Tampereen yliopisto

Susanna Aho

# KYBERRISKIT VAPAAEHTOISTEN HENKILÖVAKUUTUSTEN KORVAUSPALVELUSSA:

## Case Keskinäinen Vakuutusyhtiö

Johtamisen ja talouden tiedekunta

Kandidaatintutkielma

Kesäkuu 2021

# TIIVISTELMÄ

Susanna Aho: Kyberriskit vapaaehtoisten henkilövakuutusten korvauspalvelussa: Case Keskinäinen Vakuutusyhtiö
Kandidaatintutkielma: 35 sivua, 1 liitesivu
Tampereen yliopisto
Kauppatieteiden tutkinto-ohjelma: Vakuutus ja riskienhallinta
Kesäkuu 2021

---

Tässä tutkielmassa aiheena on ”Kyberriskit vapaaehtoisten henkilövakuutusten korvauspalvelussa: Case Keskinäinen Vakuutusyhtiö”. Kyberriskit ovat nousseet viime vuosina yhä suuremmaksi puheenaiheeksi. Teknologian kehittyminen ja digitalisaatio tuovat mukanaan monenlaisia mahdollisuuksia ja uhkia. Vakuutusyhtiössä käytännössä koko toiminta on sähköisten järjestelmien varassa, minkä vuoksi kyberriskit ovat vakuutusyhtiölle hyvin merkittävä uhka. Tässä tutkimuksessa käsitellään kyberriskejä ja niiden hallintaa vakuutusyhtiön vapaaehtoisten henkilövakuutusten korvauspalvelun näkökulmasta. Henkilövakuutusten korvauspalvelussa käsitellään paljon arkaluontoisia henkilö- ja terveystietoja, mikä tekee siitä erityisen haavoittuvaisen kyberriskeille.

Tämä tutkimus on luonteeltaan kvalitatiivinen tapaustutkimus, jossa case -yrityksenä toimii anonyymi suomalainen keskinäinen vakuutusyhtiö. Tutkimuksen tarkoituksena on löytää vastaukset kahteen päätutkimuskysymykseen: ”Millaisia kyberriskejä vapaaehtoisten henkilövakuutusten korvauspalvelussa on?” ja ”Miten korvauspalvelussa tunnistettuja kyberriskejä voidaan hallita?” Tutkimuksen taustateoria koostuu kyberriskin ja riskienhallinnan käsitteistä ja teorioista. Tutkimuksen empiirinen aineisto on kerätty haastattelemalla kahta kyberturvallisuuden asiantuntijaa. Haastattelut on toteutettu puolistrukturoituina teemahaastatteluina.

Tutkimuksessa havaittiin, että keskeisimmät case -yrityksen henkilökorvauspalvelun kohtaamat kyberriskit ovat tietomurto, kiristyshaittaohjelmat, palvelunestohyökkäykset, ihmisen puutteellinen tai virheellinen toiminta, sekä järjestelmien haavoittuvuudet ja virheet. Tärkeimpinä riskienhallintakeinoina nousivat esiin tietoturvateknologia, henkilöstön kyberosaamisen kehittäminen ja ylläpitäminen, uhkamallinnukset, käyttöoikeuksien rajaaminen minimiin, tuplasuojaukset järjestelmissä, tietoturvavalvomo, sekä järjestelmien jatkuva seuraaminen ja kehittäminen. Korvauspalvelun ja koko case -vakuutusyhtiön kohtaamien kyberriskien havaittiin tutkimuksessa olevan pitkälti samanlaisia.

