturvakumppaneiden kanssa, niin kyllä pääsääntöisesti harvalla oman tietoturvan taso on niin hyvä. Minä olen lähtenyt siitä olettamuksesta, että ulkoisten palveluiden käyttäminen todennäköisesti parantaa sitä tilannetta. – – Se ei kuitenkaan välttämättä korreloi yrityksen koon kanssa. Käytämme CGI:tä kumppanina kybervakuutuksessa, niin he joskus kehuivat esimerkiksi Nokiaa tuolta osin, että siellä tilanne on hyvä, mutta noin pääsääntöisesti korjattavaa on kutakuinkin kaikilla.”*

Asiantuntija E kuvailee pilvipalveluiden vaikutusta kyberturvallisuuteen kaksiulotteiseksi. Joissakin tilanteissa niiden käyttäminen voi parantaa kyberturvallisuutta, mutta joissakin tapauksissa se voi heikentää kyberturvallisuuden tasoa. Hänen mukaansa vaikutus riippuu hyvin pal-

jon siitä yrityksestä ja sen lähtötilanteesta, joka palveluita on ulkoistamassa. Useimmiten pienten yritysten kohdalla, joilla ei ole resursseja yrityksen sisäisiin ja turvallisiin IT-järjestelmiin, pilvipalveluiden käyttäminen yleensä parantaa yrityksen kyberturvallisuutta. Toisaalta jos yrityksen kyberturvallisuuden taso on jo valmiiksi korkealla tasolla, voi pilvipalveluiden käyttäminen heikentää kyberturvallisuutta. Kyberturvallisuuden parissa edistyneempien toimijoiden hän uskoo jo lähtökohtaisesti selvittävän tarkempaan, millaiselle palveluntuottajalle se toimintojaan ulkoistaa ja tekevän tarkat sopimukset, jotta kyberturvallisuuden taso pysyy samana tai paranee.

Myös kolmas kybervakuutusasiantuntija on samoilla linjoilla. Hänen mukaansa ei voi suoraan ja yksiselitteisesti sanoa, parantaako pilvipalveluiden käyttäminen yrityksen kyberturvallisuuden tasoa. Asiantuntija F antaa esimerkin kahdesta pienehköstä yrityksestä: toisella yrityksellä kaikki tiedot ovat omilla tietokoneillaan ja kovalevyillään, ja toinen yritys käyttää toiminnassaan esimerkiksi pilvipalveluita ja laskutuspalveluita eikä sillä ole juurikaan omia järjestelmiä. Ensimmäisen yrityksen tapauksessa riski voi realisoitua nopeasti, jos sen tallennusjärjestelmä rikkoutuu tai siihen kohdistuu kyberhyökkäys. Vastaavasti toisen yrityksen tapauksessa, jos se käyttää ammattimaisia ja tunnettuja palveluntarjoajia, kyberturvallisuus on paremmalla tasolla. On epätodennäköisempää, että suureen pilvipalveluntarjoajaan tehdään onnistunut tietomurto, koska tällaisilla suurilla toimijoilla suojaukset ovat korkealla tasolla ja niihin on vaikea murtautua. Hänen mukaansa pienten yritysten kohdalla, joilla on lähtökohtaisesti heikko suojaus IT-järjestelmissä, on usein parempi, että he käyttävät tunnettuja pilvipalveluntarjoajia. Myös asiantuntija F on muiden kybervakuutusasiantuntijoiden kanssa samaa mieltä, että suurempien yritysten tapauksissa ei voi yksiselitteisesti sanoa, johtaako pilvipalveluiden käyttäminen parempaan kyberturvallisuuteen.

Pilvipalveluiden käyttäminen on yleistynyt viime vuosina nopeasti ja niiden edut ovat monille yrityksille kiistattomia. Sen vuoksi kysymys niiden vaikutuksesta kyberturvallisuuteen on ajankohtainen ja se herätti haastateltavissa pohdintaa. Yhteenvetona haastatteluiden perusteella voidaan todeta, että kyberturvallisuusasiantuntijat suhtautuivat hieman varovaisemmin pilvipalveluiden hyödyntämiseen, vaikka myös he näkivät pilvipalveluissa selkeitä hyötyjä. Keskeisinä kysymyksinä ja huolenaiheina nähtiin erityisesti näkymän ja auditointimahdollisuuden

puuttuminen. Kybervakuutusasiantuntijoiden suhtautuminen pilvipalveluihin oli hieman positiivisempi, ja erityisesti pienten yritysten kohdalla pilvipalveluiden katsottiin parantavan kyberturvallisuutta. Suurempien yritysten tapauksessa tilanne ei ole niin yksiselitteinen, sillä se riippuu yrityksen alkuperäisestä lähtötilanteesta, parantaako vai heikentääkö pilvipalveluiden käyttäminen heidän kyberturvallisuuttaan. Yrityksen koon ja kyberturvallisuuden tason välillä ei välttämättä ole korrelaatiota, vaan myös suurissa yrityksissä voi olla tapauksia, joissa lähtötilanne on heikompi ja pilvipalvelut parantaisivat kokonaiskyberturvallisuutta.

Teorialuvussa 3.1.1 todettiin, että pilvipalvelut voivat parantaa yrityksen kyberturvallisuutta, jos pilvipalveluntarjoajan kyberturvallisuuden taso on korkeampi kuin ulkoistavalla yrityksellä. Teorialuvussa tuotiin myös esille, että ei voida yksiselitteisesti päätellä, parantaako vai heikentääkö pilvipalveluiden käyttäminen yrityksen kyberturvallisuutta. Tässä alaluvussa esitettyjen haastatteluiden perusteella voidaan todeta, että empiiriset havainnot tukevat teoriassa esitettyä näkemystä pilvipalveluiden vaikutuksesta kyberturvallisuuteen kokonaisuutena.

5 KYBERVAKUUTUS RISKIENHALLINTAKEINONA

5.1 Aineiston kuvaus

Tässä luvussa käsittelemme kybervakuutusta riskienhallintakeinona ja tarkastelemme, kuinka kybervakuutuksella voi suojautua kolmansien osapuolten aiheuttamia kyberriskejä vastaan. Aineistona on OP:n ja If Vahinkovakuutuksen kybervakuutusasiantuntijoiden haastattelut, joiden näkemykset perustuvat edustamiensa yhtiöiden kybervakuutustuotteisiin. Lisäksi aineistona käytetään vakuutusmeklariyhtiö Aonin kybervakuutusasiantuntijan haastattelua. Vakuutusmeklariyhtiön näkökulma tuo laajempaa näkemystä edellä mainittujen vakuutusyhtiöiden edustajien haastatteluun, koska vakuutusmeklariyhtiö toimii erilaisten asiakkaiden ja vakuutusyhtiöiden kanssa, joten heillä on laajempi näkemys eri vakuutusyhtiöiden tuotteiden eroavaisuuksista. Haastatellut asiantuntijat on esitelty luvussa 4.1, ja tässä luvussa aineistona käytetään kybervakuutusasiantuntijoiden D, E ja F haastatteluita.

5.2 Kybervakuutuksen kattavuus kolmansien osapuolten aiheuttamissa vahingoissa

OP tarjoaa asiakkailleen kahta kybervakuutustuotetta: suurasiakkaille tarkoitettua laajempaa ja räätälöityä kybervakuutusta sekä vakiomuotoista kybervakuutusta pk-yrityksille, joiden vuotuinen liikevaihto on alle 25 miljoonaa euroa. Pk-yrityksille tarkoitettu kybervakuutus sisältää ulkopuoliselle aiheutuvia vahinkoja kattavan vastuuvakuutuksen sekä yritykselle itselleen aiheutuvista kuluista keskeytysvakuutuksen ja kuluturvan, joka sisältää tietoturvayhtiön, asianajotoimiston ja viestintätoimiston palveluita. Lisäksi kybervakuutuksesta voidaan korvata mahdollisia kiristysvahinkoja, jos lunnasvaatimusten maksaminen on vahinkotilanteessa edullisempaa kuin vahingon selvittäminen keskeytysvahingon pitkittyessä. Suuryrityksille tarkoitettu kybervakuutus on laajemmin muokattavissa ja se voi sisältää edellä mainittujen turvien lisäksi IT-konsulttivastuuvakuutuksen, multimediavastuuvakuutuksen, luotonvalvontapalveluita ja kuluturvan mahdollisille viranomaisten langettamille sanktioille. Sekä ulkopuolisille että yritykselle itselleen aiheutuvia kuluja ja niiden korvattavuutta käsiteltiin tarkemmin kybervakuutusta käsittelevässä luvussa 3.4.

Kun tarkastellaan kybervakuutusten kattavuutta kolmansista osapuolista aiheutuvissa vahingoissa, eritellään vahingot vastuuvahinkoihin ja riippuvuuskeskeytysvahinkoihin. Asiantuntija E toteaa, että vastuuvahinkojen osalta tilanne on yksinkertaisempi, ja molemmat heidän kybervakuutustuotteistaan kattavat vastuuvahingot riippumatta siitä, säilytetäänkö tietoja yrityksen omilla palvelimilla tai esimerkiksi pilvipalveluissa. Vastuuvahinko voi syntyä, jos esimerkiksi yrityksen asiakkaiden henkilötietoja pääsee ulkopuolisille. Tällaisessa tapauksessa OP:n molemmat kybervakuutustuotteet kattaisivat vahingon, vaikka henkilötiedot olisivat vuotaneet ulkopuolisille esimerkiksi alihankkijan tai muun tallennuspalvelun kautta.

Riippuvuuskeskeytysvahingot ovat vakuuttamisen näkökulmasta haastavampia ja tällaisissa tapauksissa on kyse muusta kuin pelkästä tiedon säilyttämisestä. Riippuvuuskeskeytys voi aiheutua yritykselle tärkeän palveluntuottajan kyvyttömyydestä tarjota palveluitaan – esimerkiksi, jos yksi palveluntarjoaja tuottaa yritykselle kaikki IT-järjestelmäpalvelut. Asiantuntija E:n mukaan riippuvuuskeskeytysriskiä voidaan kattaa kybervakuutuksesta, jos siitä on erikseen

sovittu vakuutusta tehdessä. Tällaiset vakuutuksenottajan kannalta tärkeät yhteistyökumppanit ja alihankkijat tulee nimetä jo vakuutusta tehdessä, jotta ne voidaan sisällyttää kybervakuutuksen turviin ja jotta siitä voidaan korvata alihankkijoista ja palveluntuottajista aiheutuvat keskeytysvahingot.

Asiantuntija E:n mukaan vakuutushakemusvaiheessa kriittisimpien alihankkijoiden ja palveluntarjoajien nimeäminen mahdollistaa heille vakuutuksenottajan riskien ja sen riippuvuuksista aiheutuvien riskien arvioimisen paremmin. He edellyttävät jo vakuutustarjouksen saamiseksi, että kriittisimmät palveluntarjoajat ja alihankkijat tulee nimetä vakuutushakemuksessa. Vakuutushakemuksessa kolmansista osapuolista aiheutuvien riskien arviointi perustuu hyvin pitkälle luottamukseen, sillä he eivät vakuutuksenantajana auditoi vakuutettujen asiakkaidensa alihankkijoita. Kriittisimpien alihankkijoiden nimeämisen lisäksi vakuutuksenottajaa pyydetään ilmoittamaan, auditoiko se säännöllisesti alihankkijoitaan. Jos vakuutushakemuksessa ilmoitetut alihankkijat ja palveluntuottajat ovat yleisesti tunnettuja ja luotettavina pidettyjä ja vakuutuksenottaja auditoi ne säännöllisesti, voidaan asiantuntija E:n mukaan tietoja pitää luotettavina ja uskoa, että vakuutuksenottaja on huolellinen ulkoistaessaan toimintojaan. Jos vakuutushakemusvaiheessa tulee vastaan heille tuntemattomia palveluntarjoajia ja heille annettu kokonaiskuva vakuutuksenottajan toiminnasta on epäselvä, tekevät he lisäselvityksiä.

