Tampereen yliopisto

Essi Antila

KYBERVAKUUTUKSEN TARPEEN MÄÄRITTELY JA VALINTAAN VAIKUTTAVAT TEKIJÄT

Tapaustutkimus yrityksen kybervakuutuksen hankinnasta

Johtamisen ja talouden tiedekunta
Kandidaatintutkielma
Huhtikuu 2021

TIIVISTELMÄ

Essi Antila: Kybervakuutuksen tarpeen määrittely ja valintaan vaikuttavat tekijät - Tapaustutkimus yrityksen kybervakuutuksen hankinnasta
Kandidaatintutkielma
Tampereen yliopisto
Kauppatieteiden tutkinto-ohjelma: Vakuutus ja riskienhallinta
Huhtikuu 2021

Tässä kandidaatintutkielmassa tutkitaan kyberriskejä ja kybervakuutuksen hankintaa yrityksen näkökulmasta. Tutkimus on toteutettu kvalitatiivisena tapaustutkimuksena, jossa tapaus on yrityksen kybervakuutuksen hankinta. Tutkielman tarkoituksena on kartoittaa ja kuvailla yrityksen kybervakuutuksen ottamista ja sen prosessimaista etenemistä. Tutkielma tutkii yrityksen kriteerejä kybervakuutuksen tarpeen kartoituksessa sekä tunnistaa kybervakuutuksen valinnan vaiheisiin vaikuttavia tekijöitä. Tutkimuskysymykset ovat 1. Miten yritys määrittelee tarpeen kybervakuutukselle? ja 2. Mitkä tekijät vaikuttavat yrityksen kybervakuutuksen valintaan?

Teknologian ja digitalisaation kehityksen myötä kyberriskit ovat yleistyneet yritysten ja yhteiskunnan toimintaa uhkaavana ilmiönä. Kyberriskit ovat luonteeltaan jatkuvasti muuttuvia verkon kautta uhkaavia riskejä. Vakuutusala on vastannut kysyntään luomalla vakuutustuotteen kyberriskeille, kybervakuutuksen. Kyberriskien ja -ilmiöiden kehitystä ei voida ennustaa. Kybervakuutus toimii keskeisenä yritysten riskienhallinnan välineenä nykymaailman digitalisoituneessa toimintaympäristössä.

Tutkielman teoriaosuus koostuu kahdesta pääluvusta, jotka käsittelevät kyberriskin ja kybervakuutuksen ominaisuuksia, kybervakuutuksen hankinnan vaiheita sekä kybervakuutusta osana yrityksen riskienhallintaa. Tutkimusaineisto muodostui teoriaosuudessa kirjallisuudesta ja tieteellisistä julkaisuista. Teoriapohjan muodostivat kyberriskit, niiden vakuutuskelpoisuus sekä vakuutuksen hankinta prosessina. Tutkielman empiirinen osuus muodostui tapaustutkimuksen kohdeyrityksen haastattelusta, joka toteutettiin puolistrukturoituna teemahaastatteluna.

Tutkimuksen johtopäätöksien perusteella voidaan todeta, että yrityksen kybervakuutuksen tarpeisiin vaikuttavat toimialakohtaiset tekijät, yrityksen omat kriteerit ja asiakassopimuksien ehdot. Asiakassopimuksissa määritellään toimijalle yhä enemmän vastuuta kyberriskeistä. Yrityksillä ei ole riittävää asiantuntemusta kyberriskeistä, minkä seurauksena vakuutusmeklarin käyttö on yleistä kybervakuutusturvaa hankittaessa. Vakuutusmeklareiden suhteet vakuutusyhtiöihin, kokonaisasiakkuuden vaikutus, yrityksen liiketoiminnan riskisyys ja sattuma vaikuttavat kybervakuutuksen hankintaprosessin etenemiseen ja ohjaavat yrityksen kybervakuutuksen valintaa.

Tutkimuksen tulokset vahvistavat näkemystä kyberriskin alati muuttuvasta luonteesta ja sen vakuutusturvan märittelyn vaikeudesta. Kybervakuutuksen ottaminen on yrityksille usein haastavaa ja monimutkaista. Kybervakuutuksia ja niihin liittyvää terminologiaa on yksinkertaistettava ja selvennettävä. On toistaiseksi epäselvää, kenen vastuulla se on. Kybervakuutuksen vaikeaselkoisuuden vuoksi ulkopuolisten asiantuntijoiden ja vakuutusmeklarien käyttö kybervakuutusta ottaessa on lähes välttämätöntä, ellei yritys halua valmista kybervakuutuspakettia kustomoidun ratkaisun sijaan.

Avainsanat: kyberriski, kybervakuutus, vakuutuksen hankinta, vakuutusprosessi

SISÄLLYSLUETTELO

1 JOHDANTO

1.1 Tutkielman aihealueen esittely

Ensimmäiset kybervakuutukset ovat tulleet markkinoille 25 vuotta sitten. Kuitenkin vasta viime vuosina markkinat ovat merkittävästi kasvaneet, ja ne jatkavat yhä laajentumistaan. Kybervakuutusmarkkinoiden arvioidaan kasvavan maailmanlaajuisesti vuoden 2020 8 miljardista USD:sta jopa 20 miljardiin USD:iin vuoteen 2025 mennessä. Valtaosa markkinoista muodostuu yritysasiakkaiden kybervakuutuksia. (Statista Research Department, 2021.) Keskeisiä tekijöitä kybervakuutuksen nousevaan suosioon ja kysyntään ovat digitalisaation myötä kasvava tarve, muutokset lainsäädännössä ja kyberriskitietoisuuden kasvu.

Teknologian kehitys ja digitalisaatio ovat mullistaneet ihmisten ja organisaatioiden toimintatapoja ja -puitteita. Kehittynyt, moderni teknologia yhdistää valtiot, finanssialan instituutiot, yritykset sekä ihmiset toisiinsa. (Rubini, 2019, 193.) Riippuvuus teknologiasta lisää digitaalisen turvallisuuden riskejä. Näin ollen yhä useampi yritys ottaa vakuutuksen kyberriskien varalta. (OECD, 2020b.) Kybervakuutus voidaan nähdä ajankohtaisena riskienhallintavälineen jokaiselle yritykselle.

Viime vuosina tietomurtojen määrä on ollut kasvussa, ja niiden kohteeksi joutuneet yritykset ovat saaneet laajaa mediahuomiota. Esimerkiksi Target, Marriott Hotels, Facebook ja Suomessa Vastaamo ovat joutuneet isojen tietomurtojen kohteeksi. Tietovuodon seurauksena yrityksen maine kärsii lähes väistämättä, sillä yritykseen kohdistuu negatiivista huomiota. Kyberriskin realisoituessa isonkin yrityksen toiminta voi keskeytyä ja jopa päättyä. Esimerkiksi Vastaamon tietomurron ja sen seurausten myötä Vastaamo joutui hakeutumaan konkurssiin. Kyber- ja keskeytymisriski ovatkin Allianzin (2020) riskibarometrin mukaan kaksi suurinta riskiä yritykselle. Nämä kaksi riskiä ovat vahvasti toisiinsa linkittyneitä.

Lainsäädännöllä on huomattava rooli tarkasteltaessa kyberriskitietoisuuden kasvua ja kybervakuutuksien kasvavaa kysyntää. EU-maissa vuonna 2018 voimaan astuneen

GDPR-asetuksen (General Data Protection Regulation) tavoitteena on parantaa henkilötietojen suojaa ja tietosuojaoikeuksia sekä yhtenäistää tietosuojasääntelyä digitalisoituneilla markkinoilla. Asetus velvoittaa yrityksiä ilmoittamaan tapahtuneista tietomurroista. Tämän on nostanut kansan tietoisuuteen tapahtumia, jotka olisi aikaisemmin saatettu salata. GDPR-asetus ohjaa yksityisyydensuojan turvaamiseksi yrityksiä hallinnoimaan dataansa tarkemmin ja suojautumaan tietovuodoilta. Asetuksen myötä yrityksille on tullut uusia velvollisuuksia ja sanktioita. (European Commission, 2020.) Tiukentuneen sääntelyn ohella on yhä yleisempää, että liikekumppanit vaativat kyberriskeiltä suojautumista sekä vastaavia ennaltaehkäiseviä toimenpiteitä yrityksiltä (Munich Re, 2020a).

Vaikka kyberriskitietoisuus on kasvanut, moni yritys ymmärtää kyberriskin realisoitumisesta seuraavien vahinkojen laajuuden liian myöhään. Kybervakuutus on tuntemattomampi vakuutustuote, joten yritysten voi olla haastavaa arvioida omia tarpeitaan ja tarjolla olevia vakuutuksia. Kyberriskeistä ja -vakuutuksista on saatavilla vähän tilastoitua tietoa. Tilastotietoa ei ole kerätty tai hyödynnetty tarpeeksi, jotta voitaisiin saada vertailukohtaa ja luotettavaa tietoa kyberriskeihin liittyvistä tapahtumista ja tappioista (OECD, 2017). Kybervakuutusehdot ja -sopimukset koetaankin vakuutuksenottajan näkökulmasta monimutkaisina (OECD, 2016).

Yleinen väärinkäsitys on, että mitä suurempi yritys on, sitä suurempi on altistuminen kyberriskille. Tämä ei kuitenkaan välttämättä pidä paikkaansa. Riskialttiina pidettyjä yrityksiä yhdistää ennemminkin niiden toimiala ja riippuvuus toimitusketjuverkostostaan päivittäisessä toiminnassaan: Esimerkkinä rahoituslaitokset, terveydenhuollon yritykset ja muut toimijat, jotka keräävät ja käsittelevät paljon henkilökohtaista tietoa. (Munich Re, 2020b.) Tämän tutkielman tutkimusaiheita ovat kyberriskit, kybervakuutus ja kybervakuutuksen hankinta.

1.2 Tutkimuksen tavoitteet ja tutkimuskysymykset

Tutkielma voi olla luonteeltaan ennustava, kartoittava, kuvaileva ja/tai selittävä (Hirsjärvi, Remes & Sajavaara, 2009, 138). Tämä tutkielma on luonteeltaan kartoittava ja kuvaileva. Tutkielman tavoitteena on kartoittaa yrityksen tarvetta kybervakuutukselle ja kybervakuutuksen hankinnan prosessimaista etenemistä lopulliseen valintaan

vakuutuksesta. Tutkielmassa kuvaillaan myös kyberriskin ja kybervakuutustuotteen ominaisuuksia sekä kybervakuutuksen hankinnan vaiheita.

Tutkielman tutkimuskysymykset ovat seuraavat:

1. Miten yritys määrittelee tarpeen kybervakuutukselle?

2. Mitkä tekijät vaikuttavat yrityksen kybervakuutuksen valintaan?

Ensimmäisen tutkimuskysymyksen tavoitteena on kartoittaa tekijöitä, jotka vaikuttavat yrityksen kybervakuutuksen tarpeen määrittelyyn. Tarkoituksena on tunnistaa tekijöitä yrityksen kybervakuutuksen tarpeen ja kriteerien määrittelyn taustalla. Tutkimuskysymykseen etsitään vastausta tutkimalla kyberriskin ja -vakuutuksen luonteita ja ominaisuuksia, jotta voidaan luoda käsitys niihin liittyvistä tekijöistä. Vakuutuksen hankinnan ensimmäisiä vaiheita kartoittamalla niin yrityksen kuin vakuutuksenantajan näkökulmasta pyritään tunnistamaan yrityksen kriteereihin vaikuttavia ulkoisia ja sisäisiä tekijöitä.

Toisen tutkimuskysymyksen tavoitteena on kartoittaa yrityksen kybervakuutuksen valinnan etenemistä. Tarkoituksena on tunnistaa kybervakuutuksen hankinnan kartoitus-, vertailu- ja neuvotteluvaiheisiin vaikuttavia tekijöitä. Tutkimuskysymystä käsiteltäessä on ensinnäkin tunnistettava vakuutusyhtiön ja vakuutusmeklariyhtiön ominaisuuksia ja eroja kybervakuutuksen tarjoajina ja välittäjinä. Tutkimuskysymykseen etsitään vastausta tutkimalla vakuutuksen hankinnan eri vaiheita ja yrityksen valintaa ohjaavia tekijöitä. Molempiin tutkimuskysymyksiin haetaan vastauksia teoriapohjan sekä empiirisen aineiston yhdistelmästä. Tutkimusaineisto ja -menetelmät ovat esitelty tarkemmin alaluvussa 1.4.

1.3 Tutkimuksen rajaukset ja keskeisiä käsitteitä

Kandidaatintutkielman laajuuden ja aiheen hallittavuuden kannalta tutkielmaan on tehty rajauksia. Tutkielma on rajattu tarkastelemaan Suomen kybervakuutusmarkkinoilta saatavia yrityksien kybervakuutuksia. Näkökulmaa on rajattu edelleen tarkastelemaan erityisesti PK-yrityksiä vakuutuksenottajina. Tutkielma tarkastelee kybervakuutusta vain

erillisenä tuotteena, eikä huomioi jo olemassa oleviin vakuutuksiin lisäturvana saatavilla olevia lisäpaketteja. Kybervakuutuksen hankinnan vaiheita tutkittaessa on tarkasteltaviksi osiksi rajattu vakuutuksen valintaa edeltävät aiheet, eikä tässä tutkielmassa syvennytä kybervakuutuksen omistukseen ja sen jälkeisiin vaiheisiin.