Johtopäätöksenä voidaan todeta, että kyberriskejä on tunnistettu case -yrityksessä tällä hetkellä hyvin ja niille on olemassa selkeät riskienhallintakeinot. Kyberriskien geneerisyys on vakuutusyhtiölle eduksi, sillä yhtenäinen linja kyberriskien hallinnassa helpottaa riskienhallintaprosessin toteuttamista ja säästää vakuutusyhtiöltä kustannuksia. Kyberriskien uskotaan lisääntyvät tulevaisuudessa nopeasti. Etenkin 5G, tekoäly ja pilvipalvelut koetaan merkittävinä tulevaisuuden uhkina, joiden aiheuttamia riskejä on haastavaa arvioida tai hallita. Erityisesti näistä ilmiöistä olisikin aiheellista tehdä lisätutkimusta.

Avainsanat: kyberriski, kyberriskien hallinta, kyberturvallisuus, vapaaehtoinen henkilövakuutus, korvauspalvelu

# SISÄLLYSLUETTELO

# 1 JOHDANTO

## 1.1 Tutkielman tausta ja aikaisemmat tutkimukset

Uusia teknologioita otetaan käyttöön jatkuvasti, sillä ne tuovat mukanaan monenlaisia mahdollisuuksia ja hyötyjä. Työtehoa ja palvelun laatua voidaan parantaa, kun yksinkertaisia liukuhihnatehtäviä voidaan automatisoida ja samalla ihmiskontaktia tai monimutkaisempaa päätöksentekoa vaativiin tehtäviin on käytettävissä enemmän resursseja. Samalla nämä uudet teknologiat tuovat kuitenkin mukanaan myös uusia riskejä, etenkin kyberriskejä. Uudet riskit vaativat erilaisia ja tarkkaan harkittuja riskienhallintakeinoja, tai seuraukset voivat olla katastrofaaliset.

Kiinnostukseni tutkimusaiheeseen perustuu omaan työkokemukseeni vapaaehtoisten henkilövakuutusten korvauspalvelussa, sekä aiheen ajankohtaisuuteen ja merkityksellisyyteen. Kyberriskit vapaaehtoisten henkilövakuutusten korvauspalvelussa ovat aiheena mielenkiintoinen erityisesti siksi, että tapaturma- ja sairausvahinkoja käsiteltäessä ollaan erityisen paljon tekemisissä yksityishenkilöiden arkaluontoisten terveystietojen kanssa.

Kyberriskit voivat realisoituessaan aiheuttaa yritykselle merkittäviä taloudellisia seuraamuksia ja välillisesti esimerkiksi maineriskin. Esimerkiksi tietomurto- tai tietovuoto voi horjuttaa asiakkaiden luottamusta yritykseen tai yritys voi jopa menettää sen kokonaan. Asiakkaiden tietojen joutuessa vääriin käsiin asiakkaiden tietoturva joutuu uhatuksi ja tällä voi olla sekä vakuutusyhtiön että yksilön näkökulmasta vakavia seurauksia.

Swiss Re Instituten vuonna 2019 julkaisemassa raportissa ”New Emerging Risk Insights” kyberriskit on määritelty yhdeksi vaikuttavimmista riskeistä nyt ja tulevina vuosina. Raportin mukaan kyberriskit tuovat mukanaan suuria mahdollisuuksia erityisesti vakuutusten tarjoajille kybervakuutusten kysynnän kasvaessa, mutta samalla ne tuovat mukanaan myös suuria haasteita. Kyberriskeistä tekee merkityksellisen etenkin niiden seurausten vakavuus ja riskien nopea kehittyminen. Kyberhyökkäysten määrän uskotaan raportin mukaan lisääntyvän merkittävästi tulevien vuosien aikana, ja samalla niiden aiheuttamien riskien vakavuuden uskotaan kasvavan. Raportin mukaan monet yritykset

eivät ole valmistautuneet riittävän hyvin kohtaamaan kyberriskejä, vaikka näillä voi olla yritysten toiminnan kannalta hyvin vakavia seurauksia. (Swiss Re Institute, 2019, 12, 49.)