Asiantuntija E:n mukaan heillä ei ole toistaiseksi tullut vastaan tapauksia, joissa tiettyjen alihankkijoiden tai yhteistyökumppaneiden vuoksi olisi tehty muutoksia tai rajoituksia vakuutusehtoihin, eikä niillä ole ollut vaikutusta vakuutuksen hinnoitteluun. Kun vakuutushakemusvaiheessa nimetyt alihankkijat ovat tunnettuja ja luotettavina pidettyjä, on hinnoittelu ja vakuutusehdot normaalien käytäntöjen mukaisia. Hän myös huomauttaa, että pääsääntöisesti kybervakuutuksen hankkineet yritykset ovat toistaiseksi olleet keskimääräistä tietoisempia kyberriskeistä, joten he ovat kiinnittäneet huomiota myös alihankkijaverkostoonsa. Tällaisen asiakasryhmän valikoituminen kybervakuuttamisen alkuvaiheessa selittää sen, että heille ei toistaiseksi ole tullut vastaan edellä kuvattua tilannetta, että tietyn tuntemattoman palveluntarjoajan vuoksi vakuutusehtoja tai hinnoittelua olisi jouduttu muuttamaan.

If Vahinkovakuutus tarjoaa asiakkailleen Tietoturvavakuutusta, jonka sisältämät turvat ovat samankaltaisia edellä käsitellyn OP:n kybervakuutuksen kanssa. Tietoturvavakuutus kattaa vakuutuksenottajan IT-ympäristöön kohdistuneita tietoturvaloukkauksia, joista he käyttävät nimityksenä tietomurtoa. Tietoturvavakuutus sisältää lähtökohtaisesti kolme turvaa: yrityksen omat kulut, toiminnan keskeytymisen ja vahingonkorvausvelvollisuuden. Yrityksen omista kuluista korvataan tietomurron selvittämisestä ja tietojen palauttamista aiheutuvia kuluja asiantuntijapalveluiden käyttämisestä sekä luotonvalvontapalveluita. Lisäksi vakuutuksesta voidaan korvata tietomurron aiheuttamasta toiminnan keskeytymisestä johtuvia kuluja. Tietoturvavakuutuksen kolmas turva on vahingonkorvaukset, joka kattaa kolmannelle osapuolelle aiheutuvaa vahingonkorvausvelvollisuutta liikesalaisuuksien paljastumisesta, jos vakuutuksenottaja on niistä vastuussa. Asiantuntija F:n mukaan edellä esitellyt turvat sisältävä vakuutus on perusratkaisu pienemmille yrityksille, ja suuremmille yrityksille vakuutuksen sisältöä voidaan räätälöidä laajemmin asiakkaan tarpeiden mukaan.

Edellä kuvattiin, että Tietoturvavakuutus kattaa vakuutuksenottajan IT-ympäristöön kohdistuneita tietomurtoja. Asiantuntija F kuvailee vakuutuksenottajan IT-ympäristöä esimerkillä: jos asiakkaalla on ulkoistettuna erilaisia toimintoja, esimerkiksi laskutusta, jota se käyttää säännöllisesti, niin sen katsotaan kuuluvan vakuutuksenottajan IT-ympäristöön. Hänen mukaansa tällaiset vakuutuksenottajan säännöllisessä käytössä olevat palvelut ja sen IT-ympäristöön kuuluvat alihankkijat tai palveluntarjoajat kuuluvat vakuutuksen piiriin, jos niiden käyttämisestä aiheutuu tietomurto ja se aiheuttaa vakuutuksenottajalle vahinkoa. Edellä mainittujen määritelmien lisäksi tietomurron tulee olla hakkerointi, palvelunestohyökkäys, tietokonevirus tai haittaohjelma, jotta tietomurrosta aiheutuneet kustannukset voidaan korvata Tietoturvavakuutuksesta.

Asiantuntija F:n mukaan pienempien yritysasiakkaiden kanssa tasapainoillaan vakuuttamisen yksinkertaisuuden ja riskien arvioinnin välillä. Hänen mukaansa pienemmiltä asiakkailta ei vakuutushakemusvaiheessa toistaiseksi pyydetä erikseen selvittämään niiden IT-ympäristöön kuuluvia kolmansia osapuolia, vaan he olettavat, että pienemmät yritykset käyttävät tietyn määrän ulkoisia palveluntarjoajia. Pienillä yrityksillä kolmansista osapuolista aiheutuvat tietomurrot kuuluvat vakuutuksen korvauspiiriin ja niillä ei ole vakuutukseen hintaan korottavaa vaikutusta. Sitä vastoin suuremmilta asiakkailta he käyvät läpi heidän IT-toimintaympäristönsä

ja vakuutusta tehdessä voidaan määritellä, että tietyistä palveluntarjoajista aiheutuvat kyberriskit sisältyvät vakuutukseen ja tietyt palveluntarjoajat voidaan jättää korvauspiirin ulkopuolelle. Hänen mukaansa tällaisista erikseen nimetyistä palveluntarjoajista tehdään vakuutukseen laajennus ja ne voivat vaikuttaa hinnoitteluun.

Edellä esitellyt haastateltavat edustivat yhtä vakuutusyhtiötä, joiden lisäksi tutkielmaa varten haastateltiin yhtä vakuutusmeklariyhtiön edustajaa. Vakuutusmeklariyhtiö Aonin kybervakuutusasiantuntijan näkemys poikkeaa hieman edellä esitetyistä vakuutusyhtiöiden näkemyksistä, sillä asiantuntija D:n mukaan se voi vaihdella vakuutusyhtiökohtaisesti, korvaavatko kybervakuutukset myös kolmansista osapuolista aiheutuvia kybervahinkoja. Hänen mukaansa markkinoilla on tarjolla kybervakuutuksia, jotka eivät korvaa kolmansista osapuolista aiheutuvia vahinkoja käytännössä ollenkaan. Osa vakuutusyhtiöistä tarjoaa kybervakuutuksia, jotka kattavat kolmansista osapuolista aiheutuvat tietovuodot ja niiden selvittelystä ja ilmoittamisesta aiheutuvat kustannukset. Tietovuodoista aiheutuvien kustannusten lisäksi on mahdollista laajentaa kybervakuutuksia kattamaan myös kolmansista osapuolista aiheutuvat keskeytysvahingot. Hänen mukaansa tällaiset laajaa turvaa tarjoavat kybervakuutukset ovat useimmiten asiakaskohtaisesti tehtäviä yksilöllisiä vakuutuksia. Hän myös huomauttaa, että useimmiten suoraan vakuuttajalta ostettuna ja ilman tarkempaa selvitystä kybervakuutuksen laajuudesta, on todennäköistä, että keskeytysturva ei sisälly oletusarvoisesti kybervakuutukseen.

Jos kolmansista osapuolista aiheutuvat keskeytysvahingot halutaan sisällyttää kybervakuutukseen, on sillä asiantuntija D:n kokemuksen mukaan pieni vaikutus kybervakuutuksen hinnoitteluun. Hänen mukaansa se voi korottaa vakuutuksen hintaa 10–20 prosenttia riippuen vakuutettavaan riskiin vaikuttavista tekijöistä. Lisäksi kolmansista osapuolista aiheutuvien keskeytysvahinkojen sisällyttäminen kybervakuutuksen turviin tulee käydä tarkasti läpi, koska jotkut vakuutusyhtiöt voivat kattaa myös kolmansista osapuolista aiheutuvia keskeytysvahinkoja, mutta he voivat samalla lisätä erityisehtoja, että esimerkiksi inhimillisestä virheestä aiheutuvia keskeytysvahinkoja ei korvata kybervakuutuksesta. Asiantuntija D:n mukaan tällaiset asiat tulee käydä tarkasti läpi asiakkaan ja vakuutusyhtiön kanssa, minkä vuoksi vakuutusmeklariyhtiön työ kybervakuuttamisessa on tärkeää, jotta siinä huomioidaan asiakkaan kannalta riittävä laajuus.

Kaikkien kybervakuutusasiantuntijoiden haastatteluista voidaan yhteenvetona todeta, että kybervakuutuksilla voidaan kattaa kolmansista osapuolista aiheutuvia kybervahinkoja sekä vastuu- että keskeytysriskin osalta, mutta käytännöt, oletusarvoiset turvat ja hinnoittelu voivat poiketa toisistaan. Tutkielmaa varten haastateltujen molempien vakuutusyhtiöiden kybervakuutukset korvaavat kolmansista osapuolista aiheutuvia vastuu- ja keskeytysvahinkoja, jos tällaiset palveluntarjoajat tuodaan esille vakuutushakemusvaiheessa, joskin aivan pienimpien asiakkaiden kohdalla tällaista selvitystä ei välttämättä vaadita. Hinnoittelun osalta haastatteluissa ilmeni poikkeavuutta, sillä toisella yhtiöllä kybervakuutuksen laajentaminen kolmansista osapuolista aiheutuviin kyberriskeihin voi vaikuttaa suurempien asiakkaiden kohdalla hinnoitteluun, mutta toisella yhtiöllä sillä ei ole vaikutusta hinnoitteluun pienten eikä suurten asiakkaiden kohdalla. Myös vakuutusmeklariyhtiötä edustavan haastateltavan mukaan keskeytysturvan laajentamisella kattamaan myös kolmansista osapuolista aiheutuvat vahingot voi olla pieni vaikutus hinnoitteluun.

5.3 Henkilötietojen käsittelyn ulkoistaminen ja rekisterinpitäjän vahingonkorvausvelvollisuus

Erityisesti yksityisasiakkaiden kanssa toimivilla yrityksillä on usein runsaasti asiakasdataa ja henkilötietoja, joten ne ovat lainsäädännön mukaisesti rekisterinpitäjiä. Asiakkaiden henkilötietoja käsitellään yrityksissä paljon ja viime vuosina on yleistynyt suuntaus, jossa yritys on rekisterinpitäjä, mutta se on ulkoistanut henkilötietojen käsittelyä ulkopuoliselle palveluntarjoajalle. Luvussa 3.1.2 käsiteltiin EU:n tietosuoja-asetusta, joka eriyttää lainsäädännössä rekisterinpitäjän ja henkilötietojen käsittelijän sekä asettaa molemmille tiettyjä vaatimuksia henkilötietojen käsittelyn ja rekisterinpidon asianmukaisuudesta. Henkilötietojen käsittelyn ulkoistamisessa on keskeistä, että EU:n tietosuoja-asetuksen mukaan rekisterinpitäjä on vahingonkorvausvelvollinen rekisteröidyilleen, vaikka se olisi ulkoistanut henkilötietojen käsittelyn.