Kyberriski määritellään yksinkertaisimmillaan yksityishenkilöitä ja/tai organisaatioita uhkaavaksi internet-pohjaiseksi riskiksi (Statista Research Department, 2021). Tämä tutkielma tarkastelee kyberriskejä yrityksen, ei yksityishenkilön, näkökulmasta. Voidaan kuitenkin todeta, että suuri osa kyberriskeistä voivat koskea sekä yksityishenkilöitä että yrityksiä. Kyberriskin moninaisiin määritelmiin ja ominaisuuksiin syvennytään tarkemmin pääluvussa 2.

Kybervakuutus on vakuutustuote kyberriskien varalle. Yleisiä kybervakuutuksen kattamia kuluja ovat liiketoiminnan keskeytymisestä ja tulojen menetyksestä, tietojen palauttamisesta ja korvauskustannuksista aiheutuvat kulut. Kybervakuutus suojaa yritystä sekä ulkoisilta että sisäisiltä kyberriskeiltä. (Lubin, 2019, 14-15.) Kybervakuutus on yksi riskienhallinnan väline. Kybervakuutukseen ja sen hankinnan vaiheisiin syvennytään tarkemmin pääluvuissa 2 ja 3.

Vakuutuksenantaja ja *vakuutuksenottaja* ovat vakuutussopimuksen osapuolet (Rantala & Kivisaari, 2020, 56). Tässä tutkielmassa käsitellään vakuutusyhtiöitä kybervakuutuksen antajina ja vakuutusmeklariyhtiöitä kybervakuutuksen välittäjinä. Vakuutusyhtiöt myöntävät itse vakuutuksia, kun taas vakuutusmeklariyhtiöt toimivat asiakasyrityksensä edustajina ja hoitavat heidän toimeksiantamana vakuutusasioita vakuutusyhtiöiden kanssa. (Määttä & Forsman, 2005, 28.) Tutkielma on rajattu tarkastelemaan kybervakuutuksen hankintaa ja sen vaiheita Suomessa.

Vakuutuksenottajasta puhuttaessa tarkoitetaan tässä tutkielmassa PK-yritystä vakuutuksenottajana. PK-yrityksiksi luetaan pienet ja keskisuuret yritykset, joiden palveluksessa on alle 250 työntekijää ja vuosittainen liikevaihto on enintään 50 miljoonaa euroa tai taseen loppusumma enintään 43 miljoonaa euroa. (Tilastokeskus, 2021.) Tämän tutkielman empiirinen osuus muodostuu IT-alalla toimivan PK-yrityksen haastattelusta. Tutkielman viimeinen rajaus onkin tarkastella kybervakuutuksen hankintaa IT-toimialalla.

1.4 Tutkimusmenetelmät ja -aineisto

Kyberriskit ja kybervakuutus ovat toistaiseksi vähän tutkittu aihe. Kyberriski ei ole ilmiönä uusi, mutta se on jatkuvasti kehittyvä ja muuttuva riski. Aihepiirin tuntemattomuuden ja tutkielman tavoitteiden johdosta tutkimusmenetelmäksi on valittu laadullinen eli kvalitatiivinen tutkimusmenetelmä. Kvalitatiivinen tutkimus pyrkii ymmärtämään tutkimusaihetta ja muodostamaan tulkintoja (Eskola & Suoranta, 1998, 44). Eskolan ym. (1998, 48) ja Erikssonin & Koistisen (2005, 34) mukaan kvalitatiivisten tutkimusten tavoitteena ei ole muodostaa empiirisesti yleistäviä päätelmiä kuten tilastollisessa tutkimuksessa. Sen takia onkin tärkeää, että kvalitatiivisen tutkimuksen analysoitava aineisto muodostaa kokonaisuuden tai tapauksen.

Tämä tutkielma on laadullinen tapaustutkimus. Tutkielma koostuu teoria- ja empiriaosuudesta. Laadullisen tutkimuksen teorian tehtävänä nähdään tavallisesti teoria keinona ja teoria päämääränä. Teoria keinona hyödyntää teoriaa tutkimusta tehdessä, kun taas teoria päämääränä pyrkii kehittämään teoriaa edelleen. Tämä tutkielma käyttää teoriaa keinona. Teorian avulla aineistosta pystytään rakentamaan tulkintoja. Kvalitatiivinen tutkimus etenee usein induktiivisesti, aineistolähtöisesti yksittäisestä havainnosta edetään yleisempiin väitteisiin. (Eskola ym., 1998, 59.)

Tutkielman tutkimuskysymyksiin etsitään vastauksia teoriapohjan ja empiirisen aineiston avulla. Teoriapohja muodostuu kyberriskistä ja sen vakuutuskelpoisuudesta sekä vakuutuksen hankinta prosessista. Tutkielman teoriapohjan aineistona käytetään aineistona kirjallisuutta, tieteellisiä julkaisuja, internet-lähteitä ja aiempia tutkimuksia. Tutkimusaiheena kyber ja kybervakuutukset ovat muuttuneet ja kehittyneet viime vuosina paljon, joten aineistoa kerätessä on kiinnitetty huomiota ajankohtaisten ja relevanttia tietoa sisältävien lähteiden käyttöön. Ajankohtaista tietoa on kerätty erityisesti isojen kansainvälisten finanssiyhtiöiden Munich Ren ja Allianzin, Statista Research Departmentin sekä Euroopan Taloudellisen yhteistyön ja kehityksen järjestön (OECD) tutkimuksista ja julkaisuista.

Tämän tutkimuksen empiirinen osuus muodostuu tapaustutkimuksen kohteena olevan IT-alan yrityksen haastattelusta. Tutkielma on siis empiriaan pohjautuva tapaustutkimus. Tapaustutkimuksen on tarkoitus määritellä ja analysoida tapausta. Tutkielman

tutkimuskysymykset ja aineistojen analyysit perustuvat tälle määrittelylle. (Eriksson ym., 2005, 1, 4.) Haastattelut ovat tyypillisiä tapaustutkimuksen aineistolähteitä (Eriksson ym., 2005, 27).

Tämän tutkielman tapaustutkimuksen kohteena on yrityksen kybervakuutuksen hankinnan prosessi. Tutkimuksen empiirinen aineisto on poimittu tarkoituksenmukaisesti ja koostuu pienestä, vain yhdestä, tapaustutkimuksesta. Valinta on kuitenkin linjassa tutkimusmenetelmän kanssa, sillä kvalitatiivinen tutkimus ei pyri tilastolliseen yleistämiseen. Kvalitatiivinen tutkielma pyrkii kuvaamaan tapahtumaa tai ilmiötä ja ymmärtämään sitä. (Eskola ym., 1998, 44.) Tässä tutkielmassa tapaustutkimus on valittu menetelmäksi, sillä yrityksen kybervakuutuksen hankintaa halutaan ymmärtää huomioiden siihen liittyvät olosuhteet ja taustat.

Tapaustutkimuksen kybervakuutusta hankkiva yritys on alalleen tyypillinen. Yritys on toiminut IT-alalla yli 35 vuotta. Yritys on suomalainen PK-yritys, joka toimittaa IT-ratkaisuja asiakkailleen Suomeen, Ruotsiin ja Norjaan. Yrityksen asiakkaat ovat terveydenhuollon toimijoita. Yrityksen henkilöstöön kuuluu noin 90 henkilöä. Liikevaihto on 15 miljoonaa euroa. Yritys on hankkinut ensimmäisen kybervakuutuksensa 2020 loppuvuodesta.

Empiirinen aineisto kerätään yrityksen haastattelulla. Haastattelutyypiksi on valittu puolistrukturoitu teemahaastattelu. Puolistrukturoitu teemahaastattelussa ei ole valmiita vastausvaihtoehtoja, eikä kysymyksillä ole tarkkaa muotoa tai järjestystä. Teema-alueet on etukäteen päätetty. (Eskola ym., 1998, 63) Tämän haastattelutyypin valinta mahdollistaa jouston ja tarkentavien kysymysten esittämisen haastattelutilanteessa. Haastattelut analysoidaan sisällönanalyysin keinoin. Empiirisen aineiston tarkempi kuvaus ja käsittely on esiteltynä luvun neljä alussa.

1.5 Aikaisemmat tutkimukset

Tutkimuksen pääaiheita ovat kyberriskit ja kybervakuutus. Kybervakuutusala on toistaiseksi vakiintumaton ja siihen liittyvää tietoa on alettu julkaisemaan hiljalleen 2000-luvun alusta alkaen. Suurin osa tutkimuksista on englanninkielisiä. Kyberilmiöt ovat tutkimuskohteena muuttuva, eivätkä vakuutusalan käytänteet sen tutkimisessa ole vielä

vakiintuneita. Yksi viimeisimmistä julkaisuista on Strupczewskin (2021) tekemä vertaileva analyysi kyberriski-termin moninaisista määritelmistä. Analyysin tulokset viittasivat siihen, ettei vakiintunutta terminologiaa ole vielä syntynyt, mutta sitä tarvitaan, jotta ala pääsee kehittymään ja ennen kaikkea kyberriskien arviointitavat yhtenäistyvät.

Suomessa Tampereen yliopistossa Roikola on tehnyt tutkimusaiheeseen liittyvän pro gradu -tutkielman ''Kyberriskeiltä suojautuminen ja kybervakuutusmarkkinat Suomessa'' (2017). Tutkielmassa tutkittiin suomalaisten yritysten varautumista kyberriskeihin sekä Suomen kybervakuutusmarkkinoita vuonna 2016. Rytkönen on tehnyt pro gradu -tutkielman ''Kyberriskien arviointi ja kybervakuuttaminen – Kolmannet osapuolet kyberriskien lähteenä'' (2018), jossa tarkastellaan kolmansista osapuolista aiheutuvia kyberriskejä ja mahdollisuutta arvioida ja hallita niitä. Rytkönen tuo esille tutkielmassaan myös pilvipalveluiden käytön vaikutuksen yritysten kyberturvallisuuteen. Soininen on kandidaatintutkielmassaan ''Kyberriskit ja niiden hallintakeinot henkivakuutusyhtiössä: Case Nordea Henkivakuutus Suomi Oy'' (2020) tutkinut kyberriskejä henkivakuutusyhtiön kontekstissa vakuutusyhtiön näkökulmasta. Aihepiirin ajankohtaisuudesta esimerkkinä Salovaaran kandidaatintutkielma ''Kybervalmius osana kuntien toteuttamaa riskienhallintaa. Kyberturvallisuuden järjestäminen suomalaisissa kunnissa – Case Kokemäen kaupunki'' (2020), jonka tulokset osoittavat kyberturvatoimien olevan tärkeä osa organisaatioiden riskienhallintaa.

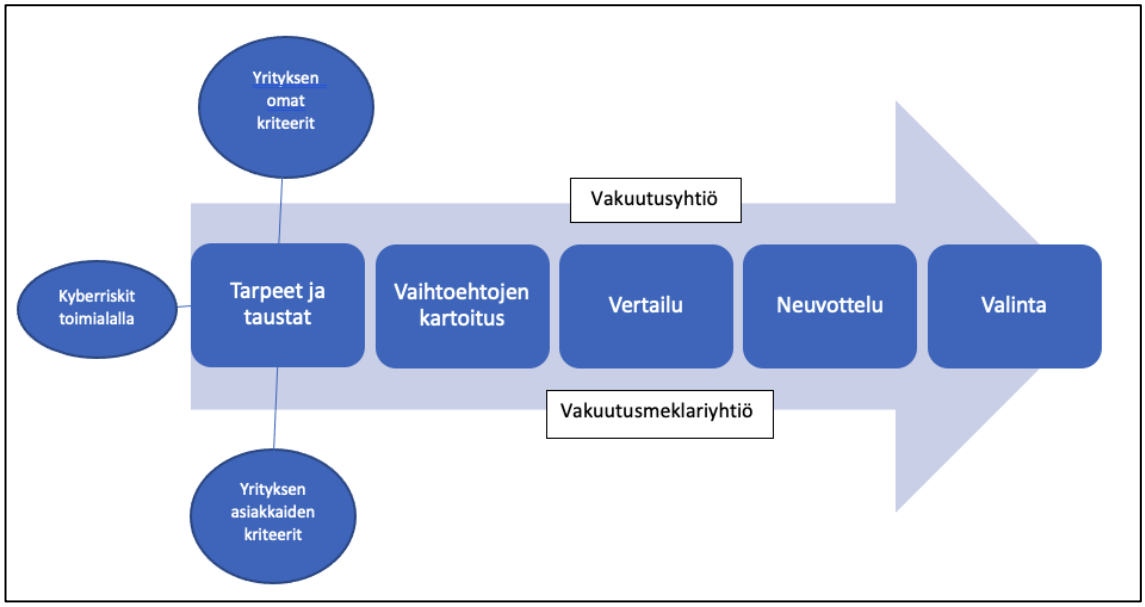
Kybervakuutuksen hankinnan vaiheita ja niihin vaikuttavia tekijöitä ei ole aikaisemmin tutkittu yrityksen näkökulmasta. Aikaisemmat tutkimukset keskittyvät lähinnä vakuutuksen omistuksen aikaisiin vaiheisiin, eivätkä sitä mitkä tekijät ovat johtaneet vakuutuksen valintaan. Tämä tutkielma tarjoaa siis uutta näkökulmaa aiheeseen.