Suomessa on aikaisemmin tehty vähän kyberriskeihin, kybervakuuttamiseen ja kyberilmiöön liittyvää tutkimusta. Kyberriskit ovat kuitenkin perinteisiin riskeihin verrattuna uusi ilmiö, ja lisäksi niille on ominaista jatkuvasti muuttuva ja vaikeasti määriteltävä luonne (Swiss Re Institute, 2019, 12, 49). Ensimmäinen varsinainen kyberhyökkäys oli "Morris Worm", ensimmäinen automatisoidusti verkossa levinnyt tietokonemato, joka saastutti tuhansia tietokoneita vuonna 1988. Kuitenkin vasta 2000 -luvun alusta lähtien kyberriskit ovat nousseet tärkeämmäksi osaksi riskienhallintaa ja niiden tunnistamiseen on alettu kiinnittää enemmän huomiota. (Eling, McShane & Nguyen, 2021, 95-96.)

Jatkuvan muutoksen ja suhteellisen vähäisen aikaisemman tutkimuksen vuoksi kyberriskejä ja kyberilmiötä onkin hyödyllistä tutkia koko ajan lisää. Seuraavat tutkimukset käsittelevät kyberriskejä tai kyberilmiötä: Tia-Liisa Roikola on kirjoittanut vuonna 2017 Pro Gradu -tutkielmansa aiheesta ”Kyberriskeiltä suojautuminen ja kybervakuutusmarkkinat Suomessa”. Mia Soininen kirjoitti vuonna 2020 kandidaatintutkielmansa kyberriskeistä ja niiden hallintakeinoista Nordea henkivakuutusyhtiössä. Sakari Rytkönen teki vuonna 2018 Pro gradu -tutkielman aiheesta ”Kyberriskien arviointi ja kybervakuuttaminen –kolmannet osapuolet kyberriskien lähteenä”. Irina Lönnqvist kirjoitti vuonna 2013 opinnäytetyönsä aiheesta ”Elämmekö kyberriskiyhteiskunnassa?” Myös Jarno Limnell on tutkinut kyber -ilmiötä vuoden 2014 tutkimuksessaan ”Kyber rantautui Suomeen”.

## 1.2 Tutkimuksen tavoitteet, tutkimusongelmat ja rajaukset

Tutkimuksen tavoitteena on tunnistaa kyberriskejä ja näiden riskienhallintakeinoja case -vakuutusyhtiön vapaaehtoisten henkilövakuutusten korvauspalvelussa. Samalla tutkitaan kyberriskien merkityksellisyyttä ja seurauksia vakuutusyhtiön korvauspalvelun näkökulmasta.

Tutkimuksella on kaksi päätutkimuskysymystä:

1. Millaisia kyberriskejä vapaaehtoisten henkilövakuutusten korvauspalvelussa on?
2. Miten korvauspalvelussa tunnistettuja kyberriskejä voidaan hallita?

Ensimmäisen tutkimuskysymyksen avulla tunnistetaan vapaaehtoisten henkilövakuutusten korvauspalveluun liittyviä kyberriskejä ja tutkitaan, millaisia seurauksia kyberriskien realisoitumisella voi olla sekä vahinkovakuutusyhtiön että asiakkaiden näkökulmasta. Kyberriskejä tunnistetaan korvauspalvelun jokaisesta työvaiheesta, työssä käytetyistä järjestelmistä ja tietojen säilyttämisestä. Tutkielmassa tutkitaan myös, kenellä on vastuu riskin mahdollisesta realisoitumisesta ja sen aiheuttamista seurauksista. Vapaaehtoisten henkilövakuutusten korvauspalvelussa tietoa jaetaan usein kolmansille osapuolille, kuten hoitolaitoksille. Erityisesti tapauksessa, jossa kyberriskin realisoitumiseen liittyy kolmas osapuoli, voi olla epäselvää, kenellä on vastuu seurauksista.