Henkilötietojen käsittelyn ulkoistaminen ja EU:n tietosuoja-asetus ovat olleet paljon julkisuudessa esillä, joten kybervakuutuksen kattavuutta tällaisissa tilanteissa on perusteltua tarkastella. Tässä yhteydessä on tarpeen selventää kolmansien osapuolten *aiheuttama* vahinko ja

kolmannelle osapuolelle *aiheutunut* vahinko. Yritys rekisterinpitäjänä kerää asiakkaistaan tietoja, joita joku kolmas osapuoli, esimerkiksi alihankkija, voi käsitellä rekisterinpitäjän lukuun. Tässä yhteydessä kolmannen osapuolen eli alihankkijan henkilötietojen käsittelystä voi aiheutua tietovuoto ja rekisteröityjen henkilötiedot vuotavat ulkopuolisille. Kybervakuutuksen turvissa mainitaan vastuuriskien osalta kolmannelle osapuolelle aiheutuvasta vahingonkorvausvelvollisuudesta. Tällaisessa tapauksessa kolmannella osapuolella tarkoitetaan vahingon kärsijää eli asiakasta, jonka henkilötietoja rekisterinpitäjä on kerännyt. Selvyyden vuoksi käytämme tässä luvussa kolmannelle osapuolelle aiheutuneesta vahingonkorvausvelvollisuudesta nimitystä rekisteröidylle aiheutunut vahinko.

Kaikki haastatellut kybervakuutusasiantuntijat olivat yksimielisiä, että rekisteröidylle aiheutunut taloudellinen vahinko voidaan korvata vastuuvahinkona, vaikka rekisterinpitäjä eli vakuutuksenottaja on ulkoistanut henkilötietojen käsittelyn ulkopuoliselle yritykselle. Asiantuntija E toteaa, että vahingon tapahduttua tarkastellaan, mitä vahinkoa rekisteröidylle on aiheutunut ja korvaus maksetaan vahingon kärsineelle riippumatta siitä, onko tietovuoto tapahtunut rekisterinpitäjällä tai ulkopuolisella henkilötietojen käsittelijällä. Tämän lisäksi kybervakuutuksesta korvataan myös tällaisissa tapauksissa kuluja EU:n tietosuoja-asetuksen edellyttämästä ilmoittamisvelvollisuudesta rekisteröidyille tietoturvaloukkauksen tapahduttua.

Myös asiantuntija F on samaa mieltä edellä esitetyn näkemyksen kanssa. Lähtökohta on, että rekisteröity on yksityishenkilö, jolle aiheutuva vahinko korvataan vakuutuksesta riippumatta siitä, kuka henkilötietoja käsittelee ja kenestä tietovuoto aiheutuu. Vaikka molemmat haastatellut yhtiöt korvaavat rekisteröidylle aiheutuvat vahingot, suoritetaan korvaukset hieman eri tavoilla. Asiantuntija E:n edustaman OP:n kybervakuutuksista korvataan tällaiset vastuuvahingot rekisteröidyille, mutta asiantuntija F:n edustamalla Ifillä rekisteröidyille aiheutuvat vahingot korvataan toiminnan vastuuvakuutuksesta. Vastaavasti ilmoittamisvelvollisuudesta aiheutuvat kustannukset korvataan Ifin Tietoturvavakuutuksesta. He edellyttävät, että asiakkaalla on sekä toiminnan vastuuvakuutus että Tietoturvavakuutus, jotta edellä esitetyt korvaukset vastuuvahinkojen ja ilmoittamiskustannusten osalta voidaan suorittaa. Asiantuntija F huomauttaa, että korvaus rekisteröidyille maksetaan joka tapauksessa, mutta rekisterinpitäjän ja henkilötietojen käsittelijän tulee tehdä kirjallinen sopimus henkilötietojen käsittelystä, kuten

EU:n tietosuoja-asetus edellyttää. Siinä voidaan sopia korvausten suorittamisen vastuusta rekisterinpitäjän ja henkilötietojen käsittelijän välillä.

Myös vakuutusmeklariyhtiötä edustavan asiantuntija D:n kokemuksen mukaan kybervakuutuksista korvataan rekisteröidyille aiheutuvat taloudelliset vahingot, vaikka rekisterinpitäjä eli vakuutuksenottaja on ulkoistanut henkilötietojen käsittelyn. Hän myös huomauttaa, että eri vakuutusyhtiöiden vakuutusehdoissa ei eksplisiittisesti puhuta EU:n tietosuoja-asetuksen määrittämästä vahingonkorvausvelvollisuudesta, vaan niissä mainitaan yleisesti, että vakuutuksesta korvataan rekisteröidyille aiheutuvia vahinkoja.

Kysymykseen rekisterinpitäjän vahingonkorvausvelvollisuudesta ja kybervakuutuksen kattavuudesta kaikki haastateltavat olivat yksimielisiä siitä, että rekisteröidyille korvataan aiheutuneet vahingot riippumatta siitä, onko rekisterinpitäjä ulkoistanut henkilötietojen käsittelyn. Haastateltavien välillä ainoa eroavaisuus syntyi, mistä vakuutuslajista korvaus suoritetaan. Muiden haastateltavien mukaan vahingonkorvausvelvollisuuden edellyttämät kulut rekisteröidyille korvataan kybervakuutuksesta, mutta yhden haastateltavan mukaan vahingonkorvaukset suoritetaan toiminnan vastuuvakuutuksesta ja muut tietovuotoon liittyvät kulut kybervakuutuksesta.

5.4 Sanktioiden korvaaminen kybervakuutuksesta

Luvussa 3.1.2 käsiteltiin EU:n tietosuoja-asetusta, sen velvoitteita ja mahdollisia tietosuojaviranomaisen langettamia sanktioita asetuksen velvoitteiden laiminlyönneistä. Kaikkien haastateltujen kybervakuutusasiantuntijoiden mukaan tietosuojaviranomaisen langettamien sanktioiden korvaamiseen kybervakuutuksista ei tällä hetkellä ole täysin yksiselitteistä linjaa. Toistaiseksi vakuutusyhtiöt ovat tehneet erilaisia tulkintoja, voidaanko sanktioita lain mukaan korvata vakuutuksesta.

Asiantuntija E:n mukaan heidän suuryrityksille suunnatusta laajemmasta kybervakuutuksesta voidaan korvata tietosuojaviranomaisen langettamia sanktioita, mutta pk-yrityksille tarkoitetusta suppeammasta kybervakuutuksesta sanktioita ei korvata. Hänen mukaansa sanktioiden

korvattavuus kybervakuutuksesta on vakuutusehtoihin kirjoitettu siten, että sanktioita voidaan korvata vakuutuksesta, mikäli se on kyseisen maan lainsäädännön mukaan mahdollista. Koska käytännön kokemusta sanktioiden langettamisesta ja niiden suuruudesta ei vielä ole, on se asiantuntija E:n mukaan jatkuvasti esillä heidän asiakkaidensa kanssa. Heidän asiakkaansa ovat kiinnostuneita vakuutusyhtiön odotuksista, millaisia nämä sanktiot mahdollisesti tulevat olemaan. Toistaiseksi he ovat joutuneet ottamaan kantaa laveasti, mistä hän toteaa:

> *”Jotenkin minun mielestä tuntuisi tällaiseen suomalaiseen oikeuskäytäntöön huonosti istuvalta, että niistä alettaisiin roiskia kovia sanktioita. Ainakin sen menettelyn täytyy olla aika raskauttavaa. Sen pitää olla joku sellainen toimija, jolta pitäisi edellyttää erittäin huolellista toimintaa ja sitten totuus ilmeneekin olevan ihan toinen. Siinä varmaan tulee sitten taas valvovalle viranomaiselle paineita, että siitä voikin jonkinlaisen rangaistuksen määrätä. Se, että pienemmille yrityksille sanktioita alettaisiin kovin tiheään määrätä, tuntuisi hieman yllättävältä.”*

Myös asiantuntija D on samaa mieltä eli tietosuojaviranomaisen langettamia sanktioita voidaan Suomessa toistaiseksi korvata kybervakuutuksista. Myös hänen mielipiteensä on, että toistaiseksi linjaus sanktioiden korvaamisesta kybervakuutuksesta on epäselvä. Esimerkiksi Ruotsissa ja Norjassa tällaisten sanktioiden korvaaminen vakuutuksesta ei ole mahdollista, ja hänen mukaansa samanlaista linjausta odotetaan myös Suomeen. Yleensä vakuutuksista ei korvata sakkoja ja sanktioita, joten kybervakuutus on vielä toistaiseksi poikkeuksellinen, koska tällaisten sanktioiden korvaaminen vakuutuksesta on mahdollista.

Asiantuntija F suhtautuu edellä esitettyjä näkemyksiä kriittisemmin sanktioiden korvaamiseen vakuutuksesta. Tietoturvavakuutuksesta viranomaisten langettamia sanktioita ei tällä hetkellä korvata. Myös hän painottaa edellä esitettyjen näkemysten kanssa, että Suomessa on toistaiseksi epäselvää, voidaanko viranomaisten määräämiä sanktioita korvata kybervakuutuksista. He ovat yhdessä alan tunnettujen asiantuntijoiden kanssa tulkinneet kriittisemmin sanktioiden korvaamisen laillisuutta, koska yleisesti sakkojen – esimerkiksi ylinopeussakkojen ja pysäköintivirhemaksujen – vakuuttaminen ei ole ollut hyvän vakuutustavan mukaista. Hänen mukaansa epäselvyyttä lisää se, että missään ei ole selkeästi ilmaistu, että sanktioiden korvaaminen vakuutuksesta on sallittua ja hyväksyttävää. Kuten aiemmin on mainittu, myös asiantuntija F nostaa esille, että Ruotsissa ja Norjassa tilanne on selkeä, että sanktioita ei voida

korvata vakuutuksesta, mutta Suomessa tilanne on epäselvä. Jos lain tulkinta olisi Suomessa selvä, voisivat he harkita sanktioiden korvauksen sisällyttämistä kybervakuutukseen.

Asiantuntija F huomauttaa lisäksi, että vakuutusyhtiöt ottavat jonkinlaisen riskin, jos he vakuuttavat Suomessa viranomaisten määräämiä sanktioita. Tällaisessa tapauksessa vakuutuksenottajat eivät tulisi todennäköisesti kärsimään, vaikka myöhemmin tulkittaisiin, että EU:n tietosuoja-asetuksen puitteissa määrättyjä sanktioita ei ole mahdollista korvata vakuutuksesta. Vakuutusyhtiön kannalta riskinä on, että vakuutussopimukset jouduttaisiin irtisanomaan, jos sanktioita on aiemmin vakuutettu ja myöhemmin tulkitaan, että niiden vakuuttaminen ei ole mahdollista. Hänen mukaansa erilaiset tulkinnat sanktioiden korvaamisesta johtuvat siitä, että kybervakuuttaminen on alkanut Yhdysvaltojen ja Lontoon markkinoilta, missä joidenkin vakuutusten klausuulitekstien mukaan sanktioiden korvaaminen on mahdollista. Myös joidenkin maiden lainsäädäntö on sallivampi sanktioiden korvaamisesta vakuutuksesta.