1.6 Teoreettinen viitekehys

Kvalitatiivisessa tutkimuksessa tarvitaan teoriaa lähtökohtaisesti enemmän kuin kvantitatiivisessa. Teoriaa tarvitaan kahdenlaista: taustateoriaa ja tulkintateoriaa. Aineistoa tarkastellaan taustateoriaa vasten.

Tutkijalla on oltava mielessään tutkimuskysymykset ja niiden avulla määritetty tulkintateoria. Tulkintateoriat ohjaavat tutkijaa aineistoa tutkaillessa. Tulkintateorioiden

määrittäminen on myös keskeistä, jotta teoria, aineisto ja analyysi muodostavat tutkielmasta eheän kokonaisuuden. (Eskola ym., 1998, 61.) Tämän tutkielman taustateoriana ovat kyberriskit ja sen vakuuttamisen prosessit. Tutkielman tulkintateorioiksi on valittu yrityksen vakuutuksen hankintaprosessi yrityksen näkökulmasta: tarpeiden kartoitus, vaihtoehtojen kartoitus ja tekijät vakuutuksen valinnan takana.



Kuvio 1: Teoreettinen viitekehys

Tutkielman teoreettisen viitekehyksen (kuvio 1) muodostamisessa on käytetty pohjana Batran & Kellerin (2016) määritelmää kuluttajan päätöksenteon vaiheista. Batran ym. (2016, 124-126) ovat kuvanneet kuluttajan päätöksentekoa askeleittain. Jokaiseen askeleeseen kuuluu tietty tiedon tarve, ja kun se on tyydytetty, on mahdollista siirtyä seuraavalle askeleelle. Jokainen askel vie lähemmäksi lopullista päätöstä, mutta askelia voi joutua palaamaan taaksepäin tai päätöksentekoprosessista voi pudota kokonaan pois. Tämän teorian vaiheita pystytään soveltamaan yrityksen vakuutuksenhankintaa tutkittaessa. Teoriasta on poimittu tämän tutkimuksen rajauksiin sopivat kohdat ja paikoitellen muokattu kohtien otsikointia. Päätöksenteon vaiheiksi on poimittu tarpeet ja taustat, vaihtoehtojen kartoitus, vertailu, neuvottelu ja valinta. Vaiheet on sijoitettu nuolen sisälle teoreettisen viitekehyksen kuvioon (kuvio 1). Nuoli kuvaa vakuutusprosessin etenemistä ja nuolen sisällä vaiheet kuvaavat asiakkaan eli vakuutuksenottajan päätöksentekoa.

Teoreettinen viitekehys kuvaa kybervakuutuksen hankinnan prosessina ja esittelee tässä tutkielmassa huomioitavia päätöksenteon vaiheita ja niihin vaikuttavia tekijöitä. Erityisesti tämä tutkielma huomioi tarpeita ja taustoja tutkittaessa yrityksen omat, yrityksen asiakkaiden ja toimialan kriteerit. Sitä seuraavat vaiheet vaihtoehtojen kartoitus, vertailu ja neuvottelu ennen vakuutuksen valintaa. Näitä vaiheita tutkittaessa huomioidaan vakuutusyhtiöt kybervakuutuksen antajina sekä vakuutusmeklariyhtiöt kybervakuutuksen välittäjinä.

1.7 Tutkielman rakenne

Tutkielma noudattaa perinteistä IMRD-rakennetta. Tutkielma koostuu viidestä pääluvusta. Johdannossa esitellään tutkielman aihealue, tutkimuskysymykset ja -tavoitteet, keskeiset käsitteet ja rajaukset, tutkimusmenetelmät ja -aineistot, aikaisemmat tutkimukset, teoreettinen viitekehys sekä tutkielman rakenne.

Tutkielman teoreettinen osuus koostuu kahdesta pääluvusta. Luku 2 taustoittaa kyberriskien ja kybervakuutuksen ominaisuuksia sekä esittelee kybervakuutuksen roolia osana yrityksen riskienhallintaa IT-alalla. Luvussa 3 syvennytään kybervakuutuksen valintaan. Alkuun esitellään kybervakuutuksen elinkaaren vaiheet. Alaluku 3.2 esittelee Suomen markkinoilla kybervakuutuksia myöntävät ja välittävät tahot, vakuutusyhtiöt ja vakuutusmeklariyhtiöt. Luvussa kuvataan kybervakuutuksen hankinnan etenemistä ja pohditaan vakuutusyhtiöiden ja vakuutusmeklariyhtiöiden toimintaa, antamia tietoja ja vakuutustarjouksia sekä prosessiin vaikuttavia tekijöitä.

Neljännessä pääluvussa esitellään tapaustutkimus ja haastattelun tulokset. Haastatteluaineisto analysoidaan teoriaosuuksissa esitettyjen seikkojen valossa. Tämän jälkeen tutkielman teoria- ja empiriaosuudet on käsitelty, jonka jälkeen voidaan esittää johtopäätökset. Viides pääluku vastaa tutkimuskysymyksiin, arvioi tutkimusta ja pohtii mahdollisuuksia jatkotutkimukselle. Lähteet ja liitteet ovat listattuna tutkielman lopussa.

2 KYBERRISKIT JA KYBERVAKUUTUS

2.1 Kyberriski

2.1.1 Kyberriskin määritelmiä ja ominaisuuksia

Ennen kyberriskin määritelmiin ja sitä kautta sen ominaisuuksiin tutustumista on keskeistä ymmärtää käsitteet kyber ja kyberisku, joiden määritelmät toimivat pohjana kyberriskille. Termi *kyber* viittaa sähköisiin viestintäverkostoihin sekä virtuaalitodellisuuteen. Kyberiin liittyy siis aineettomuus. (Evans, 2019, 476.) Kyber nähdään poikkeuksellisen nopealiikkeisenä ja ennalta-arvaamattomana (Antonucci, 2017, 102-103). Nämä ominaisuudet erottavat kyberriskit muista riskeistä. *Kyberiskuksi* kutsutaan tapahtumaa, jossa rikollinen taho yrittää luvattomasti päästä käsiksi dataan verkon tai laitteen kautta. Kyberisku voi kohdistua järjestelmiin, prosesseihin, tekniikkaan ja dataan. Kun puhutaan altistumisesta kyberiskulle tai muulle kybertapahtumalle, on kyse kyberriskistä. (Evans, 2019, 5-6.)

Mukhopadhyay, Chatterjee, Saha, Mahanti & Sadhukhan (2013, 11) määrittävät kyberriskiksi ilkivaltaisiin sähköisiin tapahtumiin liittyvän riskin, josta seuraa liiketoiminnan häiriöitä ja rahallisia menetyksiä. Ögut, Raghunathan & Menon (2011, 497) taas näkevät kyberriskin synonyyminä tietoturvalle, sekä pitävät sitä altistumisella taloudellisille ja maineellisille menetyksille tieto- ja viestintätekniikkaa käyttäessä.

Eling & Schnell (2016, 12) näkevät kyberriskin kattavan kaikki tieto- ja viestintätekniikan käytöstä aiheutuvat riskit, jotka vaarantavat tietojen tai palveluiden luottamuksellisuuden, saatavuuden tai eheyden. Määritelmän mukaan kyberriskit ovat joko luonnonkatastrofien tai ihmisten aiheuttamia. Ihmisten aiheuttamat riskit voivat syntyä inhimillisistä virheistä, kyberrikollisuudesta, kybersodasta tai kyberterrorismista.

Curti, Gerlach, Kazinnik, Lee, & Mihov (2019, 4) katsovat kyberriskin yhdeksi operatiivisen riskin muodoista. He määrittävät sen sisäisten, ulkoisten tai kolmansien osapuolien aiheuttamien digitaalisten tapahtumien aiheuttamien menetysten riskiksi.

Kyberriski voi aiheutua tahallisesti tai tahattomasti. Kyberriskin tekijä voi olla rikollinen, mutta riski voi toteutua myös inhimillisen virheen johdosta. Kyberriskin kohteena voi olla yritys tai vaihtoehtoisesti joku yrityksen toimitusketjusta tai sidosryhmistä. Kyberriski voi siis kohdistua yritykseen suoraan tai kolmannen osapuolen kautta. Samoin kyberriskistä aiheutuneet vahingot voivat kohdistua yritykseen itseensä tai kolmansiin osapuoliin. (Colicchia, Creazza, & Menachof, 2019, 220; 234.) Kyberriskin vaikutukset voivat olla maineellisia, organisatorisia, oikeudellisia ja/tai taloudellisia (Evans, 2019, 16). Kyberriskin ominaisia piirteitä ovat keskinäiset riippuvuudet, mahdolliset äärimmäiset tapahtumat, suuri epävarmuus tietojen ja mallintamisen suhteen sekä muutosriski (Eling ym., 2016, 12).

2.1.2 Kyberriskin vakuutuskelpoisuus

Kyberriskin vakuutuskelpoisuutta voidaan pohtia Rantala & Kivisaaren (2020, 63-65) esittämän neljän vakuutuskelpoisuuden edellytyksen kautta: ennustettavuuden, stabiliteetin, riippumattomuuden ja riskin toteutumisen harvinaisuuden.

Riskin ennustettavuus tulisi olla määriteltävissä, sillä riskin toteutumisen todennäköisyyden kautta pystytään asettamaan sopivat vakuutusmaksut. Stabiliteetti vakuutuskelpoisuuden edellytyksenä taas viittaa siihen, muuttuuko riski ajan mukana ennalta-arvaamattomasti. Kyberriskin ennustettavuus on hankalaa sen teknologian mukana jatkuvasti muuttuvan luonteen johdosta (Munich Re, 2020b). Kyberriskeistä saatavilla olevaa dataa ei ole myöskään onnistuttu vielä hyödyntämään, eikä luotettavia pitkän aikavälin tilastoja ja yhteenvetoja ole vielä saatavilla (OECD, 2017).

Vakuutuskelpoisen riskin tulisi myös olla riippumaton edunsaajasta sekä toteutua harvoin. Edunsaaja ei siis saa itse tahallisesti aiheuttaa vahinkoa. Mikäli vakuutus korvaa kaiken riskistä aiheutuneen vahingon, saattaa tämä tehdä vakuutuksenottajan riskikäyttäytymisestä uhkarohkeampaa ja aiheuttaa moraalikatoa. Suurin osa toteutuneiden kyberriskien seurauksista ovat pieniä, mutta vahingot ovat pahimmillaan pitkäaikaisia ja laajoja. Kuten aikaisemmin todettiin, kyberriski ei ole täysin ennustettava, kuten eivät ole siitä seuraavat vahingotkaan.

Kuten Rantala ym. (2020. 63) toteavatkin, eivät edellä esitellyt edellytykset ole täysin ehdottomia. Kyberriski ei täytä kaikkia ehtoja alati muuttuvan luonteensa vuoksi, mutta kyberriski on kuitenkin vakuutuskelpoinen. Biener, Eling & Wirfs (2014) pitävät kyberriskin vakuutuskelpoisuuden suurimpina haasteina menetysten satunnaisuutta, tietojen epäsymmetriaa ja korvausrajojen asettamista. Lubin (2019) nostaa haasteeksi näiden lisäksi myös yleisesti seurattavien yhteisten periaatteiden puuttumisen ja epäselvät korvausehdot. Biener ym. (2014) ja Lubin (2019) kuitenkin näkevät markkinoiden kasvun myötä näiden haasteiden vaikutuksien pienentyvän, sillä vakuutuspoolien kasvaessa ja tilastoidun tiedon kerääntyessä tulevaisuudessa pystytään yhä paremmin määrittämään vakuutusmaksut kyberriskille.

2.2 Kyberriskien luokittelu ja yleisimpiä ilmenemismuotoja

2.2.1 Kyberriskien luokittelu

Myös kyberriskien luokittelusta löytyy useita eri määritelmiä. Yksinkertaistetuimmat luokittelut määrittelevät kyberriskin tahallisuuden ja tahattomuuden kautta. Luokittelua voi tarkentaa määrittelemällä riskin alkuperän, aiheuttajan, tarkoituksen sekä tapahtuman seuraukset ja Basel-viitekehyksen mukaisen tapahtumaluokituksen. (Curti ym., 2020, 5-8.) Toiset luokittelut määrittelevät kyberriskit toiminnan, hyökkäystyypin ja lähteen mukaan (Eling ym., 2016, 476). Kyberriskin muuttuvan luonteen takia yleiseksi tavaksi on tullut luokitella kyberriskiä juurikin riskin lähteiden avulla. Seuraavissa luokitteluissa lähteiden kautta on otettava huomioon, että kyberriski voi syntyä useamman lähteen yhdistelmästä.

Colicchia ym. (2019) luokittelevat kyberriskit riskien lähteiden kautta sisäisiin ja ulkoisiin, sekä vielä näiden luokkien sisällä tahallisiin ja tahattomiin. Sisäisiä riskin lähteitä ovat nykyiset ja entiset työntekijät, tekniset ongelmat ja sähkökatkot. Ulkoisia tekijöitä taas ovat sidosryhmät (mukaan lukien asiakkaat, kilpailijat ja yhteistyökumppanit), kyberhakkerit, tiedustelupalvelu ja muu vakoilutoiminta sekä muut valtiot. Ulkoisiin tekijöihin lasketaan myös teknisten ongelmien ja sähkökatkojen lisäksi luonnonkatastrofit. (Colicchia ym., 2019, 219-222.)

Yleisimpänä luokitteluna pidetään Cebula & Youngin (2010) kyberriskien luokittelua riskien lähteiden mukaan neljään luokkaan: inhimilliset tekijät, järjestelmien ja teknologian pettäminen, sisäisten prosessien heikkoudet ja ulkoiset tekijät. Inhimillisiin tekijöihin lukeutuvat sekä tahalliset että tahattomat ihmisen tekemät tai tekemättä jätetyt teot ja niiden seurauksena mahdollistuneet kyberriskit. Kyse voi olla inhimillisestä virheestä, huolimattomudesta tai rikollisissa aikeissa aiheutetusta petoksesta tai vandalismista. (Cebula ym., 2010, 2-4.) Ihminen voi olla hyökkääjä kyberiskun takana, mutta kyberisku voi vaihtoehtoisesti hyödyntää inhimillisiä virheitä ja niistä seuraavia mahdollisuuksia heikkoihin kohtiin iskemiseen. Inhimilliset virheet ovat päätekijä kyberhyökkäyksien takana (Munich Re, 2020b).

Järjestelmien ja teknologian pettämiseen liittyvissä kyberriskeissä on kyse fyysisiin laitteisiin, ohjelmistoihin ja järjestelmiin kohdistuvista kyberiskuista. Esimerkiksi vanhentuneet laitteistot, ylläpidon puute ja heikot turvallisuusasetukset aiheuttavat kyberriskejä. (Cebula ym., 2010, 4-5.) Sisäisten prosessien heikkoudet liittyvät yrityksen sisäisten prosessien suunnitteluun, toteutuksiin ja odotuksiin. Mikäli prosessien yksittäisissä tekijöissä on puutteita, saattaa koko ketju altistua kyberriskeille. Esimerkiksi puutteellinen tiedonkulku ja toiminnan seuraus ja kehitys voivat olla altistavia tekijöitä ja luoda heikkoja kohtia ketjuun. Organisaation sisäiset prosessit on oltava huolella suunniteltuja ja toteutettuja, kyberuhat huomioiden. (Cebula ym., 2010, 5-6.) Ulkoisia tekijöitä kyberriskin lähteinä voivat olla katastrofit, lainsäädännön muutokset, liiketoimintaympäristön muutokset ja riippuvuus sidosryhmistä. Yritys ei voi itse hallita tai ennustaa ulkoisia tapahtumia. (Cebula ym., 2010, 6-8.)

2.2.2 Yleisimpiä kyberriskin ilmenemismuotoja

Kolme yleisintä kyberriskin ilmenemismuotoa vuosina 2019 ja 2020 ovat olleet tietomurrot (data breaches), kiristäjävirukset (ransomware) ja sähköpostihuijaukset yrityksen nimissä (Business Email Compromise) (Munich Re, 2020a; Munich Re, 2021).

Kiristäjäviruksien (ransomware) käyttö kyberiskuissa on yleistynyt valtavasti, ja niitä käytetään yhä kohdennetuimmin tavoin. Hyökkääjä murtautuu uhrin järjestelmään ja asentaa sinne haittaohjelmia, jotka salaavat ja kryptaavat datan tai koko tietokonejärjestelmän estäen niiden käytön. Vastineeksi salauksen purkamisesta

hyökkääjä vaatii uhrilta lunnaita, useimmiten kryptovaluutan muodossa. Lunnaat määritellään vastaamaan uhrin taloudellista vahvuutta, ja voivat vaihdella tuhansien ja miljoonien eurojen välillä. Tanskalainen kuulokojeita valmistama yhtiö joutui kiristäjäviruksen kohteeksi ja kärsi jopa 80 miljoonan euron tappiot. Tappioihin luetaan mukaan myös liiketoiminnan keskeytymisestä, sen palauttamisesta, asiakkaiden hyvityskuluista ja IT-järjestelmien uudelleenpystyttämisestä ja laitteiden hankinnasta aiheutuneet kulut. Yhtiö odottaa saavansa kybervakuutuksesta noin 12 miljoonan euron korvaukset. (Munich Re, 2020a; Munich Re, 2021.)

Tietomurroissa on samankaltaisia ominaisuuksia kuin kiristäjäviruksissa. Tietomurrossa hyökkääjä on murtautunut uhrin järjestelmiin ja saanut haltuunsa yrityksen dataa, pahimmillaan arkaluontoisia yritys- tai asiakastietoja. Hyökkääjä saattaa vaatia lunnaita tietojen palautusta tai tuhoamista vastaan. Tietovuodoista aiheutuu suuria kuluja, joihin luetaan mukaan viranomaisten ja asianomaisten henkilöiden kontaktointi, tapauksen selvittäminen, toimenpiteet vahinkojen hillitsemiseksi ja tietojen palauttamiseksi sekä mahdolliset sakot ja korvaukset. (Munich Re, 2020a; Munich Re, 2021.)

Sähköpostihuijaukset väärennetyillä yrityssähköposteilla ovat kolmas yleisimmistä viime vuosien kyberriskeistä. Tässä petoksessa hyökkääjä joko hankkii pääsyn yrityksen sähköpostitilille tai luo samankaltaisen väärennetyn tilin. Näin hyökkääjä pystyy lähettämään sähköpostiviestin yrityksen työntekijöille tai asiakkaille. Mikäli työntekijät tai asiakkaat erehtyvät luulemaan viestiä aidoksi ja avaavat sen tai painavat viestin sisältämää linkkiä, pääsee hyökkääjä tunkeutumaan uhrin koneelle ja pahimmillaan saa haltuunsa yrityksen järjestelmät ja tiedostoja. Erityisesti PK-yritykset ovat tällaisten sähköpostihuijauksien kohteina. (Munich Re, 2020a; Munich Re, 2021.)

2.3 Kybervakuutuksen ominaisuudet, korvaukset ja rajoitukset

2.3.1 Kybervakuutus

Kybervakuutus on vakuutustuote, joka on suunniteltu kyberriskien vakuuttamiseen. Vakuutus auttaa kattamalla kyberriskistä johtuvia menetyksiä (Mukhopadhyay ym., 2013, 24). Kybervakuutustuotteita on ollut markkinoilla 90-luvulta asti. Vakuutustuotteelle syntyi kysyntää, kun kyberriskien toteutumisten yleistyessä niitä ei

ollut sisällytetty vakuutussopimusten korvausten piiriin. Tämän myötä erilliset kybervakuutustuotteet ovat vakiintuneet markkinoille. (Aon, 2017, 4.) Kybervakuutus on alkujaan tuotu markkinoille vastuuvakuutuksena. Vakuutussuoja on muuttunut ja laajentunut vuosien varrella, nykyään kybervakuutus sisältää yleisimmin keskeytys- ja vastuuvakuutuksen (Munich Re, 2020a). Vakuutuksenantajan velvollisuutena voidaankin katsoa olevan vakuutussuojan jatkuva kehittäminen vastaamaan muuttuvaa toimintaympäristöä ja kyberriskejä (Voelker 2015, 44).

Kybervakuutuksen kattavia peruselementtejä ovat suojaus liiketoiminnan keskeytymisiltä ja tietovarkauksilta (Munich Re, 2020a). Kybervakuutuksen vahinkojen korvattavuus ja rajaukset määritellään sen vakuutusehdoissa. Vakuutusmaksut, korvaukset ja omavastuuosuudet määritellään vakuutuksenantajan toimesta vastaamaan kunkin vakuutuksenottajan riskejä ja tarpeita. Vakuutusmaksu perustetaan yleisesti yrityksen liikevaihtoon, toimialaan ja vakuutettavaan summaan ja omavastuun suuruuteen. Kybervakuutukseen on usein liitettynä myös asiantuntijapalveluita, joita hyödynnetään riskikartoituksessa sekä kybervahingon sattuessa vahingon minimoimisessa ja tilanteen ennalleen palauttamisessa (Pohjola Vakuutus, 2020, 1; If, 2021).

2.3.2 Kybervakuutuksen korvaukset ja rajoitukset

Kukin vakuutuksenantaja saa itse määritellä tarjoamansa kybervakuutuksen vakuutusehdot, noudattaen maan lainsäädäntöä. Yleisesti voidaan sanoa, että useimmat kybervakuutukset korvaavat taloudellisia vahinkoja, jotka voivat syntyä esimerkiksi tietomurroista, kiristäjäviruksista, palvelunestohyökkäyksistä tai haittaohjelmista. Korvauksen piiriin kuuluvat myös kyberiskun syiden selvittely ja mahdolliset kulut tietojen ja ohjelmistojen palauttamisesta sekä korvauskustannuksista. Yleisesti kybervakuutus siis kattaa kuluja liiketoiminnan keskeytymisestä, tulojen menetyksestä, tietojen palauttamisesta ja korvauskustannuksista. (Lubin, 2019, 14; Pohjola Vakuutus, 2020, 1-2; If, 2021.) Maineen hallintaan liittyvät kulut kyberriskin realisoiduttua on myöskin mahdollista kattaa kybervakuutuksella, samoin kuin asiakkaiden tiedottaminen ja tukeminen tietovuodoissa. Kybervakuutuksen ehdoissa määritellään erikseen korvaukset itse vakuutuksenottajalle sekä toiselle osapuolelle. Kybervakuutus voi kattaa

myös kolmannelle osapuolelle aiheutuneesta vahingosta seuraavia kuluja (Lubin, 2019, 15).

Kybervakuutuksen ehdoissa rajataan yleisesti ulkopuolelle korvaukset liittyen henkilö- ja esinevahinkoihin, sakkoihin, sotaan, terrorismiin ja ydinvahinkoihin. Vakuutuksesta ei myöskään korvata vahinkoja, jotka ovat johtuneet tietoturvaohjeiden laiminlyönnistä tai välinpitämättömyydestä. (Lubin, 2019, 17; Pohjola Vakuutus, 2020, 1-2; If, 2021.) Kybervakuutuksen rajoituksiin ja korvaavuuteen voidaankin siis soveltaa vahingonkorvausoikeudellisia käsitteitä vahingon tuottamuksellisuudesta. Yleisesti voidaan todeta, että tuottamuksellisuuden aste vaikuttaa korvauksiin (OECD, 2020a, 24). Tapaukset käsitellään tapauskohtaisesti. Maailmanlaajuisesti eri tarjoajien kybervakuutusehtoja tarkasteltaessa suurinta hajontaa vakuutusehdoissa aiheuttavat petoksiin ja varkauksiin liittyvät rajoitukset (OECD, 2020a, 6).

2.4 Kybervakuutus osana riskienhallintaa IT-alalla

Tieto- ja viestintätekniikka-ala (Information and Communication Technology) yhdistää teollisuus- ja palvelualoja tietojen käsittelyn ja sähköisen viestinnän keinoin. IT-ala edistää tekniikan kehitystä sekä tuotannon ja tuottavuuden kasvua. (OECD, 2021.) Yritysten modernit toimitusketjut, jotka ovat riippuvaisia monista yrityksistä, ovat monimutkaisia. Yhä useampi toimitusketju kulkee usean toimialan välillä. Tämä nostaa riskienhallinnan vaatimuksia, sillä kyberiskut ovat todennäköisempiä ja toistuvampia monimutkaisissa ketjuissa. Suurin kysyntä kybervakuutuksille tulee toimialoilta, joihin kyberiskut vaikuttavat eniten: terveydenhuoltoalalta, teollisuusalalta sekä IT-, rahoitus ja palveluyrityksistä. (Munich Re, 2020a.)

Kyberriskit ovat siis suuri riski erityisesti IT-alan toimijoille, joiden liiketoiminta on siirtymässä entistä enemmän kohti palvelupohjaisia kokonaisuuksia. Yritykset siis tarjoavat laitteet ja ohjelmistot, niiden asennukset, opastuksen ja tuen käytössä sekä huollon ja päivitykset. Tämän seurauksena IT-alan toimijoiden vastuut ovat lisääntyneet, minkä vuoksi kybervakuuttaminen on nousemassa keskeiseen osaan IT-alan yritysten riskienhallintaa. Kybervakuutukset ovat tärkeä täydentävä menetelmä oman tietoturvasuojaustoimien ohelle selviytymään kyberiskujen vaikutuksista liiketoimintaan

(Mukhopadhyay ym., 2013, 11). Vakuuttaminen on yksi riskienhallinnan keino siirtää riski vakuutusyhtiön kannettavaksi (Rantala ym., 2020, 51).

Kyberriskit eivät ole toimialakohtaisia, joskin kyberriskien voidaan katsoa uhkaavan eniten yrityksiä, joiden toiminta painottuu internetiin ja/tai yritys käsittelee arkaluontoisia tietoja. Arkaluonteisiksi tiedoiksi luetaan esimerkiksi henkilö-, luottokortti- ja terveystiedot. Maailmanlaajuisesti vuosina 2013-2019 IT-alan osuus kybervakuutuskorvauksista oli toiseksi korkein terveydenhuoltoalan kattaessa suurimman osuuden. (Statista Research Department, 2021.) Oli toimiala mikä tahansa, verkkoon yhteydessä olevat yritykset ovat altistuneita kyberriskeille. Riskille altistuminen ei katso yrityksen kokoa, eivätkä PK-yritykset voi ajatella olevansa suojassa. Suuryritykset suojaavat toimintaansa isompien resurssien turvin, joten PK-yritykset voivat olla helpompia ja nopeampia kyberiskujen kohteita. Myös PK-yritysten on syytä panostaa kyberturvallisuuteensa.