Kuten tässä luvussa tuotiin aiemmin esille asiantuntija E:n näkemys sanktioiden määräämisestä, on myös asiantuntija F samaa mieltä, että niiden laajamittaista käyttöä pidetään epätodennäköisenä:

> *”Tilanne on se, että kyllä aika pitkälle täytyy mennä, jotta oikeasti tämän tyyppisiä sakkoja tai seuraamusmaksuja määrättäisiin. Kyllähän se ensimmäisenä on varmasti kehotus, että lopettakaa toiminta ja hoitakaa asia kuntoon, annetaan varoituksia ja ehkä sen jälkeen voi olla viimeisenä keinona nämä sakot. Se vain kuvastaa, kuinka tärkeänä tämän asian kuntoon laittamista on pidetty, että sinne on laitettu tällainen aika mittava sanktio viime kädessä.”*

Kybervakuutusasiantuntijoiden haastatteluista voidaan päätellä, että sanktioiden korvaamiseen kybervakuutuksesta ei ole selkeää linjaa, ja eri toimijat markkinoilla suhtautuvat varovasti niiden korvaamiseen tai ottamaan kantaa niiden korvattavuuteen. Tällä hetkellä osa yhtiöistä on tulkinnut lainsäädäntöä siten, että sanktioita voidaan korvata kybervakuutuksesta, mutta osa yhtiöistä on ottanut tiukemman linjauksen niiden korvaamisesta, kuten edellä esitetyistä asiantuntijahaastatteluista voidaan päätellä. Koska sanktioiden korvaaminen vakuutuksesta on Ruotsissa ja Norjassa kiellettyä ja yleisesti sakkojen korvaamista vakuutuksesta on pidetty hyvän vakuutustavan vastaisena, voidaan olettaa, että lähivuosina Suomessa tullaan

tekemään selkeä linjaus, voidaanko viranomaisten määräämiä sanktioita korvata vakuutuksesta.

6 YHTEENVETO

6.1 Tutkimusongelmiin vastaaminen

Tässä tutkielmassa selvitettiin vastauksia kolmeen tutkimusongelmaan. Ensimmäinen tutkimusongelma käsitteli kolmansista osapuolista aiheutuvien kyberriskien analysointia eli miten niitä voidaan tunnistaa ja arvioida. Tutkielman tekijän yleisnäkemyksen ja esitetyn teorian pohjalta voitiin olettaa, että ensimmäiseen tutkimusongelmaan ei tulla saamaan yksiselitteistä vastausta, koska riskienhallinnan alalla ei ole yleisesti vakiintunutta menetelmää kolmansista osapuolista aiheutuvien kyberriskien arviointiin. Empiiriset haastattelut sekä kyberturvallisuus- että kybervakuutusasiantuntijoille vahvistivat tutkielman ennakko-oletusta. Ensimmäistä tutkimusongelmaa käsittelevä empiirinen aineisto ja sen analysointi tarjosivat mielenkiintoisia ja toisistaan osin poikkeavia näkemyksiä.

Luvuissa 4.2 ja 4.3 esitettiin vastauksia empiirisen aineiston pohjalta ensimmäiseen tutkimusongelmaan. Haastattelujen perusteella kolmansista osapuolista aiheutuvia kyberriskejä voidaan parhaiten tunnistaa yrityksen kannalta kriittisten prosessien ja omaisuuserien tunnistamisella, jonka jälkeen kartoitetaan, mitä tietoa kolmansilla osapuolilla on, ketkä niitä pääsevät käsittelemään ja voidaanko heidän toimintaansa auditoida. Erityisesti kyberturvallisuusasiantuntijat nostivat esille, että keskeinen ongelma kolmansista osapuolista aiheutuvien kyberriskien tunnistamisessa on se, että yrityksiltä puuttuu usein näkymä heidän yhteistyökumppaneidensa ja alihankkijoidensa toimintaan ja tietojärjestelmiin. Yritykset eivät silloin tarkasti tiedä, mitä tietoja, kuka ja miten niitä käsitellään. Näkymän puuttuminen johtaa tilanteeseen, jossa kolmansista osapuolista aiheutuvia kyberriskejä on vaikea tunnistaa.

Tämä pätee erityisesti pieniin yrityksiin, joilla ei ole resursseja tai mahdollisuutta päästä auditoimaan suurempia palveluntarjoajia tai vaatimaan heitä toimimaan tilaajan haluamalla tavalla. Suuremmilla yrityksillä tilanne on parempi ja ne pääsevät yleensä auditoimaan palveluntarjoajiaan sekä määrittämään tarkempia reunaehtoja tietojenkäsittelylle.

Ensimmäisellä tutkimusongelmalla selvitettiin lisäksi, miten kolmansista osapuolista aiheutuvien kyberriskien suuruutta voidaan arvioida. Esitetyn teorian pohjalta voitiin olettaa, että kvalitatiiviset arviointimenetelmät ja erityisesti riskimatriisit olisivat yleisimpiä arviointimenetelmiä. Haastateltujen asiantuntijoiden mukaan yrityksissä on käytössä sekä kvantitatiivisia menetelmiä että kvalitatiivisia asiantuntija-arvioon perustuvia menetelmiä. Haastatteluissa nousi kuitenkin useimmiten esille kvalitatiiviset menetelmät niiden yksinkertaisuudesta johtuen, joten voidaan olettaa, että kvalitatiiviset menetelmät ovat toistaiseksi yleisempiä. Erityisesti riskimatriisit mainittiin useissa haastatteluissa. Kaikki haastateltavat olivat yksimielisiä, että kolmansista osapuolista aiheutuvien riskien suuruuden arviointi on haastavaa ja niiden arvioimiseen ei ole olemassa erityistä menetelmää. Kolmansista osapuolista aiheutuvia kyberriskejä arvioidaan samankaltaisilla menetelmillä kuin muitakin kyberriskejä ja niihin pätevät samat lainalaisuudet.

Kyberriskien tunnistamisessa ja arvioinnissa on olennaista tarkastella kolmansista osapuolista aiheutuvia kyberuhkia, yrityksen itsensä ja kolmansien osapuolien haavoittuvuuksia sekä erilaisia toimijoita niiden taustalla. Erilaiset kyberuhat saivat haastatteluissa odotettua vähemmän keskustelua aikaan, mutta lähes kaikissa haastatteluissa nousivat esille haittaohjelmat ja verkkohyökkäysten seurauksena tapahtuvat tietovuodot kolmansien osapuolten kautta. Haittaohjelmien ja verkkohyökkäysten nouseminen esille haastatteluissa tuki esitetyn teorian mukaista näkemystä yleisimmistä kyberuhista.

Kyberuhkien sijaan erilaiset haavoittuvuudet saivat aikaan runsaampaa keskustelua haastatteluissa. Haavoittuvuuksien kannalta ongelmallisimmiksi nähtiin sekä yrityksen omien että sen yhteistyökumppaneidensa tietojärjestelmien ohjelmistohaavoittuvuudet. Ohjelmointivirheet erilaisissa ohjelmistoissa ovat yleisiä, minkä seurauksena esimerkiksi hakkerit etsivät jatkuvasti tällaisia virheitä ohjelmistoista. Ohjelmointivirheet muodostavat haavoittuvuuden, jota erilaiset kyberuhat, esimerkiksi haittaohjelmat, voivat hyödyntää mahdollistaen murtautumi-

sen yrityksen tietojärjestelmiin. Keskeistä tämän tutkielman kannalta on, että haavoittuvuudet voivat olla yrityksen käyttämien kolmansien osapuolten tietojärjestelmissä. Yritysten toimitusketjut voivat muodostua lukuisista eri alihankkijoista, jokaisella voi olla erilaisia ohjelmistoja ja siten myös haavoittuvuuksia voi olla lukuisia. Tietomurtoja toteuttavat tahot etsivät yritysten toimitusketjuista heikoimman kohdan, joka useimmiten on jokin pienempi alihankkija, jonka kyberturvallisuus on heikko. Alihankkijan haavoittuvuutta hyödyntämällä verkkohyökkäyksen tekijät pääsevät käsiksi toimitusketjussa olevan suuremman yrityksen järjestelmiin, joka on ollut heidän alkuperäisenä kohteenaan. Ongelmalliseksi haastatteluissa nähtiin näkymän puute kolmansien osapuolten tietojärjestelmiin, minkä seurauksena haavoittuvuuksien ja mahdollisten tietomurtojen havaitseminen on haastavaa ja niitä ei välttämättä havaita tarpeeksi ajoissa.

Haastatteluissa myös kartoitettiin, millaiset toimijat ovat erityisesti kolmansista osapuolista aiheutuvien kyberriskien taustalla. Tulosten perusteella voidaan todeta, että kyberrikolliset ovat useimmiten kyberriskien aiheuttajia ja heidän motiivinaan on nopea rahan ansaitseminen. Koska tutkielmassa kartoitettiin erityisesti kolmansista osapuolista aiheutuvia kyberriskejä, pyrittiin haastatteluissa selvittämään, onko juuri kolmansista osapuolista aiheutuvien kyberriskien taustalla tietyt tahot. Tulosten perusteella voidaan todeta, että kyberriskien taustalla olevat tahot ovat samoja riippumatta siitä, kohdistuuko kyberhyökkäys suoraan yritykseen vai sen käyttämään kolmanteen osapuoleen, esimerkiksi alihankkijaan.

Tutkielman toinen tutkimusongelma tarkasteli viime vuosina yhä enemmän jalansijaa saaneita pilvipalveluita ja niiden vaikutusta yrityksen kyberturvallisuuteen, mitä käsiteltiin luvussa 4.4. Toiseen tutkimusongelmaan ei tämän tutkielman aineiston perusteella voida vastata yksiselitteisesti, parantaako vai heikentääkö pilvipalveluiden käyttäminen kategorisesti yrityksen kyberturvallisuuden tasoa. Pilvipalveluiden vaikutus kyberturvallisuuteen riippuu ulkoistavan yrityksen alkuperäisestä kyberturvallisuuden tasosta, palveluntarjoajan kyberturvallisuudesta ja pilvipalveluun siirrettävän tiedon luottamuksellisuudesta sekä kriittisyydestä yrityksen toiminnan kannalta.

Lähtökohtaisesti ensimmäinen määrittävä tekijä on ulkoistavan yrityksen kyberturvallisuuden taso verrattuna palveluntarjoajaan. Jos yrityksen omat resurssit ovat vähäiset ja sillä ei ole

mahdollisuuksia ja osaamista turvallisiin IT-järjestelmiin, voi olla perusteltua käyttää ammattimaisesti ja suuressa mittakaavassa toimivia pilvipalveluita. Tällaisessa tilanteessa kokonaiskyberturvallisuus useimmiten paranee, koska yrityksen tietojenkäsittelyä ja -säilytystä on siirretty turvallisempaan ympäristöön. Yleistettynä voidaan sanoa, että erityisesti pienten yritysten kohdalla pilvipalveluiden käyttäminen parantaa kyberturvallisuuden tasoa, koska resurssit ja IT-osaaminen pienillä yrityksillä on useimmiten heikolla tasolla. Vastaavasti voidaan yleisesti todeta, että suuremmilla yrityksillä kyberturvallisuus on usein otettu paremmin huomioon ja niillä on enemmän resursseja rakentaa vain yrityksen omaan käyttöön tarkoitettuja järjestelmiä. Tässä yhteydessä on tärkeä huomioida, kuten tutkielman aineistossa nousi esille, että yrityksen koon ja kyberturvallisuuden tason välillä ei välttämättä ole säännönmukaista yhteyttä. Erään haastatellun asiantuntijan mukaan on tapauksia suurista yrityksistä, joilta odotetaan hyvää kyberturvallisuuden tasoa, mutta todellisuudessa niiden kyberturvallisuus on heikolla tasolla, minkä vuoksi yrityksen koosta ei voi suoraan päätellä sen kyberturvallisuuden tasoa.

Keskeistä on myös ulkoistettavan tiedon luottamuksellisuus ja sen kriittisyys yrityksen toiminnan kannalta. Tutkielman aineiston perusteella voidaan todeta, että pilvipalveluiden käyttäminen lisää joustavuutta ja hyötyjä enemmän kuin riskejä, mikäli pilvipalveluun ulkoistettava tieto ei ole erittäin luottamuksellista ja yrityksen toiminnan jatkuvuuden kannalta kriittistä. Toisin sanoen, jos pilvipalveluiden kautta mahdollisesti menetettävät tiedot tai niiden käyttämisen estyminen eivät aiheuta merkittäviä vahinkoja yritykselle, on pilvipalveluiden käyttäminen hyötyjen näkökulmasta perusteltua. Aineistossa nousi myös esille kriittisempi suhtautuminen pilvipalveluihin, jos pilvipalveluun siirrettävät tiedot ovat erittäin luottamuksellisia tai kriittisiä yrityksen toiminnan kannalta. Tällaisessa tilanteessa pilvipalveluista saatavat hyödyt jäävät pienemmiksi kuin niistä aiheutuvat riskit. Erityisesti suuret yritykset ja kriittisen infrastruktuurin toimijat, joilla on riittävät resurssit sisäisiin ja suljettuihin IT-järjestelmiin, ovat viime aikoina ottaneet aiemmin ulkoistettuja palveluita takaisin yrityksen itsensä hoidettaviksi.

Tutkielman kolmas tutkimusongelma selvitti, miten kybervakuutukset kattavat kolmansista osapuolista aiheutuvia kybervahinkoja. Kybervakuutuksen kattavuutta käsiteltiin luvuissa 5.2,

5.3 ja 5.4. Tämän tutkimusongelman aineistona on käytetty kahden suomalaisen kybervakuutusta tarjoavan vakuutusyhtiön edustajan haastattelua ja sitä on täydennetty yhden Suomessa toimivan vakuutusmeklariyhtiön edustajan haastattelulla.

Tähän tutkielmaan haastateltujen molempien vakuutusyhtiöiden nykyiset kybervakuutukset kattavat myös kolmansista osapuolista aiheutuvia vahinkoja, mutta vakuutettavien riskien oletusarvoinen laajuus vaihtelee vakuutusyhtiöittäin. Vastuuvahingot ovat tämän tutkielman aineiston perusteella yksinkertaisia kybervakuuttamisen näkökulmasta. Tällaiset ulkopuoliselle aiheutuneet vahingot korvataan kybervakuutuksesta, vaikka yritys olisi ulkoistanut toimintojaan kolmannelle osapuolelle ja vahinko aiheutuu heidän virheestään. Riippuvuuskeskeytysriskien vakuuttaminen eli kolmansista osapuolista aiheutuvien kybervahinkojen seurauksena syntyvien liiketoiminnan keskeytyskulujen vakuuttaminen ei ole yhtä suoraviivaista kuin vastuuvahinkojen vakuuttaminen. Riippuvuuskeskeytysriskien vakuuttaminen vaihtelee yhtiö- ja tuotekohtaisesti. Molempien haastateltujen yhtiöiden kybervakuutuksissa pienempien yritysten tapauksessa riippuvuuskeskeytysvahingot kuuluvat kybervakuutukseen, eikä yritysten käyttämiä yhteistyökumppaneita tarvitse erikseen ilmoittaa vakuutusyhtiöille. Vastaavasti suurempien yritysten tapauksessa molemmat yhtiöt edellyttävät vakuutuksenottajaa ilmoittamaan heidän käyttämänsä yhteistyökumppanit, joista aiheutuvat keskeytysvahingot voidaan sisällyttää kybervakuutukseen tapauskohtaisesti.

Yritykset käsittelevät ja säilyttävät erilaisia salassa pidettäviä tietoja, joista osa on yleensä henkilötietoja. Henkilötietojen käsittelyyn tulee kiinnittää erityistä huomiota, koska niiden käsittelyä säännellään esimerkiksi EU:n tietosuoja-asetuksella, jonka laiminlyönnistä voi joutua korvausvastuuseen. Vahingon kärsivä osapuoli on yleensä yksityishenkilö, joten lailla on turvattu, että yksityishenkilö on oikeutettu korvaukseen tietosuojaloukkauksen tapahduttua. Tutkielman kolmannella tutkimuskysymyksellä selvitettiin myös, korvaako kybervakuutus EU:n tietosuoja-asetuksen edellyttämää korvausvelvollisuutta vahingon kärsijälle, jos henkilötietojen käsittelyä on ulkoistettu ja vahinko on aiheutunut kolmannen osapuolen laiminlyönnistä tai virheestä. Tutkielman aineisto vahvistaa, että rekisterinpitäjän kybervakuutuksesta korvataan rekisteröidyille aiheutuneet vahingot tietosuojaloukkauksesta, vaikka vahingon

olisi aiheuttanut ulkopuolinen henkilötietojen käsittelijä. Yhden haastatellun yhtiön käytännöissä on poikkeus, ja kyseinen vahinko korvattaisiin toiminnan vastuuvakuutuksesta, mutta rekisteröidyille aiheutuneet vahingot korvattaisiin joka tapauksessa samalla periaatteella.

Lisäksi kolmannella tutkimusongelmalla selvitettiin, voidaanko kybervakuutuksesta korvata mahdollisia sanktioita, joita tietosuojaviranomaiset voivat määrätä henkilötietojen käsittelyn laiminlyönneistä. Sanktioiden korvaaminen kybervakuutuksesta on tällä hetkellä vielä epäselvää, koska lainsäädännössä ei selkeästi ilmaista, voidaanko tietosuojaviranomaisen langettamia sanktioita korvata kybervakuutuksesta. Toistaiseksi vakuutusyhtiöt ovat tehneet erilaisia tulkintoja ja osa vakuutusyhtiöitä korvaa sanktioita kybervakuutuksesta, mutta osa yhtiöistä on kieltäytynyt sisällyttämästä niitä kybervakuutukseen. Sanktioiden korvaaminen kybervakuutuksesta vaihtelee eri maiden lainsäädännön mukaan, ja esimerkiksi Ruotsissa ja Norjassa sanktioiden korvaaminen vakuutuksesta on kiellettyä. Sanktioiden korvattavuutta kybervakuutuksesta tarkasteltiin tässä tutkielmassa suomalaisten vakuutusyhtiöiden näkökulmasta, joten tulokset edustavat vain suomalaista käytäntöä. Toistaiseksi Suomessa odotetaan viranomaisten selkeää päätöstä, onko sanktioiden korvaaminen lainsäädännön mukaan sallittua. Vastauksena tutkimusongelmaan voidaan todeta, että toistaiseksi sanktioida voidaan korvata kybervakuutuksesta, mutta osa vakuutusyhtiöistä ei silti sisällytä niitä kybervakuutuksiinsa.

6.2 Johtopäätökset

Tutkielmassa tarkasteltavan ilmiön ympärillä vaikuttavat vahvasti kaksi trendiä. Yritykset siirtyvät yhä tietointensiivisempään liiketoimintaan, mikä tarkoittaa digitaalisen liiketoiminnan kasvua. Sen lisäksi yritykset erikoistuvat yhä enemmän ydinliiketoimintaansa ja ulkoistavat merkittävän osan muusta liiketoiminnastaan, mikä useimmiten tarkoittaa luottamuksellisten tietojen ja yhteisten IT-järjestelmien jakamista. Kasvanut riippuvuus ja verkottuneisuus lisäävät uudenlaisia kyberriskejä, joihin ei ole aiemmin osattu varautua. Kolmansista osapuolista aiheutuvia kyberriskejä pidetäänkin siten yhtenä vakavimmista ja vaikeimmin hallittavista kyberriskeistä tulevaisuudessa.

Tämän tutkielman sekä teoreettisen että empiirisen aineiston perusteella voidaan päätellä, että kolmansista osapuolista aiheutuvien kyberriskien arviointiin ei ole olemassa yhtä vakiintunutta ja luotettavaa menetelmää, jolla niiden todennäköisyyksiä ja taloudellisia vaikutuksia voitaisiin arvioida riittävän tarkasti. Todennäköisin syy arviointimenetelmien puuttumiseen on, että kolmannet osapuolet kyberriskien lähteenä on tunnistettu vasta aivan viime aikoina vakavaksi riskiksi. Sen lisäksi näkymän puuttuminen kolmansien osapuolten tietojärjestelmiin tekee kyberriskien arvioinnista hyvin vaikeaa. Kolmansilla osapuolilla on käytössä suuri määrä erilaisia ohjelmistoja ja järjestelmiä, joten paljon erilaisia alihankkijoita käyttävän yrityksen voi olla vaikea havaita niissä mahdollisesti olevia haavoittuvuuksia.

Tutkimushaastatteluiden perusteella kolmansista osapuolista aiheutuvia kyberriskejä arvioidaan samankaltaisilla menetelmillä kuin yritykseen suoraan kohdistuvia kyberriskejä. Pääasiassa tällaiset menetelmät ovat erilaisia riskimatriiseja, joissa vahinkojen todennäköisyyksille ja vaikutuksille annetaan arvioon perustuen vakavuusluokituksia. Tällaisten menetelmien käytössä piilee kuitenkin vaara. Jos kolmansista osapuolista aiheutuvia kyberriskejä arvioidaan samankaltaisilla menetelmillä kuin yritykseen suoraan kohdistuvia kyberriskejä, voi riskienhallintatyössä jäädä huomioimatta ennalta arvaamattomia ja vakavia riskejä. Kyberturvallisuudessa edistyneempi yritys tuntee omat järjestelmänsä ja mahdolliset haavoittuvuutensa sekä osaa arvioida niistä mahdollisesti syntyviä vahinkoja, mutta ne eivät voi vastaavalla varmuudella arvioida alihankkijoidensa haavoittuvuuksia. Tässä piilee tutkittavan aihepiirin kenties suurin ongelma, koska muiden yritysten IT-järjestelmien turvallisuuden ja luotettavuuden arviointi ei parhaimmillaankaan voi olla yhtä aukotonta kuin yrityksen omien järjestelmien ja toimintatapojen auditointi. Tietovuotojen kannalta yksi keskeisistä asioista on reagointiaika tietovuodon tai tietomurron tapahtuessa, ja tätä kyvykkyyttä voi olla hyvin haastava arvioida kolmansilta osapuolilta. Kun tietojenkäsittelyä on ulkoistettu, on samalla myös kontrolli tiedon hallinnasta osittain ulkoistettu. Yritys ei välttämättä saa heti tietoonsa, jos tietovuoto on tapahtunut eikä alihankkija ole sitä itse kyennyt havaitsemaan.

Vaikka tässä tutkielmassa on useasti tuotu esille, että kolmansista osapuolista aiheutuvien kyberriskien arviointi on haastavaa, tullaan siihen tulevaisuudessa todennäköisesti kiinnittämään yhä enemmän huomiota, minkä seurauksena riskien arviointimenetelmät kehittyvät

edistyneemmiksi. Koko EU:n alueella voimaan tuleva tietosuoja-asetus tulee osaltaan muuttamaan tilannetta, koska se edellyttää parempaa riskiarviota henkilötietojen käsittelystä sekä rekisterinpitäjän ja henkilötietojen käsittelijän välistä kirjallista sopimusta. Kirjallisten sopimusten tekeminen ja vastuiden määrittäminen kolmansien osapuolten kanssa kiinnittää yritysten huomiota arvioimaan myös ulkoistamisesta aiheutuvia kyberriskejä. Vaikka kaikki kolmansille osapuolille ulkoistettava tietojenkäsittely ei sisällä henkilötietoja ja siten ole EU:n tietosuoja-asetuksen alaista toimintaa, voidaan tietosuoja-asetuksen katsoa lisäävän yritysten riskitietoisuutta myös muun tietojenkäsittelyn ulkoistamisessa.