Tulee kuitenkin muistaa, ettei kybervakuutus itsessään poista yrityksen tarvetta huolellisiin tietoturvakäytäntöihin. Vakuuttamisen lisäksi yritysten tulisi lähestyä kyberriskienhallintaa myös proaktiivisesti ja pyrkiä torjumaan kyberriskejä kiinnittämällä huomiota verkkoturvallisuuteen, kriittisten järjestelmien ja tietojen varmuuskopiointiin, haittaohjelmien torjuntatyökaluihin, identiteetin ja käyttöoikeuksien hallintaan sekä tietoturvakonsultointiin. Tapahtumien torjunta nähdään yhtenä tärkeimpänä tekijänä kyberriskien hallinnassa. (Low, 2017, 20; Munich Re, 2021.) Yritysten tulisikin pyrkiä suhtautumaan kyberriskeihin ennemmin ennakoivasti kuin reaktiivisesti (Evans, 2019, 9; 94). Erityisesti inhimillisten virheiden ollessa suurin syy kyberriskien aiheuttajana (Munich Re, 2020b), on yrityksien hyvä kouluttaa ja sitouttaa henkilöstöä tietoturva-asioissa.

Mikäli kyberriski realisoituu, on toimintasuunnitelman oltava selvä vahinkojen minimoimiseksi ja tilanteen palauttamiseksi ennalleen mahdollisimman nopeasti (Munich Re, 2021). Kyberriskienhallinnan ei siis voida katsoa enää kuuluvan yrityksen IT-osaston vastuulle, vaan se vaatii kaikkien osastojen panosta (Eling ym., 2016, 479-480). Yrityksen on otettava huomioon myös sidosryhmänsä ja niistä mahdollisesti aiheutuvat heikkoudet. Kyberriskienhallinnan on oltava jatkuvasti kehittyvää, kuten kyberriskikin on ominaisuuksiltaan alati muuttuva.

3 KYBERVAKUUTUKSEN HANKINTA PROSESSINA

3.1 Kybervakuutuksen hankinta ja vakuutuksen elinkaarimalli

Muodostaakseen käsityksen kybervakuutuksen hankinnan vaiheista yrityksen näkökulmasta, on tarkasteltava yleistä mallia vakuutuksen elinkaaresta. Vakuutuksen elinkaari muodostuu neljästä osasta: tarve, hankintavaihe, omistusvaihe ja luopuminen (Ives & Mason, 1990, 59). Seuraavaksi käsitellään näitä vaiheita kybervakuutuksen hankinnassa vakuutuksenottajan, yrityksen, näkökulmasta. Tutkielman tutkimuskysymykset vaativat tarkempaa syventymistä kahteen ensimmäiseen osaan, tarpeeseen ja hankintavaiheeseen.

Tarvevaiheessa vakuutuksenottaja määrittää ja tarkentaa, minkälaista palvelua tarvitsee (Ahonen, Puustinen & Salonen, 2007, 108–109). Yrityksen on siis kartoitettava nykytilanteensa ja siihen liittyvät mahdolliset riskit sekä mietittävä myös tulevaisuuden aiheuttamia muutoksia. Yrityksen on huomioitava omat tarpeensa, sidosryhmien tarpeet sekä toimialan riskit kybervakuutustarpeen kartoittamisessa. Yritysten on huomioitava myös asiakassopimusten kautta tulevat mahdolliset vastuut kybervakuuttamiselle. Kun tarpeet kybervakuutukselle on kartoitettu, on seuraavana vuorossa vaihtoehtojen kartoitus ja vertailu. Hankintavaiheessa haetaan tietoa ja vertaillaan eri yhtiöiltä saatuja tarjouksia. (Ahonen ym., 2007, 108–109.) Hankintavaiheeseen kuuluu myös neuvottelu vakuutusehdoista ja -maksuista.

Vakuutuksenantaja kartoittaa asiakkaan tarpeen ja sen perusteella tarjoaa sopivaa tuotetta. Yritys on ennen vakuutuksenantajan tekemää kartoitusta jo itse tehnyt oman tarvekartoituksensa, mutta vakuutusyhtiöllä on myös velvollisuus selvittää asiakkaan vaatimukset ja tarpeet. Vakuutuksenantajan on esitettävä vakuutustuotteen tiedot ja ehdot ymmärrettävästi ja puolueettomasti vakuutuksenottajalle (Direktiivi, 2016/97/EU). Yritys vertailee saatujen tarjousten sisältöä ja vakuutusehtoja. Vakuutusyhtiöiden toimintatavat eroavat vakuutusmeklareiden toimintatavoista vakuutusta hankkiessa. Tarkemmin näiden kahden tekijän eroihin tutustutaan luvussa 3.2.

Elinkaarimallin mukaisesti kybervakuutuksen hankintavaihe-osio päättyy, kun sopiva kybervakuutus valitaan ja sopimus laaditaan. Kybervakuutuksen omistusvaiheessa yrityksen tulee päivittää vakuutusturvaa, mikäli heidän toimintaansa tulee muutoksia. Yrityksen on myös noudatettava vakuutusehtojen mukaisia velvoitteita tietoturvallisuuden ylläpidosta. Mikäli kybervahinkoja sattuu, saattavat vakuutusmaksut nousta sen seurauksena. Muuten kybervakuutus on voimassa vakuutussopimuksen mukaisesti.

3.2 Kybervakuutuksen tarjoajat

Suomessa kybervakuutusta tarjoavia vakuutusyhtiöitä ovat Pohjola Vakuutus, If, Fennia, LähiTapiola, Turva ja AIG (tilanne maaliskuussa 2021). Suomessa toimivista vakuutusmeklareista isoimmat kybervakuutuksien välittäjät ovat Aon, Marsh ja Howden. Suomessa yritys voi hankkia kybervakuutuksen joko suoraan vakuutusyhtiöltä tai riippumattoman vakuutusmeklariyhtiön kautta vakuutusyhtiöltä. Erityisesti keskisuuret ja suuret yritykset käyttävät vakuutusmeklareita, sillä yritysvakuuttaminen on usein monimutkaista ja vaatii asiantuntijan käyttöä. Vuonna 2019 Suomen vakuutusmaksutuloista vakuutusmeklarivälitteisten vakuutusmaksutulojen osuus oli 6,9% (Finanssivalvonta, 2019). Laki vakuutusten tarjoamisesta (234/2018) koskee niin vakuutusyhtiöitä kuin vakuutusmeklareita. Laki pyrkii yhdentämään vakuutusten tarjontaa koskevia säännöksiä jakelukanavasta riippumatta.

Vakuutusyhtiöt tarjoavat yritysasiakkailleen valmiita kybervakuutuspaketteja. Osa yhtiöistä myös räätälöi suuryrityksille kustomoituja kybervakuutuksia tai tarjoaa valmiiden ja räätälöityjen pakettien yhdistelmiä. Usein kybervakuutuksen pohjana on kuitenkin valmispaketti. Vakuutusmeklariyhtiö edustaa asiakastaan vakuutusasioissa vakuutusyhtiöihin päin. Vakuutusmeklari on riippumaton vakuutuksenantajista ja ajaa puolueettomasti asiakkaansa etuja. Vakuutusmeklariyhtiöt tarjoavat erilaajuista palvelua vakuutuksen ottamisessa, parhaimmillaan he hoitavat kaiken riskikartoituksesta vakuutuksien kilpailutuksen kautta korvausten hakemiseen.

Käytännössä vakuutusyhtiöiden ja vakuutusmeklareiden tavoite on sama: arvioida asiakkaan riskit ja sen mukaan löytää valikoimasta sopivin vakuutus. Vakuutusyhtiöt tarjoavat tuotteita vain omasta valikoimastaan, kun taas vakuutusmeklarit pystyvät

tarjoamaan useampia ratkaisuja eri vakuutusyhtiöiltä. Molemmat kartoittavat asiakkaan tarpeita ja riskejä, mutta eri yhtiöiden toiminta seuraa eri kaavoja. Arvioitavia tekijöitä voivat olla esimerkiksi järjestelmiin, tietokantoihin ja organisaation toimialaan liittyvät uhat, organisaation suojaustoimet, miten paljon arkaluontoisia tietoja on sekä mitä ja miten on ulkoistettu (Lubin, 2019, 22).

Huomioitavaa kybervakuutuksen hankinnassa on se, ettei kybervakuutus ole lakisääteinen vakuutus. Näin ollen vakuutusyhtiö voi kieltäytyä ottamasta riskejä kantaakseen. Vakuutussopimuslaki ei edellytä vakuutusyhtiötä myöntämään vapaaehtoista vakuutusta. Vakuutusyhtiöillä voi myös olla edellytyksiä vakuutuksen myöntämiselle, kuten tietoturvan tason varmistaminen riittävällä virustorjunnalla, palomuurilla ja ajantasaisilla ohjelmistoilla.

Kuten tutkielmassa on aikaisemmin tullut esiin, kyberriskin luokittelusta tai vakuuttamisesta ei ole vielä olemassa yleisesti seurattavia periaatteita. Näin ollen kybervakuutuksenantajat ja -välittäjät pystyvät pitkälti itse valitsemaan mitä reunaehtoja noudattavat ja käyttävät arvioidessaan vakuutuksenottajan vakuutustarpeita. Tämän seurauksena yhtiöt kysyvät asiakkailta osittain eri kysymyksiä kerätessään tietoa osana riskienkartoitusta ja prosessit saattavat edetä toisistaan mahdollisesti eroavilla tavoilla. Suurinta vaihtelua eri vakuutustentarjoajien esitietokysymyksissä aiheuttavat kysymykset liittyen turvallisuusstandardien noudattamiseen yrityksessä (Lubin, 2019, 19-21). Yhtiöiden tarjoamat kybervakuutukset eroavat vakuutusehdoiltaan, joten niitä ei voi vertailla keskenään varauksetta.

3.2.1 Kybervakuutus vakuutusyhtiöltä

Kybervakuutuksen hankinta voi edetä eri tavoin vakuutusyhtiöstä riippuen. Yleisesti kybervakuutuksen hankinta vakuutusyhtiöltä alkaa olemalla yhteydessä vakuutusyhtiöön jonkun kanavan kautta. Vakuutusyhtiön edustaja aloittaa prosessin pyytämällä tietoja yritykseltä. Tiedon lähteenä voivat toimia kirjalliset hakemukset, saatavilla olevan aineiston analyysit ja tapaamiset. Vakuutusyhtiö pyrkii näin arvioimaan riskejä kokonaisvaltaisesti. Vakuutusyhtiöt saattavat hyödyntää kyberriskien arvioimisessa kolmannen osapuolen asiantuntijapalveluita, jolloin kyberriskien arvioiminen on ulkoistettu tälle tekijälle.

Vakuutusyhtiö esittää asiakkaalle ehdotuksen tietojen perusteella. Ehdotus käydään läpi ja mikäli tiedot täsmäävät eikä niissä ole muututtavaa, tulee tarjous asiakkaalle mahdolliseksi hyväksyä. Mikäli asiakas haluaa pyytää tarjouksia useammalta vakuutusyhtiöltä, joutuu hän käymään tarjousprosessin läpi kaikkien kanssa erikseen ja tekemään itse tarjousten vertailun. Yrityksen on syvennyttävä tarjouksiin ja löydettävä itselleen sopivin valinta. Tämä vaatii asiantuntemusta. Vakuutusyhtiöltä kybervakuutusta ottaessa on myös huomioitava keskittämisedut. Mikäli yritys keskittää vakuutuksensa samalle yhtiölle, tarjoavat yhtiöt usein huomattaviakin alennuksia vakuutusmaksuihin. Vakuutusmaksuja jopa tärkeämpää on kuitenkin tutustua vakuutusehtoihin ja etsiä parasta sopivuutta yrityksen tarpeisiin, eikä katsoa vain vakuutuksen hintaa.

Kybervakuutusta valitessa tulee myös pohtia asiaa asiakkuuden muodostumisen kannalta. Eri asiakkaiden asiakkuudet muodostuvat toisistaan poikkeavasti: ne syntyvät, kehittyvät ja päättyvät eri tavoin, joten eri asiakkuuksien tukemiseen on käytettävä erilaisia välineitä. Finanssialalla panostetaan pitkiin asiakkuuksiin, sillä ne ovat yhtiöille arvokkaimpia ja kannattavimpia. (Ylikoski, Järvinen, & Rosti, 2006, 81-82.) Tällä on vaikutuksena myös kybervakuutusta hankkiessa. Yritys tekee päätöksen siitä, keneltä lähtevät hakemaan tarjouksia. Jos yritys on jo keskittänyt asiakkuutensa yhdelle vakuutusyhtiölle ja on tyytyväinen palveluun, saattaa tarjousten pyyntö muilta jäädä tekemättä. Toisaalta jos yritys etsii ensisijaisesti palvelua, vaivattomuutta ja nopeutta, saattaa tämä vaikuttaa suoraan kokonaisvaltaista palvelua tarjoavan meklariyhtiön valintaan.