Pilvipalveluiden hyödyntäminen liiketoiminnassa on kasvanut voimakkaasti viime vuosikymmenen aikana. Tiedon vaivaton saatavuus, joustavuus ja laiteinvestointien väheneminen ovat pilvipalveluiden kiistattomia etuja, mutta pilvipalveluiden laajamittainen hyödyntäminen on kenties tapahtunut riskiarviointien ja turvallisuuden kustannuksella. Empiirisen aineiston perusteella oli jopa yllättävää, kuinka varauksellisesti osa haastatelluista asiantuntijoista suhtautui pilvipalveluihin kyberturvallisuuden näkökulmasta. Pilvipalvelut tuovat monissa liiketoiminnoissa selkeitä etuja, mutta niihin ulkoistettavan tiedon luottamuksellisuudessa tulisi käyttää harkintaa. Erityisenä riskinä voidaan nähdä, että pilvipalveluita käyttää suuri määrä käyttäjiä erilaisilla päätelaitteilla. Suuri laitteiden ja käyttöjärjestelmien kirjo vaikuttaa siten, että pilvipalveluihin kirjautumisten määrä kasvaa ja tunnistautuminen tapahtuu useilta eri laitteilta. Laitteiden ja käyttöjärjestelmien suuri määrä kasvattaa haavoittuvuuksien mahdollisuutta, mikä voi lopulta johtaa haavoittuvuuden hyväksikäyttämiseen ja tietomurtoon. Pilvipalveluiden käyttö on liiketoiminnallisesta näkökulmasta hyvin perusteltua, mutta turvallisuuden ja ulkoistettavan tiedon luottamuksellisuuden arviointi tulisi seurata tarkasti turvallisuusvaatimuksia, ja niitä tulisi arvioida suhteessa ulkoistamisesta saataviin hyötyihin.

Tähän tutkielmaan tarkasteltavaksi riskienhallintamenetelmäksi valittiin kybervakuutus, joka on vakuutusmarkkinoilla uusi ja vakiintumaton vakuutustuote. Kybervakuutusten sisältö, ehdot ja rajoitukset vaihtelevat vakuutusyhtiöittäin, joten kolmansien osapuolten aiheuttamien kybervahinkojen korvattavuus tarjosi mielenkiintoisen tutkimuskohteen. Tutkimushaastatteluiden perusteella suomalaisten vakuutusyhtiöiden kybervakuutuksilla voi suojautua hyvin

kolmansien osapuolten aiheuttamilta vastuuvahingoilta. Lisäksi kybervakuutuksilla voi varautua riippuvuuskeskeytysvahinkoihin, jos tällaiset riippuvuudet ja kriittiset palveluntarjoajat on otettu huomioon vakuutusta tehdessä.

Tutkielman tuloksissa oli jopa yllättävää, kuinka avoimesti haastatellut vakuutusyhtiöiden edustajat suhtautuivat kolmansista osapuolista aiheutuviin kybervahinkoihin ja niiden korvaamiseen kybervakuutuksesta. Koska kolmansista osapuolista aiheutuvat kyberriskit ovat vaikeasti arvioitavissa, oli tutkijan ennakko-olettamuksena, että kolmansien osapuolten aiheuttamissa kybervahingoissa olisi enemmän rajoitusehtoja ja maksimikorvausten rajoituksia. Lisäksi riippuvuuskeskeytysriskien sisällyttäminen pienten yritysten kybervakuutukseen ilman ennakkoselvitystä ja hinnankorotusta vaikutti yllättävältä, koska vakuutusyhtiöt ottavat silloin kantaakseen tietyn määrän riskiä, jonka suuruutta ja todennäköisyyttä ne eivät välttämättä voi arvioida. Tässä yhteydessä vakuutusyhtiöiden perustelut ovat toisaalta luontevia, koska pienten asiakkaiden kohdalla vakuutuksen myynti on tehtävä vaivattomaksi, ja kannettava riski ei välttämättä muodostu suureksi.

Tutkielman empiiristen haastatteluiden perusteella suomalaisilla vakuutusyhtiöillä ei ole menetelmiä arvioida asiakkaidensa käyttämistä kolmansista osapuolista aiheutuvia kyberriskejä. Kolmansista osapuolista aiheutuvat vastuu- ja riippuvuuskeskeytysriskit sisällytetään kybervakuutukseen, mutta niistä aiheutuvaa riskiä ei ole mahdollista hinnoitella tarkasti. Jos kolmansista osapuolista aiheutuvat vastuu- ja riippuvuuskeskeytysvahingot lisääntyvät huomattavasti, tulevat todennäköisesti kybervakuutusten ehdot, korvausmäärät ja hinnoittelu muuttumaan tulevaisuudessa. Kybervakuutusmarkkinat ovat Suomessa ja Euroopassa kuitenkin kehityksen alkuvaiheessa ja kybervakuutuksesta korvattujen vahinkojen määrä on niin pieni, että kybervakuutusten kehityssuunnista voi tehdä vain suuntaa antavia arvioita.

6.3 Tutkielman arviointi

Tutkielman merkitystä ja sen luotettavuutta tulee arvioida kriittisesti. Tämä tutkielma tehtiin riskienhallinnan ja kyberturvallisuuden alalla verrattain uudesta ja vähän tunnetusta aihepiiristä, joten tutkielman merkitys on sen uutuusarvossa. Uudesta aihepiiristä tehtävä tutkielma ei välttämättä tarjoa tarkkoja ja yksiselitteisiä vastauksia, vaan pikemminkin tuo esille uusia

näkökulmia, joista on mahdollista toteuttaa tulevaisuudessa uusia tutkimuksia. Vähän tunnettu ja uusi aihepiiri on tutkielman kannalta haaste mutta samalla myös sen ansio.

Uutuusarvon lisäksi tutkielman merkityksen määrittelee sen luotettavuus. Vaikka tutkimus pyritään tekemään mahdollisimman objektiivisesti ja virheitä välttäen, voivat tutkimustulosten luotettavuus ja pätevyys vaihdella. Luotettavuuden arvioinnissa voidaan käyttää useita erilaisia tapoja ja menetelmiä. Tavallisesti luotettavuuden arvioinnissa käytetään reliabiliteetin ja validiteetin käsitteitä. Tutkimuksen reliabiliteetilla kuvataan tutkimustulosten toistettavuutta ja kykyä tuottaa ei-sattumanvaraisia tuloksia. Tutkimustulosta voidaan pitää reliaabelina, jos kaksi tutkijaa päätyy samaan lopputulokseen käyttämällä samoja menetelmiä ja aineistoja. Lisäksi tuloksia voidaan pitää reliaabeleina, jos samaa ilmiötä tutkitaan eri tutkimuskerroilla ja saadaan sama lopputulos. Tutkimuksen validiteetilla kuvataan tutkimusmenetelmän tai mittarin kykyä mitata juuri sitä, mitä sen on tarkoituskin mitata. (Hirsjärvi ym. 2009, 231) Validiteetti voidaan jakaa eri osa-alueisiin, joista tavallisesti validiteettia määritetään rakennevalidiuden avulla. Rakennevalidiudella tarkoitetaan, onko tutkimus tehty siitä, mitä sen on oletettu koskevan ja tukevatko siinä käytetyt käsitteet tutkituksi aiottua ilmiötä. (Hirsjärvi & Hurme 2008, 187)

Tutkimuksen luotettavuuden arvioinnissa käytettävät reliabiliteetin ja validiteetin käsitteet ovat syntyneet kvantitatiivisen tutkimuksen piirissä, minkä vuoksi reliabiliteetti ja validiteetti ovat saaneet kvalitatiivisissa tutkimuksissa erilaisia tulkintoja. Kvalitatiivisen tutkimuksen arvioinnissa reliabiliteetin ja validiteetin käyttämistä arviointikriteerinä on kyseenalaistettu. Vaikka edellä käsiteltyjä termejä ei haluaisi käyttää, tulisi myös kvalitatiivisen tutkimuksen luotettavuutta arvioida jollakin menetelmällä. Kvalitatiivisen tutkimuksen luotettavuutta lisää, jos tutkija selostaa tarkasti tutkimuksen toteuttamisen kaikki vaiheet, aineiston tuottamisen olosuhteet, aineiston analyysin luokitteluperusteet ja tutkimustulosten tulkintaperusteet. (Hirsjärvi ym. 2009, 232–233)

Kvalitatiivisessa tutkimuksessa luotettavuuden arviointia ei voi erottaa yhtä selkeästi kuin kvantitatiivisessa tutkimuksessa, minkä vuoksi kvalitatiivisen tutkimuksen luotettavuuskriteereitä on kritisoitu selkeyden puutteesta. Kvalitatiivisen tutkimuksen luotettavuuden arvioinnissa tutkijalla on suuri rooli, koska hän joutuu jatkuvasti miettimään omia ratkaisujaan ja sa-

maan aikaan ottamaan kantaa analyysin kattavuuteen ja tutkimuksensa luotettavuuteen. Kvalitatiivisen tutkimuksen luotettavuuden arviointi voidaan pelkistää tutkimusprosessin luotettavuuden arvioinniksi. Kvalitatiivisen tutkimuksen luotettavuuden arviointiin käytettäviä käsitteitä voidaan soveltaa, kehittää vanhoille termeille uusia sisältöjä tai hylätä kokonaan vanhat termit. Tutkimuksen luotettavuuden arvioinnissa käsitteet itsessään eivät ole tärkeitä, vaan mikä sisältö niille annetaan. (Eskola & Suoranta 1998, 209–212) Tämän tutkielman arvioinnissa keskitytään tutkimusprosessin kokonaisuuden luotettavuuden arviointiin, eikä niinkään reliabiliteetin ja validiteetin arvioimiseen yksittäin.

Tämän tutkielman luotettavuutta arvioidaan ensin teoreettisen taustan ja lähteiden soveltuvuutta arvioimalla, jonka jälkeen arvioidaan empiirisen aineiston, analyysimenetelmän ja tulkintojen luotettavuutta. Tutkielman teoreettinen tausta ja käytetyt käsitteet pyrittiin valitsemaan mahdollisimman hyvin tutkittavaa ilmiötä selittäväksi. Ensimmäisellä teorialuvulla haluttiin antaa lukijalle kattava kuva aihepiirin perustana olevista kyberriskeistä, kyberuhista, haavoittuvuuksista sekä toimijoista ja motiiveista kyberriskien taustalla. Tieteellisessä kirjallisuudessa kyberriskejä, kyberuhkia ja haavoittuvuuksia käsitellään muun muassa riskienhallinnan, kyberturvallisuuden ja informaatioteknologian tieteenaloilla, mikä asettaa tutkijan tekemään valintoja käytettävien lähteiden ja käsitteiden hyödyntämisessä. Tälle aihepiirille on ominaista, että asioita käsitellään toisiaan sivuavilla käsitteillä, minkä vuoksi tutkielmassa käytettyjen käsitteiden johdonmukaisuuteen kiinnitettiin erityistä huomiota. Ensimmäisen teorialuvun muodostamaa taustateoriaa voidaan pitää luotettavana, koska siinä käytetty aineisto edustaa alalla yleisesti luotettuina pidettyjä lähteitä, ja se kuvailee tarkasti tutkielmassa selitettävän ilmiön perustana olevia ilmiöitä.