3.2.2 Kybervakuutus vakuutusmeklariyhtiön välittämänä

Kybervakuutuksen hankinta vakuutusmeklariyhtiön kautta alkaa, kun asiakasyritys tekee toimeksiantosopimuksen vakuutusmeklarille. Meklari käy läpi asiakkaan nykyisen vakuutusturvan ja kartoittaa riskit vakuutusta varten. Vakuutusmeklari tekee näiden sekä asiakkaan tarpeiden pohjalta ehdotuksen ja käy sen sisällön läpi asiakkaan kanssa. Meklari huolehtii, että vakuutusturva vastaa yrityksen tarpeita, eikä kustannuksia menisi ylivakuuttamiseen tai muuhun päällekkäiseen vakuuttamiseen. Mahdollisten parannuksien jälkeen vakuutusmeklari valmistaa tarjouspyynnön, jonka yritys hyväksyy. Meklari lähettää tarjouspyynnön vakuutusyhtiöille. (Määttä ym., 2005, 120-125.)

Tarjousajan kuluttua umpeen meklari laatii vertailun saatujen tarjousten sisällöstä. Saadut tarjoukset saattavat olla laadittu vakuutusyhtiön ehdoilla, vakuutusmeklarin esittämillä ehdoilla tai niiden yhdistelmällä. Jos tarjouksiin ei olla tyytyväisiä tai niihin halutaan tarkennusta, jatkaa meklari neuvottelua. Meklari esittää lopulliset tarjoukset asiakkaalle esitellen puolueettomasti niiden hyvät ja huonot puolet ja suosittelee omasta mielestä parasta vaihtoehtoa. Asiakas tekee lopullisen valinnan. (Määttä ym., 2005, 125-126). Vakuutusmeklarit etsivät tarvittaessa parhaita vakuutuksia myös ulkomaalaisilta vakuutusyhtiöistä, tai hajauttavat vakuutukset eri vakuutusyhtiöihin (Savolainen, 2021).

Vakuutusmeklarit neuvottelevat vakuutusyhtiöiden kanssa tarjouksista. Vakuutusmeklareiden pitkäaikaiset suhteet ja hyvät keskusteluyhteydet vakuutusyhtiöihin mahdollistavat meklareille paremman neuvotteluaseman vakuutusehdoista keskusteltaessa (Savolainen, 2021). Jotkut vakuutusyhtiöt tarjoavat yritysasiakkaille vakuutuksia vain meklareiden välityksellä. Vakuutusyhtiöt usein tarjoavat meklareille edullisempia vakuutusmaksuja, sillä meklarit tekevät lähes kaiken vakuutusmyyjän työn valmiiksi vakuutusyhtiölle (Savolainen, 2021). Usein vakuutusmeklareiden käyttö on kannattavaa, jos yritys hakee vakuutusratkaisua monimutkaisiin riskeihin ja etsii tarpeisiinsa kustomoitua tuotetta. Mikäli vakuutusmeklarin lopullisissa tarjouksissa asiakkaalle on vakuutusyhtiöiden valmispaketteja, ei vakuutusmeklarin palkkion maksamisen jälkeen yritys ole juuri saanut hyötyä meklarin käytöstä. Näin ollen tyypillisesti keskisuuret ja suuret yritykset käyttävät vakuutusmeklareita vakuutuksenhankinnassa.

Kybervakuutustarjouksia hankkiessa myös yrityksen neuvotteluasemalla on merkitystä. Suuren yrityksen neuvotteluasema voi olla parempi kuin pienen, sillä isot yritykset ovat arvokkaita asiakkaita niin vakuutusyhtiöille kuin vakuutusmeklareille. Tämän takia suuri yritys pystyy mahdollisesti neuvottelemaan itselleen muutoksia kybervakuutusehtoihin. Pienelle yritykselle taas tarjotaan ennemmin valmiita kybervakuutuspaketteja, joiden ehdoissa ei juuri ole neuvotteluvaraa. Vakuutusmeklarin käyttö mahdollistaa vakuutussopimusten vakioehtojen muokkauksen tai muut poikkeusjärjestelyt, sillä vakuutusmeklarilla on parempi neuvotteluasema vakuutusyhtiöihin verrattuna yritykseen (Savolainen, 2021).

4 KYBERVAKUUTUKSEN HANKINTA JA SIIHEN VAIKUTTANEET TEKIJÄT

4.1 Aineiston kuvaus ja käsittely

Tapaustutkimuksessa on kyse ilmiön selittämisestä ja jäsentelystä (Eriksson ym., 2005, 33). Tämän tutkielman tapaustutkimuksen kohteena on yrityksen kybervakuutuksen hankinta. Aineisto on kerätty haastattelemalla yritystä, joka on hankkinut kybervakuutuksen loppuvuodesta 2020. Yritys ja haastateltava esiintyvät anonyymisti tässä tutkielmassa. Yritys on tässä tutkielmassa toissijainen, sillä tutkielma pyrkii selittämään ja kuvailemaan kybervakuutuksen hankintaa. Koska yritys toimii IT-alalla, on analysoinnissa ja johtopäätösten tekemisessä otettava huomioon toimialan vaikutukset.

Haastattelutyypiksi valittiin puolistrukturoitu teemahaastattelu. Haastateltavaksi valittiin keskeisin kyberriskeistä ja niiden hallinnasta vastaava henkilö. Haastateltavalla on yli 25 vuoden kokemus erilaisista vastuuasemista IT-alalla ja liiketoiminnan kehityksessä. Haastateltavalle lähetettiin haastatterlurunko (ks. Liite 1) etukäteen ennen haastattelua. Haastattelu suoritettiin Microsoft Teamsin välityksellä ja äänitettiin haastateltavan suostumuksella. Keskustelut litteroitiin heti haastattelun jälkeen. Valmis teksti haastattelusta on lähetetty haastateltavan luettavaksi, jotta on varmistettu, että häntä on ymmärretty oikein.

Aineiston käsittely tehdään teemoittain. Teemat on rakennettu viitekehyksessä (kuvio 1) esiteltyjen vakuutuksen valinnan vaiheiden mukaisesti. Haastatteluja on analysoitu teorialähtöisen sisällönanalyysin keinoin ja muodostettu sen kautta tiivistetyt kuvaukset kybervakuutuksen hankinnan eri vaiheista sekä kuvailtu ja tunnistettu vaiheisiin liittyviä tekijöitä. Teoriapohjainen sisällönanalyysi peilaa tutkimusaineistoa tutkimukseen valittuun teoriapohjaan (Sarajärvi & Tuomi, 2018, 105). Tutkimusaineisto on sisällönanalyysille tyypillisesti pelkistetty ja ryhmitelty (Sarajärvi ym., 2018, 105-106), ja tämän avulla on tunnistettu keskeisimpiä tekijöitä vakuutuksenhankinnan vaiheissa ja muodostettu ymmärrys yrityksen kybervakuutuksen hankinnasta.

4.2 Tarpeet ja taustat kybervakuutuksen hankinnassa

Haastateltava kertoo, ettei heillä ole ollut kybervakuutusta ennen vuotta 2020. Yrityksessä oltiin tietoisia riskeistä, mutta niitä oli tunnistettu ja pyritty hajauttamaan, jolloin vakuutusta ei oltu katsottu tarpeelliseksi. Haastateltava toteaa yrityksen olleen tietoisia kyberriskeistä, mutta ottaneensa tietoisen riskin. Yritys oli siis ollut tietoinen kyberriskeistä ja jo osaltaan pyrkinyt estämään niitä, mutta varsinaisen kybervakuutuksen ottamisen tarve nousi ensisijaisesti uudesta solmitusta asiakassopimuksesta. Haastateltava kertoo uuden asiakassopimuksen sopimusehdoissa olleen vaatimuksena kybervakuutus kattamaan tiettyjä sopimuksen vastuita.

Toisena tekijänä kybervakuutuksen tarpeen kasvussa on yrityksen toiminnan siirtyminen yhä enemmän uusiin pilviteknologioihin, joiden seurauksena riskit ja vastuut muuttuvat. Pilviratkaisut voivat sisältää monien eri toimijoiden ratkaisuja. Kyberhyökkäyksissä voi olla haastavaa osoittaa vastuiden jakautuminen.

``Uusiin teknologioihin siirtymisen kautta meillä on laajemmat vastuut asiakkaiden liiketoiminnasta.´´ -Haastateltava

Yrityksen kybervakuutussopimuksen kattavuuden kriteerit oli suoraan esitetty asiakassopimuksessa. Haastateltava kertoo, etteivät he tämän takia käyttäneet ulkopuolista arvioijaa, mutta käyttivät asiakassopimuksen kriteerien ohella omia riskiarviointejaan uuteen teknologiaan siirtymisestä. Muita kriteerejä haastateltava kertoo olleen laajasti sanottuna vakuutuksen kattavuus ja hinta.

4.3 Vaihtoehtojen kartoitus

Yrityksen tarve kybervakuutukselle tuli ajankohtaiseksi uuden asiakassopimuksen myötä. Haastateltava kertoo, että yrityksen oli saatava kybervakuutus voimaan mahdollisimman nopeasti. Vakuutusyhtiöitä ja -meklareita kontaktoitiin ensisijaisesti yritykselle tuttujen yhteyshenkilöiden kautta tai muulloin verkkosivujen lomakkeiden kautta. Vaihtoehtojen kartoittaminen osoittautui kuitenkin vaikeaksi. Haastateltava toteaa, että kybervakuutuksesta oli vaikea saada tietoa ja tarjouksia.

``Tuntuu, että tämä [kybervakuutus] on kaikille ei-niin-selkeä alue.´´- Haastateltava

Haastateltava huomauttaa kuitenkin, että tähän saattoi osaltaan vaikuttaa kokemukset erään vakuutusyhtiön kanssa. Vakuutusyhtiön puolelta yhteyshenkilö vaihtui kesken kybervakuutuksen alustavien kartoitusten. Uusi yhteyshenkilö oli tietämätön kybervakuutuksen yleisistä ehdoista, ja vastasi yhteydenottoihin hitaasti ja ympäripyöreästi. Haastateltava koki vaikeaksi saada selkeitä sitovia vastauksia tiettyihin vakuutusturvaa koskeviin yksityiskohtiin. Hän kertoi pohtineensa, ymmärsivätkö he terminologian eri tavoin vai oliko yhteyshenkilö varovainen sanomisissaan tarkoituksella. Voi myös olla mahdollista, ettei yhteyshenkilö tuntenut tuotetta riittävästi.

Hyvin pian vaihtoehtojen kartoittamisen aloittamisen jälkeen yritykselle kävi selväksi, että vakuutusyhtiöt tuntuivat toimivan tuote edellä ja vakuutusmeklarit tarve edellä. Valmiin kybervakuutuspaketin ottaminen on nopeampaa ja selkeämpää, kun taas meklarin kanssa prosessi etenee hitaammin, mutta on selkeästi vuorovaikutteisempaa ja vaatii yritykseltä enemmän panostusta. Haastateltava kertoo, että meklariyhtiöille piti osata avata tarve tarkasti, heidän kokemuksensa mukaan tarkemmin kuin vakuutusyhtiölle. Yrityksellä on asiantuntemusta alalta ja ehdot heidän haluamalleen kybervakuutukselle olivat selvät, mutta silti meklariyhtiölle tarvittavan tiedon toimittaminen koettiin työläänä ja aikaa vievänä.

4.4 Vakuutuksenantajien ja -tarjouksien vertailu

Yrityksen yksi vaatimus oli saada kybervakuutus hankittua mahdollisimman nopeasti. Tämän takia yritys lähti ensisijaisesti kartoittamaan valmiita pakettiratkaisuja tarjoavia vakuutusyhtiöitä. Se oli nopealla aikajäänteellä ainoa vaihtoehto. Päätökseen valita valmispaketti vaikutti myös se, että yritys halusi saada aikaa käydäkseen rauhassa meklarin kanssa neuvottelut pitkäaikaisemmasta kybervakuutusratkaisusta.

Vaihtoehtojen vertailu vakuutusyhtiöiltä osoittautui kuitenkin vaikeaksi yrityksen toimialan takia. Yritys tekee terveydenhuollon ohjelmistoja, jotka käsittelevät arkaluontoisiksi luokiteltuja tietoja. Tämä karsii vakuutuksentarjoajia, joista osa ilmoitti suoraan ensimmäisessä yhteydenotossa, etteivät tarjoa kybervakuutusta näin korkeariskiselle toimialalle. Haastateltava toteaakin, että vakuutustarjouksia oli vaikea

saada. Hän kertoo esimerkin, miten eräs vakuutusyhtiö oli tarjonnut yritykselle suoraan valmispakettia, jonka korvausmäärät olivat huomattavasti pienemmät, mitä yritys tarvitsi. Yrityksen pyytäessä tarjousta haluamallaan korvaussummalla tarjouspyyntöön ei edes vastattu. Kybervakuutustarjouksia oli vaikea vertailla, sillä vähäisetkin saadut tarjoukset oli laadittu eri tavoin ja niiden vakuutusehdot vaihtelivat. Tarjouksia oli siis vaikea laittaa järjestykseen.

Yritys päätyi vaihtoehtojen kartoituksen ja vertailun jälkeen valitsemaan itse suoraan vakuutusyhtiöltä valmispaketin. Näin toimien he pystyivät täyttämään uuden asiakassopimuksen edellytykset, ja yritys sai tarvitsemaansa lisäaikaa kattavamman ja perusteellisemman kybervakuutuksen valintaan. Haastateltava kertoo, että meklariyritys tuntui kartoittavan vakuutustarvetta paremmin ja tarjoavan useampia mahdollisuuksia vakuutukselle. He eivät aio kilpailuttaa meklareita vaan valita tutun tekijän alalta, jonka kanssa ovat aikaisemminkin tehneet yhteistyötä.