Toinen teorialuku muodostaa tutkielman tulkintateorian, jolla haluttiin kuvata tutkielman keskipisteenä olevaa ilmiötä eli kolmansista osapuolista aiheutuvia kyberriskejä, niiden arviointia ja suojautumista kybervakuutuksella. Tulkintateoriaa ja osittain myös tutkielman aiheenrajausta voidaan kritisoida muiden riskienhallintakeinojen poisjättämisellä ja keskittymisellä vain kybervakuuttamiseen. Kritiikki on perusteltua, koska kyberriskien vähentäminen on riskienhallintakeinoista yleisin, ja kybervakuuttaminen muodostaa toistaiseksi pienen osan kyberriskien hallintakeinoista. Kuten tutkielman johdantoluvussa on perusteltu, kolmansista osapuolista aihetuvat kyberriskit ovat usein epätodennäköisiä mutta vaikutuksiltaan suuria, ja

juuri tämän tyyppisiin riskeihin varaudutaan usein vakuutuksilla. Sen vuoksi on perusteltua keskittyä riskienhallintakeinoista vain kybervakuutukseen tutkielman tulkintateoriassa. Myös tulkintateoriaosuutta voidaan pitää luotettavana samoista syistä kuin taustateoriaa eli käytetty aineisto on yleisesti luotettavana pidettyä ja se selittää tutkittavana olevaa ilmiötä.

Tämän tutkielman luotettavuuden arvioinnissa keskeisintä on haastatteluaineiston ja sen analyysin luotettavuus. Haastatteluaineistona käytettiin kolmen kyberturvallisuusasiantuntijan ja kolmen kybervakuutusalan asiantuntijan haastatteluita. Haastatellun kohderyhmän jakamista kahteen asiantuntijuusalueeseen voidaan pitää perusteltuna ja tutkimuksen luotettavuutta lisäävänä, jotta aineistoon saadaan useampia näkökulmia. Kuuden asiantuntijahaastattelun aineistoa voidaan pitää tarpeeksi laajana, koska suurimmassa osassa kysymyksistä haastatellut olivat joko samaa tai lähes samaa mieltä. Haastattelujoukkoa kasvattamalla tuloksissa ei välttämättä olisi ollut huomattavia eroja. Haastatteluaineiston luotettavuutta lisää, että haastattelut litteroitiin mahdollisimman pian haastattelun jälkeen ja ne annettiin tarkastettavaksi haastateltavalle.

Eskolan ja Suorannan (1998, 211) mukaan kvalitatiivisessa tutkimuksessa lähtökohtana on tutkijan avoin subjektiviteetti ja sen myöntäminen, että tutkija on tutkimuksensa keskeinen tutkimusväline. Sen vuoksi tutkielman luotettavuuden arvioinnissa tulee tarkastella kriittisimmin tutkijan tekemää analyysiä ja tulkintoja. Kvalitatiiviseen aineistoon perustuvan analyysin luotettavuutta voidaan arvioida analyysin kattavuudella, arvioitavuudella ja toistettavuudella. Analyysin kattavuudella tarkoitetaan sitä, että tulkinnat eivät perustu satunnaisiin poimintoihin aineistosta. Arvioitavuudella kuvataan sitä, että lukija pystyy seuraamaan tutkijan päättelyä. Analyysin toistettavuudella tarkoitetaan, että analyysissä käytetyt luokittelu- ja tulkintasäännöt esitetään mahdollisimman yksiselitteisesti, jotta myös toinen tutkija pystyisi tekemään niitä soveltamalla samat tulkinnat. (Eskola & Suoranta 1998, 216–217)

Tämän tutkielman aineiston analysoinnissa noudatettiin edellä esitettyjä periaatteita. Analyysin luotettavuutta parannettiin aineiston kattavalla analysoinnilla, ja jokaisesta käsiteltävästä aihepiiristä käytiin läpi jokaisen haastateltavan vastaukset ja tuotiin esille olennaisimmat näkemykset. Arvioitavuutta lisättiin aineiston selkeällä ja johdonmukaisella esitystavalla. Jokaisesta teemasta tuotiin esille ensin haastateltavien näkemykset yksittäin, minkä jälkeen kunkin

alaluvun lopuksi tehtiin yhteenveto ja päätelmät aineiston yhtäläisyyksistä ja eroista. Näin lukija pystyy seuraamaan tutkijan päättelyä. Analysointimenetelmällä pyrittiin luokittelemaan aineisto teemojen mukaisesti sekä etsimään yhtäläisyyksiä ja eroja. Analysointimenetelmä ja sen kuvaus pyrittiin pitämään yksinkertaisena, jotta analyysi olisi toistettavissa.

Tutkielmaa voidaan kokonaisuutena pitää luotettavana edellä esitettyjen perusteiden mukaisesti. Tutkielma tarjoaa uusia näkemyksiä ja pohdintaa eikä niinkään tarkkoja ja yksityiskohtaisia vastauksia. Tämän tutkielman ensisijainen ansio on sen uutuudessa, koska se kartoittaa aiemmin tutkimatonta aihepiiriä.

6.4 Lopuksi

Tutkielmassa nostettiin esille, että kolmansista osapuolista aiheutuvia kyberriskejä arvioidaan samankaltaisilla menetelmillä kuin yritykseen suoraan kohdistuvia kyberriskejä. Ongelmakohdaksi tunnistettu näkymän puute yrityksen alihankkijaverkostoon ja heidän IT-järjestelmiinsä muodostavat riskienhallintatyölle selkeän ongelmakohdan, koska näkymän puutteen vuoksi riskien tunnistaminen ja luotettava arviointi on haastavaa ja joissakin tapauksissa jopa mahdotonta. Tämä ongelma-alue tarjoaa laajan ja monipuolisen jatkotutkimusmahdollisuuden, jota voi tarkastella eri näkökulmista. Esimerkiksi alihankinnan ketjuuntuminen suoran sopimussuhteen ulkopuoliselle yritykselle, niin sanotulle neljännelle osapuolelle, on kyberriskien näkökulmasta toistaiseksi tuntematonta aluetta. Alihankinnan pilkkominen pienempiin osiin ja ketjuttaminen on kasvava suuntaus ulkoistamisessa, joten kyberriskien huomioinen ja niiden tutkiminen tässä kontekstissa olisi hyödyllistä riskienhallinnan tieteellisessä kentässä.

Pilvipalvelut ovat yksi yleinen muoto yritysten käyttämistä kolmansista osapuolista. Pilvipalveluiden tulevaisuus näyttää valoisalta, vaikka niiden käyttämisestä aiheutuu tietyissä tilanteissa riskejä. Tiukentuva lainsäädäntö ja ihmisten kiinnostus tietosuojaa kohtaan saavat myös pilvipalveluntarjoajat kiinnittämään huomiota omiin käytäntöihinsä, avoimuuteen ja tietojen fyysisten säilytyspaikkojen valintaan. Pilvipalveluiden vaikutus kyberturvallisuuteen oli vain yksi osa tätä tutkielmaa, mutta kyseinen aihe osoittautui tutkimuksen edetessä ajankohtaiseksi ja hedelmälliseksi, josta voi tehdä kokonaan uusia tutkimuksia. Esimerkiksi pilvipalveluiden erilaisten palvelu- ja hankintamallien vaikutusta kyberturvallisuuteen on syytä tutkia

laajemmin, mitä ei tässä tutkielmassa käsitelty. Lisäksi pilvipalveluihin ulkoistettavan tiedonkäsittelyn hyötyjen ja riskien arvioimiseen tulisi saada lisää tieteellistä tietoa, joista yritykset voisivat saada tukea liiketoimintapäätöksilleen.

Kuten aiemmin on todettu, kybervakuutus on vielä melko uusi vakuutustuote, ja se hakee muotoaan vakuutuksen laajuuden, ehtojen ja maksimikorvausmäärien osalta. Tämän vuoksi kybervakuutus tarjoaa monia eri mahdollisuuksia ja näkökulmia tutkia kybervakuutusta. Tutkielmaa tehtäessä havaittiin selkeä ongelmakohta, koska vakuutusyhtiöt vakuuttavat asiakkaidensa käyttämistä kolmansista osapuolista aiheutuvia kyberriskejä, mutta niillä ei ole keinoja arvioida niistä aiheutuvia riskejä. Kybervakuutuksen hankintaprosessi on toistaiseksi vakiintumaton ja varsinkin suurempien vakuutuksenottajien kohdalla se nähdään raskaana. Vakuutusalaa käytännönläheisesti hyödyttävä jatkotutkimusmahdollisuus on tutkia kybervakuutuksen hankintaprosessia ja selvittää keinoja, millä yksinkertaisilla menetelmillä vakuutuksenottajan kyberriskit voidaan kartoittaa hakemusvaiheessa luotettavasti ja asiakkaan kannalta vaivattomasti.

LÄHDELUETTELO

Kirjallisuus:

Alasuutari, Pertti. 2011. Laadullinen tutkimus 2.0. 4. uud. painos. Tampere: Vastapaino.

Allianz. 2015. A Guide to Cyber Risk. Allianz Global Corporate & Specialty SE. Saatavilla: https://www.allianz.com/v_1441789023000/media/press/document/other/Allianz_Global_Corporate_Specialty_Cyber_Guide_final.pdf.

Allianz. 2016. Allianz Risk Barometer Top Business Risks 2016. Saatavilla: http://www.agcs.allianz.com/assets/PDFs/Reports/AllianzRiskBarometer2016.pdf.

Andreasson, Ari, Riikonen, Jaana & Ylipartanen, Arto. 2017. Osaava tietosuojavastaava. Helsinki: Tietosanoma.

Aon. 2017. Global Cyber Market Overview. Aon. Saatavilla: http://www.aon.com/inpoint/bin/pdfs/white-papers/Cyber.pdf.

Bendovschi, Andreea. 2015. Cyber-Attacks – Trends, Patterns and Security Countermeasures. Procedia Economics and Finance. Vol. 28. No. 1. 24–31.

Berliner, Baruch. 1985. Large risks and limits of insurability. Geneva Papers on Risk and Insurance. Vol. 1. No. 1. 313–329.

Biener, Christian, Eling, Martin & Wirfs, Jan H. 2015. Insurability of Cyber Risk: An Empirical Analysis. Geneva Papers on Risk and Insurance: Issues and Practice. Vol. 40. No. 1. 131–158.

Boyson, Sandor. 2014. Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. Technovation. Vol. 34. No. 7. 342–353.

Cebula, James J. & Young, Lisa R. 2010. A Taxonomy of Operational Cyber Security Risks. Carnegie Mellon University. Saatavilla: https://www.sei.cmu.edu/reports/10tn028.pdf.

Denning, Dorothy E. 2001. Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy. Teoksessa: Ronfeldt, David F. & Arquilla, John (toim.). Networks and netwars: the future of terror, crime, and militancy. Santa Monica, California: Rand. 239–289.

Eling, Martin & Schnell, Werner. 2016. What do we know about cyber risk and cyber risk insurance? Journal of Risk Finance. Vol. 17. No. 5. 474–491.

ENISA. 2017. Threat Landscape Report 2016. European Union Agency for Network and Information Security. Saatavilla: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016.

Eskola, Jari & Suoranta, Juha. 1998. Johdatus laadulliseen tutkimukseen. 10. painos. Tampere: Vastapaino.

Franke, Ulrik. 2017. The cyber insurance market in Sweden. Computers & Security. Vol. 68. No. 1. 130–144.

Gordon, Lawrence, Loeb, Martin & Sohail, Tashfeen. 2003. A framework for using insurance for cyber-risk management. Communications of the ACM. Vol. 46. No. 3. 81–85.

Hardy, Marianna. 2014. Target store data breaches: examination and insight. New York: Nova Publishers.

Hirsjärvi, Sirkka & Hurme, Helena. 2008. Tutkimushaastattelu: teemahaastattelun teoria ja käytäntö. Helsinki: Gaudeamus Helsinki University Press.

Hirsjärvi, Sirkka, Remes, Pirkko & Sajavaara, Paula. 2009. Tutki ja kirjoita. 15. uud. painos. Helsinki: Tammi.

Institute of Risk Management. 2014. Cyber Risk Executive Summary. Institute of Risk Management. Saatavilla: https://www.theirm.org/media/2293893/IRM_Cyber-Risk_Exec-Summ_A5_low-res.pdf.

ISO. 2008. ISO/IEC 27005:2008. International Organization for Standardization. Saatavilla: http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf.

Keegan, C. 2014. Cyber security in the supply chain: A perspective from the insurance industry. Technovation. Vol. 34. No. 7. 380–381.

Kyberturvallisuuskeskus. 2014. Pilvipalveluiden turvallisuus: mitä organisaatioiden tulisi huomioida pilvipalveluja hyödyntäessä. Viestintävirasto. Saatavilla: https://www.viestintavirasto.fi/attachments/tietoturva/Pilvipalveluiden_tietoturva_organisaatioille.pdf.

Limnéll, Jarno. 2014. Kyber rantautui Suomeen. Helsinki: Aalto-yliopisto.

Limnéll, Jarno, Majewski, Klaus & Salminen, Mirva. 2014. Kyberturvallisuus. Jyväskylä: Docendo.

Marotta, Angelica, Martinelli, Fabio, Nanni, Stefano, Orlando, Albina & Yautsiukhin, Artsiom. 2017. Cyber-insurance survey. Computer Science Review. Vol. 24. No. 1. 35–61.

Mell, Peter & Grance, Tim. 2011. The NIST definition of cloud computing. Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology Gaithersburg. Saatavilla: http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf.

Nishat Faisal, Mohd, Banwet, D. K. & Shankar, Ravi. 2007. Information risks management in supply chains: an assessment and mitigation framework. Journal of Enterprise Information Management. Vol. 20. No. 6. 677–699.

OCC. 2013. OCC BULLETIN 2013-29 Third-Party Relationships Risk Management Guidance. Office of the Comptroller of the Currency - U.S. Department of Treasury. Saatavilla: https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html.

Öğüt, Hulisi, Raghunathan, Srinivasan & Menon, Nirup. 2011. Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection. Risk Analysis. Vol. 31. No. 3. 497–512.

Park, Kristian, Sen, Sanjoy & Griffiths, Danny. 2015. Third Party Governance and Risk Management. Deloitte. Saatavilla: http://www2.deloitte.com/uk/en/pages/risk/articles/third-party-governance-risk-management.html.

Ponemon Institute. 2016. Tone at the Top and Third Party Risk. Ponemon Institute. Saatavilla: https://sharedassessments.org/summit/SA-2016-Ponemon-Study-Tone-At-The-Top-And-Third-Party-Risk-Final.pdf.

Ponemon Institute. 2017. 2017 Cost of Data Breach Study: Global Overview. Ponemon Institute. Saatavilla: http://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2017_Global_CODB_Report_Final.pdf.

Quigley, K., Burns, C. & Stallard, K. 2015. 'Cyber Gurus': A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection. Government Information Quarterly. Vol. 32. No. 2. 108–117.

Rakes, Terry R., Deane, Jason K. & Paul Rees, Loren. 2012. IT security planning under uncertainty for high-impact events. Omega. Vol. 40. No. 1. 79–88.

Rantala, Jukka & Kivisaari, Esko. 2014. Vakuutusoppi. 12. uudistettu painos. Helsinki: Finanssi- ja vakuutuskustannus Finva.

Rid, Thomas. 2012. Cyber War Will Not Take Place. Journal of Strategic Studies. Vol. 35. No. 1. 5–32.

Romanosky, Sasha. 2016. Examining the costs and causes of cyber incidents. Journal of Cybersecurity. Vol. 1. No. 1. 1–15.

Shackelford, Scott J. 2012. Should your firm invest in cyber risk insurance? Business Horizons. Vol. 55. No. 4. 349–356.

Sharma, Satyendra & Routroy, Srikanta. 2016. Modeling information risk in supply chain using Bayesian networks. Journal of Enterprise Information Management. Vol. 29. No. 2. 238–254.

Straub, Detmar W., Goodman, Seymour E. & Baskerville, Richard. 2008. Information security: policy, processes, and practices. Armonk, N.Y: M.E. Sharpe.

Touhill, Gregory J. & Touhill, C. J. 2014. Cybersecurity for executives: a practical guide. 1. painos. Hoboken, New Jersey: John Wiley & Sons, Inc.

Tuomi, Jouni & Sarajärvi, Anneli. 2018. Laadullinen tutkimus ja sisällönanalyysi. Helsinki: Kustannusosakeyhtiö Tammi.

U.S. Dept. of Justice. 2016. Ukrainian Hacker Admits Role in Largest Known Computer Hacking and Securities Fraud Scheme. United States Department of Justice. Saatavilla: https://www.justice.gov/usao-nj/pr/ukrainian-hacker-admits-role-largest-known-computer-hacking-and-securities-fraud-scheme.

Ulsch, N. M. 2014. Cyber threat: how to manage the growing risk of cyber attacks. 1. painos. Hoboken, New Jersey: Wiley.

Valtiovarainministeriö. 2016. EU-tietosuojan kokonaisuudistus, VAHTI-raportti 1/2016. Valtiovarainministeriö. Saatavilla: https://www.vahtiohje.fi/c/document_library/get_file?uuid=c97ee414-1fc0-4a91-969c-2ef0657605d1&groupId=10128.

von Solms, Rossouw & van Niekerk, Johan. 2013. From information security to cyber security. Computers & Security. Vol. 38. No. 1. 97–102.

Wangen, Gaute. 2015. The Role of Malware in Reported Cyber Espionage: A Review of the Impact and Mechanism. Information. Vol. 6. No. 2. 183–211.

Windelberg, Marjorie. 2016. Objectives for managing cyber supply chain risk. International Journal of Critical Infrastructure Protection. Vol. 12. No. 1. 4–11.

Wolf, Marty J. & Fresco, Nir. 2016. Ethics of the software vulnerabilities and exploits market. The Information Society. Vol. 32. No. 4. 269-279.

World Economic Forum. 2017. The Global Risks Report 2017 12th Edition. World Economic Forum. Saatavilla: http://www3.weforum.org/docs/GRR17_Report_web.pdf.

Zhang, Qi, Cheng, Lu & Boutaba, Raouf. 2010. Cloud computing: state-of-the-art and research challenges. Journal of Internet Services and Applications. Vol. 1. No. 1. 7–18.

Zissis, Dimitrios & Lekkas, Dimitrios. 2012. Addressing cloud computing security issues. Future Generation Computer Systems. Vol. 28. No. 3. 583–592.

Oikeudelliset lähteet:

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus)

Henkilötietolaki (22.4.1999/523)

Henkilölähteet:

Asiantuntija A. Jyväskylän yliopiston kyberturvallisuuden professori. Haastattelu 24.1.2018.

Asiantuntija B. Insta Group Oy:n turvallisuusjohtaja. Haastattelu 10.1.2018.

Asiantuntija C. Insta DefSec Oy:n teknologiajohtaja. Haastattelu 10.1.2018.

Asiantuntija D. Aon Finland Oy:n asiakaspäällikkö ja kybervakuutusasiantuntija. Haastattelu 26.1.2018.

Asiantuntija E. OP Vakuutus Oy:n Senior Underwriter. Haastattelu 23.11.2017.

Asiantuntija F. If Vahinkovakuutus Oyj:n tuotepäällikkö. Haastattelu 29.1.2018.

LIITTEET

Liite 1: Kyberturvallisuusasiantuntijoiden haastattelurunko

HAASTATELTAVAN TAUSTATIEDOT:

- Kerro taustastasi, koulutuksestasi, nykyisistä tehtävistäsi ja vastuistasi sekä kyberturvallisuusosaamisestasi.

KYBERRISKIEN TUNNISTAMINEN:

1. Kuinka vakavana uhkana pidät kolmansista osapuolista aiheutuvia kyberriskejä?
2. Millaisia kyberriskejä kolmannet osapuolet aiheuttavat?
3. Miten niitä voidaan tunnistaa?
4. Liittyykö niihin joitakin tyypillisiä kyberuhkia?
    a. Tyypillisiä haavoittuvuuksia?
5. Millaiset toimijat ovat useimmiten niiden taustalla (esim. kyberrikolliset, haktivistit)?

KYBERRISKIEN ARVIOINTI:

6. Miten kolmansien osapuolien aiheuttamien kyberriskien suuruutta voidaan arvioida?
    a. Kvantitatiivinen tai kvalitatiivinen arviointi?
7. Kuinka tietojenkäsittelyn ulkoistaminen ja pilvipalveluiden käyttäminen vaikuttavat kyberturvallisuuden tasoon?
8. Millaisia haasteita kolmannet osapuolet aiheuttavat kyberriskien hallinnassa?

MUUTA HUOMIOITAVAA:

9. Kuinka tehokkaana riskienhallintakeinona pidät kybervakuutusta verrattuna muihin riskienhallintakeinoihin?
10. Mitä vaikutuksia EU:n tietosuoja-asetuksella on kolmansista osapuolista aiheutuvien kyberriskien hallintaan?
11. Lisättävää?

Liite 2: Kybervakuutusasiantuntijoiden haastattelurunko

HAASTATELTAVAN TAUSTATIEDOT:

- Kerro taustastasi, koulutuksestasi, nykyisistä tehtävistäsi ja vastuistasi sekä kybervakuutus- ja kyberturvallisuusosaamisestasi.

KYBERRISKIEN TUNNISTAMINEN:

1. Kuinka merkittävänä pidät kolmansia osapuolia kyberriskien aiheuttajina?
2. Miten kolmansien osapuolten aiheuttamia kyberriskejä voidaan tunnistaa?
3. Mitkä ovat merkittävimpiä kolmansien osapuolten aiheuttamia kyberuhkia ja mitä haavoittuvuuksia ne hyödyntävät?

KYBERRISKIEN ARVIOINTI:

4. Miten kolmansien osapuolten aiheuttamien kyberriskien suuruutta voidaan arvioida?
5. Kuinka tietojenkäsittelyn ulkoistaminen ja pilvipalveluiden käyttäminen vaikuttavat kyberturvallisuuden tasoon?

KYBERVAKUUTUS:

6. Millainen on kybervakuutustuotteenne ja kattaako se kolmansista osapuolista johtuneet vahingot?
7. Arvioidaanko kybervakuuttamisessa kolmansista osapuolista aiheutuvia kyberriskejä?
    a. Vaikutukset ehtoihin, rajoituksiin tai hinnoitteluun?
8. Jos henkilötietojen käsittelyä on ulkoistettu ja vahingon aiheuttaa kolmas osapuoli, kuinka kybervakuutus korvaa vahingon kärsineille ja rekisterinpitäjälle aiheutuneet vahingot?
    a. Mahdolliset sanktiot EU:n tietosuoja-asetuksen laiminlyönnistä?
9. Parantaako kybervakuutus yritysten tietoisuutta kyberriskeistä ja parantaako se yrityksen kyberturvallisuuden tasoa?
10. Lisättävää?