4.5 Neuvottelu ja valinta

Kybervakuutuksen valintaan vaikuttivat aikajänne, tarjousten vähyys ja päätös varata kunnolla aikaa meklarin kanssa lopullisen vaihtoehdon laatimiseen. Haastateltava kertoo, että saivat lopulta vain yhdeltä vakuutusyhtiöltä suurin piirtein tarpeitaan vastaavan vakuutustarjouksen. Neuvottelut käytiin etäyhteyksin. Kyseessä oli vakuutusyhtiö, jonne yritys on jo pidemmän aikaa keskittänyt asiakkuutensa. Haastateltava kertoo, ettei kybervakuutuksen saaminen kyseiseltä yhtiöltä kuitenkaan ollut itsestäänselvyys.

``Vakuutusyhtiön kanssa piti kyllä neuvotella ja kriteereissä joustamaan, jotta ylipäätään saimme kybervakuutuksen. Emme olisi saaneet sitä ilman kokonaisasiakkuutemme vaikutusta.´´- Haastateltava

Kun ottaa pakettivakuutuksen, ei siitä pysty juurikaan neuvottelemaan vakuutusyhtiön kanssa. Haastateltava kertoo heidän pystyneen neuvottelemaan vain vakuutuksen irtisanomisehdoista. Kyberriskin luonteen huomioiden voidaan pitää luontevana sitä, etteivät vakuutusyhtiöt ole halukkaita vakuuttamaan pelkästään kyberriskejä. Kuten tämänkin yrityksen tapauksessa, kybervakuutusta ei olisi myönnetty ilman kokonaisasiakkuutta. Yritys aloittaa meklarin kanssa neuvottelut tämän vakuutuskauden

aikana, jotta saavat kriteerejään paremmin vastaavan pitkäaikaisemman kybervakuutusratkaisun. Meklarin tehtäväksi voidaankin etsiä asiakkaan tarpeisiin sopivaa ratkaisua laajasta vakuutuksenantajien valikoimasta. Haastateltava arvelee yrityksen nykyisten kybervakuutuksen hankintakokemuksien perusteella, ettei meklarin ehdottamat vakuutusratkaisut tule olemaan kotimaisilta vakuutuksentarjoajilta. Suomen kybervakuutusmarkkinat ovat pienet Eurooppaan markkinoihin verrattuna, ja edelleen Euroopan kybervakuutusmarkkinat ovat kehittymättömät Yhdysvaltojen markkinoihin verrattuna (Munich Re, 2020a).

4.6 Yhteenveto haastatteluista

Yritys kokee kybervakuutuskentän epämääräiseksi. Kyberriskit muuttuvat koko ajan, joten yritykselle on haastavaa pitkäaikaisissa asiakassopimuksissa määritellä sopimusehdot vastaamaan nykypäivän sekä tulevaisuuden riskejä. Kyberriskien hallinta on haastavaa asiakassopimuksissa ja asiakassopimusten korvausvastuissa, sillä tulevien vuosien mahdollisia uusia riskejä tulkitaan voimassaolevan sopimuksen mukaisesti.

Kybervakuutuksen hankinnasta tekee epämääräisen myös suhteiden ja verkostojen vaikutus vakuutusprosessiin: vakuutusyhtiöt myöntävät kybervakuutuksen kokonaisasiakkuuden perusteella, jota ilman vakuutusta ei myönnettäisi. Myöskään vakuutusmeklareita ei välttämättä kilpailuteta, mikäli yritys on jo luonut suhteita tiettyyn toimijaan. Kilpailuttamatta jättäminen saattaa johtaa paremman vaihtoehdon huomioitta jättämiseen, mutta toisaalta suhteiden hyödyntäminen vakuutusmaailmassa vaikuttaa olevan tavanomaista. Kärjistettynä kybervakuutuksen ottaminen ja lopulliseen valintaan päätyminen voidaan nähdä jossain määrin sattumusten sarjan tuloksena.

Valmiita pakettiratkaisuja tarjoavilla vakuutusyhtiöillä ei ole valmiutta räätälöidä asiakaskohtaisesti sopimuksia. Valmiiden pakettiratkaisujen korvaussummat ovat lähtökohtaisesti alhaisia. Korkeamman riskin toimintaa ei olla edes halukkaita vakuuttamaan. Vakuutusyhtiöt eivät ole halukkaita vakuuttamaan korkeariskistä toimintaa kyberriskeiltä, joiden ennustettavuutta ja vahinkojen laajuutta on hankala arvioida.

Yritys oli tyytyväinen lopputulokseen vakuutuksen kanssa. Haastateltava kertoo, että he kokivat nopean pakettivakuutuksen olleen siihen tilanteeseen oikea ratkaisu. Myöhemmin meklarin kanssa käytävien neuvottelujen tuloksena he odottavat saavansa kohdennetumpaa vakuutusturvaa oletusarvoisesti kustannustehokkaammin. Vakuutusturvaa tullaan kartoittamaan myös ulkomaisilta vakuutusyhtiöiltä, jotka ovat toimineet Suomen kybervakuutusmarkkinoita suuremmilla markkinoilla ja omaavat enemmän kokemusta alalta. Yrityksellä ei itsellään olisi resursseja kartoittaa ulkomaisia vakuutuksentarjoajia ja käydä heidän kanssaan neuvotteluja. Tulee mielenkiintoiseksi nähdä, minkälaisia kybervakuutustarjouksia vakuutusmeklari saa yritykselle neuvoteltua. On mahdollista, että paras ratkaisu saataisiin etsimällä sopivaa vakuutusta kokonaisasiakkuudelle kybervakuutustarpeet huomioiden. Tämä oletettavasti vaikuttaa vakuutusyhtiöiden halukkuuteen tarjota ratkaisuja, sillä selvästi pelkkien kyberriskien vakuuttamiseen liittyy haluttomuutta vakuutusyhtiöiden puolelta. Yritys kokee kybervakuutuksen turvan tarpeelliseksi.

``Ylipäätään koemme kybervakuutuksen tarpeelliseksi, riskit on olemassa ja pahimmillaan vaikutukset ovat katastrofaalisia yrityksellemme ja voivat vaarantaa koko liiketoiminnan. Jos tällainen tilanne toteutuu, kyllä vakuutus helpottaa selviytymistä tilanteesta.´´- Haastateltava

Yritys on kokenut toimialallaan toimittajan vastuiden ja riskien tietoturvan ja tietosuojan osalta kasvaneen merkittävästi ja kokevat omassa tilanteessaan kybervakuutuksen ottamisen itsestäänselvyytenä.

5 JOHTOPÄÄTÖKSET

5.1 Johtopäätökset ja tutkimuskysymyksiin vastaaminen

Tämä tutkielma etsi vastauksia kahteen päätutkimuskysymykseen: *Mitkä tekijät vaikuttavat yrityksen kriteereihin kybervakuutukselle* sekä *Mitkä tekijät vaikuttavat kybervakuutuksen kartoitus-, vertailu- ja neuvotteluvaiheisiin ja ohjaavat yrityksen valintaa.* Tutkielman tapaustutkimus oli IT-alalla toimivan PK-yrityksen kybervakuutuksen hankinta.

Tutkielman teoriapohjan ja empiirisen tapaustutkimuksen pohjalta voidaan todeta, että kybervakuutuksen ottaminen on yrityksille usein hankalaa ja monimutkaista. Kybervakuutuksia ja niihin liittyvää terminologiaa olisi yksinkertaistettava ja selvennettävä. Kyberriski on käsitteenä niin laaja, että sen piiriin voi kuulua miltei mitä vain nykyajan digitaalisessa maailmassa.

Mitkä tekijät vaikuttavat yrityksen kriteereihin kybervakuutukselle? Yrityksen on huomioitava tarpeitaan kartoittaessa omat yrityksen sisäiset vaatimuksensa sekä sidosryhmien asettamat vaatimukset. Yrityksen toimiala vaikuttaa tarpeeseen, sillä lähtökohtaisesti korkeariskisellä toimialalla toimivat yritykset haluavat herkemmin ottaa kybervakuutuksen. Asiakassopimuksien vastuissa on toimijalle yhä enemmän myös vastuita kyberriskeistä. Kyberriskit on nykymaailmassa otettava huomioon joka vaiheessa. Yrityksen joka tasolla varaudutaan kyberriskeihin, joiden suurimpana aiheuttajana on edelleen inhimilliset tekijät (Munich Re, 2020b).

Yrityksillä ei aina ole riittävää vakuutusosaamista itsellään arvioida kyberriskejä ja niiden toteutumista. Kyberriskin alati muuttuvan luonteen vuoksi vakuutusturvaa on haastavaa arvioida ja ylläpitää. On myös tarpeellista pohtia, kenen vastuulla on huolehtia riittävästä vakuutusturvasta alati muuttuvassa toimintaympäristössä, onko vastuu yrityksellä vai vakuutusyhtiöllä? Onko vakuutusyhtiöilläkään riittävää kybervakuutusten osaamista eri toimialojen ja yritysten riskien arviointiin ja kybervakuutusten tarjontaan?

Mitkä tekijät vaikuttavat kybervakuutuksen kartoitus-, vertailu- ja neuvotteluvaiheisiin ja ohjaavat yrityksen valintaa? Vakuutusyhtiöiden tarjoamat tuotteet ovat vaikeaselkoisia, eikä kybervakuutustuotteita voi varauksetta vertailla keskenään. Yritykset varsinkin korkeariskisellä IT-alalla kaipaavat räätälöityjä ratkaisuja, mutta vakuutusyhtiöt eivät ole halukkaita neuvottelemaan kybervakuutuksen vakuutusehdoista.

Kybervakuutuksen vaikeaselkoisuuden vuoksi ulkopuolisten asiantuntijoiden ja vakuutusmeklareiden käyttö kybervakuutusta ottaessa on lähes välttämätöntä, ellei halua valmista kybervakuutuspakettia. Meklareiden käytössä on omat haasteensa, ja kybervakuutuksen lopulliseen valintaan vaikuttaa monta tekijää. Meklareilla on lähtökohtaisesti vahvempi neuvotteluasema vakuutusyhtiöön päin pitkien yhteistöiden ja hyvien suhteiden seurauksena.

Riskit ja niiden korvausvelvollisuus yrityksen asiakkaiden kanssa tekemissä sopimuksissa voivat olla epäselviä ja poiketa toisistaan, mikä ennestään vaikeuttaa vertailua ja oikean vakuutussuojan hankkimista. Kybervakuutuksen hankinnan etenemistä tai vakuutusehtoja ei voi yleistää, sillä kybervakuutuksen ottaminen etenee osin yksilöllisesti. Yritykset eivät ole halukkaita kertomaan omista vakuutussopimuksistaan tai kybervakuutuksen ottamisen kokemuksistaan omalla nimellään.

Yhteiset reunaehdot kyberriskeistä ja kybervakuuttamisesta puuttuvat edelleen, vaikka vakuutus on ollut olemassa jo 30 vuotta. Näin ollen ennakkotapaukset puuttuvat, eikä tietoa ole kerätty ja analysoitu reunaehtojen ohjaamina. Terminologian yksinkertaistamista ja selventämistä kaivataan, mutta on epäselvää, kenen vastuulla se on. Edelleen yritykset kokevat kybervakuutuksen hankinnan sekavaksi, vaikka kysyntä on kasvanut.

5.2 Tutkimuksen arviointi

Tämän tutkimuksen laatimisessa on noudatettu tarkasti hyvää tieteellistä käytäntöä. Tutkimuskysymys muuttui ja tarkentui tutkimusprosessin edetessä. Tämä on tyypillistä kvalitatiiviselle tutkimukselle (Eriksson ym., 2005, 20). Tutkimuksen aihe on ajankohtainen ja rajaukset on esitelty tarkasti johdannossa.

Tutkimus on aina riippuvainen tutkijan henkilöhistoriasta, koulutuksesta, kokemuksista ja ennakkotiedoista (Eriksson ym., 2005, 43). Näin tämä tutkielma ei voi saavuttaa täyttä objektiivisuutta. Kvalitatiivisen tutkielman tavoitteena on löytää ja paljastaa tosiasioita (Hirsjärvi ym., 2009, 157). Tutkimuksen validiteettiin on kiinnitetty huomiota läpi tutkielman, ja tutkimuksen tarkoitus, kohde, tutkimusaineisto ja -menetelmät on esitelty huolellisesti sen parantamiseksi.

Kvalitatiivisen tutkimuksen arvioinnissa tulee myös pohtia aineiston kattavuutta. Tutkimuksen reliabiliteettia olisi voinut lisätä käyttämänä useamman yrityksen kybervakuutuksen hankinnan tapausta aineistona. Toisaalta kandidaatintutkielman laajuutta katsoen rajaus yhteen tapaukseen tässä tutkielmassa oli tarpeellinen.

Haastatteluun osallistunen henkilötietoja ja vastauksia käsiteltiin luottamuksellisesti ja säilytettiin vain tutkijan hallussa. Yrityksen toiveiden mukaan yritys tai haastateltava eivät ole tunnistettavissa tutkimuksesta. Haastateltavalla oli pitkä ura takana alan tehtävissä, sekä hän oli ainoa yrityksestä, joka oli ollut mukana jokaisessa vaiheessa kybervakuutuksen hankintaa ja oli siitä päävastuussa.

Tieteellisellä tiedolla on merkitystä, mikäli tieto antaa syvyyttä, täsmentää ongelmia ja luo ymmärrystä (Hirsjärvi ym., 2009, 20). Tämän tutkimuksen tulokset tuovat tutkijan mielestä arvokasta uutta näkökulmaa kybervakuutusprosessin tutkimiseen. Tutkimuksen tavoitteiden voidaan katsoa täyttyneen, sillä tutkielman teoria ja empiria tukivat toisiaan ja niiden avulla tutkimuskysymyksiin löydettiin vastaukset.

5.3 Mahdollisuudet jatkotutkimukselle

Tulevaisuudessa tutkimuksen aihepiiristä on mahdollista jatkaa tutkimusta monin eri tavoin. Ensinnäkin tämä tutkielma rajautui IT-alan yrityksen kybervakuutuksen hankintaan. Tutkimusta voisi jatkaa ja laajentaa tarkastelemaan myös eri toimialoja. Näin voisi tehdä vertailua eri toimialojen tarpeiden ja vakuutuksen hankinnan välillä.

Tämän tutkimuksen pohjalta voidaan todeta, että asiakkuuden arvolla vakuutusyhtiölle tai vakuutusmeklarille on vaikutusta kybervakuutuksen hankinnassa. Tätä voisi tutkia

enemmän, syventyen esimerkiksi kokonaisasiakkuuden vaikutukseen vakuutussopimusten muokattavuuteen.

Ulkomaisten toimijoiden kybervakuutustarjouksien vertailu Suomessa tarjottaviin kybervakuutuksiin voisi olla myös mielenkiintoinen näkökulma. Yhdysvaltojen kybervakuutusmarkkinat ovat paljon kehittyneemmän kuin Suomen, joten näiden markkinoiden vertailu loisi katsauksen markkinoihin sekä osaltaan antaisi tietoa Suomen vasta kehittyvän kybervakuutusmarkkinan kehityssuunnasta.

Tämä tutkielma rajautui yritysten kybervakuutusten tarkasteluun, mutta yksityishenkilöiden kybervakuutuksien suosio on myös nousussa. Covid-19 – pandemian myötä etätyö on lisääntynyt ja toiminta siirtynyt entisestään verkkoon. Tämän myötä myös yksityishenkilöitä uhkaavat kyberriskit. Tämä avaa lukuisia jatkotutkimusaiheita.

Myös ajankohtaisen Covid-19 – pandemian vaikutukset kybervakuuttamiseen tulevat esiin lähiaikoina. Pandemian seurauksena etätyö on lisääntynyt ja sekä yksityishenkilöt että yritykset tukeutuvat entisestään verkkoon. Tämän myötä kyberriskit pääsevät edelleen lisääntymään ja hyödyntämään uuden tilanteen heikkoja kohtia. Nähtäväksi tulee kybervakuutusten kehittyminen vastaamaan uudenlaisia tarpeita, vai muodostavatko kyberriskit jo tänä päivänä niin ison riskin etteivät vakuutusyhtiöt suostu enää vakuuttamaan sitä. Saattaa olla, että kybervakuutus muuttuu enemmänkin kyberturvallisuutta ja -neuvontaa tarjoavaksi ja korostuvaksi palveluksi.

LÄHDELUETTELO

Kirjallisuuslähteet

Ahonen, A., Puustinen, P. & Salonen, J. (2007). Ymmärrämmekö toisiamme – sähköiset vakuutuspalvelut lähemmäksi kuluttajaa. Teoksessa Järvinen, R., Lammi, M., & Leskinen, J. (toim.) Kuluttajat kehittäjinä. Miten asiakkaat vaikuttavat palvelumarkkinoilla? Kuluttajatutkimuskeskuksen vuosikirja 2007. Helsinki: Kuluttajatutkimuskeskus.

Antonucci, D. (2017). The Cyber Risk Handbook : Creating and Measuring Effective Cybersecurity Capabilities, John Wiley & Sons.

Aon. (2017). Global Cyber Market Overview - Uncovering the Hidden Opportunities.

Biener, C., Eling, M. & Wirfs, J. (2014). Insurability of Cyber Risk: An Empirical Analysis. Geneva Papers on Risk and Insurance - Issues and Practice. 40. 1-28. 10.1057/gpp.2014.19.

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

Colicchia, C., Creazza, A., & Menachof, D. A. (2019). Managing cyber and information risks in supply chains: Insights from an exploratory analysis. Supply Chain Management, 24(2), 215-240. Saatavilla sähköisesti: http://dx.doi.org.libproxy.tuni.fi/10.1108/SCM-09-2017-0289

Curti, F., Gerlach, J., Kazinnik, S., Lee, M. J., & Mihov, A. (2019). Cyber risk definition and classification for financial risk management. Federal Reserve Bank of St Louis, August, mimeo.

Eling, M. & Schnell, W. (2016). Ten key questions on cyber risk and cyber risk insurance, Technical report, The Geneva Association (the International Association for the Study of Insurance Economics). Edited by Fabian Sommerrock. Saatavilla sähköisesti: https://www.genevaassociation.org/media/954708/cyber-risk-10-key-questions.pdf

Eriksson, P. & Koistinen, K. (2005). Monenlainen tapaustutkimus. Kuluttajatutkimuskeskus.

Eskola, J., & Suoranta, J. (1998). Johdatus laadulliseen tutkimukseen. Vastapaino.

Evans, A. (2019). Managing Cyber Risk (1st ed.). Routledge. Saatavilla sähköisesti: https://doi.org/10.4324/9780429057632

Hirsjärvi, S., Remes, P. & Sajavaara, P (2009). Tutki ja kirjoita. 15. uudistettu painos. Helsinki: Kustannusosakeyhtiö Tammi.

Ives, B. & Mason, R. O. (1990). Can information technology revitalize your customer service? Academy of Management Executive. Vol. 4. No. 4. S. 52–69.

Low, P. (2017). Insuring against cyber-attacks. Computer Fraud & Security, Vol. 4. Saatavilla sähköisesti: https://doi.org/10.1016/S1361-3723(17)30034-9.

Lubin, A. (2019). Public Policy and The Insurability of Cyber Risk. 6 Journal of Law and Technology at Texas (julkaistaan 2021). Saatavilla sähköisesti: http://dx.doi.org/10.2139/ssrn.3452833

Määttä, M. & Forsman, R. (2005) Vakuutusedustus – asiamiesten ja vakuutusmeklarien toiminta. Helsinki: Suomen vakuutusalan koulutus ja kustannus.

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A & Sadhukhan, S. (2013). Cyber risk decision models: to insure IT or not? Decis. Support Syst. Vol. 56.

OECD. (2020a). Encouraging Clarity in Cyber Insurance Coverage: The Role of Public Policy and Regulation. Saatavilla sähköisesti: www.oecd.org/finance/insurance/Encouraging-Clarity-in-Cyber-Insurance-Coverage.pdf

OECD. (2020b). Enhancing the Availability of Data for Cyber Insurance Underwriting: The Role of Public Policy and Regulation. Saatavilla sähköisesti: www.oecd.org/finance/insurance/Enhancing-the-Availability-of-Data-for-Cyber-Insurance-Underwriting.pdf

OECD. (2017). Enhancing the role of insurance in cyber risk management. OECD Publishing, Paris. Saatavilla sähköisesti: http://dx.doi.org/10.1787/9789264282148-en

Ögut, H., Raghunathan, S. & Menon, N. (2011). Cybersecurity risk management: public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection. Risk Analysis.

Pohjola Vakuutus. (2020). Kybervakuutus. Tuoteopas, 1.4.2020 alkaen.

Rantala, J., & Kivisaari, E. (2020). Vakuutusoppi (13. uudistettu painos.). FINVA.

Roikola, T. (2017). Kyberriskeiltä suojautuminen ja kybervakuutusmarkkinat Suomessa. Tampereen yliopisto. Johtamisen ja talouden tiedekunta. Pro gradu -tutkielma.

Rubini, A. (2019). Fintech in a Flash : Financial Technology Made Easy: Vol. Third edition. De Gruyter.

Rytkönen, S. (2018). Kyberriskien arviointi ja kybervakuuttaminen: kolmannet osapuolet kyberriskien lähteenä. Tampereen yliopisto. Johtamisen ja talouden tiedekunta. Pro gradu -tutkielma.

Salovaara, E. (2020). Kybervalmius osana kuntien toteuttamaa riskienhallintaa. Kyberturvallisuuden järjestäminen suomalaisissa kunnissa – Case Kokemäen kaupunki. Tampereen yliopisto. Johtamisen ja talouden tiedekunta. Kandidaatintutkielma.

Soininen, M. (2020). Kyberriskit ja niiden hallintakeinot henkivakuutusyhtiössä : Case Nordea Henkivakuutus Suomi Oy. Tampereen yliopisto. Johtamisen ja talouden tiedekunta. Kandidaatintutkielma.

Strupczewski, G. (2021). Defining cyber risk. Safety science, 135, 105143. Saatavilla sähköisesti: https://doi.org/10.1016/j.ssci.2020.105143

Ylikoski, T., Järvinen, R., & Rosti, P. (2006). Hyvä asiakaspalvelu: menestystekijä finanssialalla. Finanssi- ja vakuutuskustannus.

Oikeudelliset lähteet

Direktiivi 2016/97/EU. Euroopan parlamentin ja neuvoston direktiivi vakuutusten tarjoamisesta.

European Commission. (2020). Statement/20/913 Joint statement ahead of the 2nd year anniversary of the General Data Protection Regulation. Annettu Brysselissä 20.5.2020.

Laki vakuutusten tarjoamisesta (234/2018). Annettu Helsingissä 20.5.2018. Saatavilla sähköisesti https://www.finlex.fi/fi/laki/alkup/2018/20180234.

Henkilölähteet

Haastateltava. Kyberriskeistä ja niiden hallinnasta vastaava henkilö. Haastattelu 29.3.2021.

Internet-lähteet

Allianz. (2020). Allianz Risk Barometer 2020 – From market developments and fire to loss of reputation or brand value. Luettu 25.2.2021. https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/allianz-risk-barometer-2020-business-risks.html

Finanssivalvonta. (2019). Vakuutusmeklarit 2010-2019. Välitetyt vakuutukset kuva 1. Luettu 30.3.2021. https://www.finanssivalvonta.fi/tilastot/vakuutus/vakuutusmeklarit/

If. (2021). Tietoturvavakuutus. Vahvista yrityksesi tietoturvaa kybervakuutuksella. Luettu 25.3.2021. https://www.if.fi/yritysasiakkaat/vakuutukset/vastuuvakuutukset/tietoturvavakuutus

Munich Re. (2020a). Cyber insurance: Risks and trends 2020. Luettu 4.3.2021. https://www.munichre.com/topics-online/en/digitalisation/cyber/cyber-insurance-risks-and-trends-2020.html

Munich Re. (2020b). Evaluating cyber risk? Here are some things to consider. Luettu 4.3.2021. https://www.munichre.com/topics-online/en/digitalisation/cyber/evaluating-cyber-risk.html

Munich Re. (2021). Cyber insurance: Risks and trends 2021. Luettu 23.3.2021. https://www.munichre.com/topics-online/en/digitalisation/cyber/cyber-insurance-risks-and-trends-2021.html

OECD. (2016). Cyber risk insurance. Luettu 1.2.2021. http://www.oecd.org/finance/insurance/cyber-risk-insurance.htm

OECD. (2021). Information and communication technology. Luettu 3.3.2021. https://doi.org/10.1787/04df17c2-en

Savolainen, S. (2021). 9 syytä käyttää vakuutusmeklaria. Luettu 6.4.2021. https://vakuutio.fi/blogi/9-syyta-kayttaa-vakuutusmeklaria/

Statista Research Department. (2021). Cyber insurance – Statistics & Facts. Luettu 28.2.2021. https://www.statista.com/topics/2445/cyber-insurance/

Tilastokeskus. (2021). PK-yritys. Luettu 3.3.2021. https://www.stat.fi/meta/kas/pk_yritys.html

LIITTEET

Liite 1: Haastattelurunko

Yrityksen kybervakuutuksen ottaminen

Taustatiedot

Tehtävä yrityksessä

Tausta it-alalla/työelämässä

Teema 1 Tarpeet ja taustat

Oliko teillä ennestään kybervakuutusta?

Minkä takia otitte kybervakuutuksen?

Suorittiko yrityksenne kyberriskien arvioinnin itse, vai käytättekö ulkopuolista asiantuntijaa?

Mitkä olivat kriteerinne kybervakuutukselle?

Teema 2 Vaihtoehtojen kartoitus

Mistä lähditte liikkeelle vakuutuksentarjoajien kartoittamisessa?

Oliko tietoa kybervakuutuksista ja niiden tarjoajista helppo löytää?

Minkälaiseksi koitte kartoitus ja tarjousten pyyntö prosessin?

Teema 3 Vertailu

Saatujen tarjousten vertailtavuus?

Mikä ohjasi päätöksentekoa?

Teema 4 Neuvottelu ja valinta

Miten neuvottelut etenivät? Neuvottelitteko sekä vakuutusyhtiön että vakuutusmeklarin kanssa?

Lopulliseen valintaan vaikuttavat tekijät?

Minkälaiseksi koitte neuvotteluasemanne?

Lopuksi

Miten yrityksenne kokee kybervakuutuksen antaman turvan?

Millainen lopputulos oli kybervakuutuksen suhteen?