Toisen tutkimuskysymyksen avulla tutkitaan, millaisia riskienhallintakeinoja vapaaehtoisten henkilövakuutusten korvauspalvelussa tunnistettujen kyberriskien hallitsemiseksi voidaan käyttää. Riskienhallintakeinoja tunnistetaan vapaaehtoisten henkilövakuutusten korvauspalvelun näkökulmasta, mutta myös koko vahinkovakuutusyhtiön kannalta. Tutkittavaa ympäristöä on tältä osin laajennettu myös case- vakuutusyhtiön muihin osastoihin, sillä kyberriskien hallinta on oleellisesti koko vakuutusyhtiön vastuulla, eikä tätä siksi voida rajata pelkästään henkilökorvauspalveluun. Riskejä tunnistetaan kuitenkin tässä tutkimuksessa vain vapaaehtoisten henkilövakuutusten korvauspalvelun osalta. Tutkimuskysymyksiin etsitään vastauksia kahdesta asiantuntijahaastattelusta kerätystä empiirisestä aineistosta. Empiiristä aineistoa peilataan tutkielman taustateoriaan, joka koostuu kyberriskeihin liittyvästä kirjallisuudesta, tieteellisistä artikkeleista ja raporteista, sekä aikaisemmista tutkimuksista.

Kyseessä on case -tutkimus, jonka aihealue on rajattu case -vakuutusyhtiön vapaaehtoisten henkilövakuutusten korvauspalveluun. Muut markkinoilla vaikuttavat vakuutusyhtiöt ja case- vakuutusyhtiön muut osastot on rajattu pois tutkimuksesta, sillä kyberriskit ovat merkittävä uhka etenkin vapaaehtoisten henkilövakuutusten korvauspalvelussa, jossa käsitellään paljon arkaluontoisia asiakkaiden terveystietoja. Aihealueen rajaamiseen vaikutti myös se, että työskentely-ympäristö vapaaehtoisten henkilövakuutusten parissa on minulle entuudestaan tuttu ja siten tutkimuksen kohteena mielenkiintoinen. Tutkimuksen kohdistaminen koko vakuutusyhtiöön tai useisiin eri toimijoihin olisi lisäksi voinut olla vaikeaa, jolloin syvällinen perehtyminen aiheeseen ja

tutkimusprosessin hallinta olisi ollut haastavaa. Case-tutkimus koskee vain yhtä vakuutusyhtiötä, joten tutkimuksen tuloksia ei voida yleistää koskemaan koko toimialaa.

## 1.3 Keskeiset käsitteet

Tässä alaluvussa selitän tutkittavan aiheen ymmärtämisen kannalta keskeiset käsitteet. Samalla määrittelen, mitä käsitteillä tässä tutkimuksessa tarkoitetaan.

*Riskillä* voidaan yleisesti viitata vaaraan tai uhkaan, jonka seurauksena esimerkiksi yksittäiselle henkilölle, yritykselle tai jonkun omaisuudelle voi tapahtua jotakin epäedullista. Riskiin liittyy oleellisesti epävarmuus. Jos jonkin tapahtuman sattuminen tai sen seuraukset ovat täysin ennalta tiedossa, ei kyseessä ole riski. (Juvonen, Koskensyrjä, Kuhanen, Ojala, Pentti, Porvari & Talala, 2014, 8–10.) Tässä tutkielmassa riskillä viitataan ainoastaan negatiivisiin epävarmuustekijöihin.

*Kyberriskillä* tarkoitetaan tässä tutkimuksessa taloudellisen tappion riskiä, liiketoiminnan häiriötä tai maineriskiä, joka aiheutuu informaatioteknologian toimimattomuudesta. Kyberriski voi realisoitua esimerkiksi tietomurtona, tietovuotona tai järjestelmien toiminnan häiriönä. (Institute of Risk Management, 2014, 8.)

*Kyberturvallisuudella* tarkoitetaan sähköisessä muodossa olevan tiedon, kyberavaruuden, kommunikaatio- ja informaatioteknologian sekä näiden käyttäjän tietojen suojaamista. Kyberturvallisuus sisältää sekä yhteiskuntien että yksilöiden aineettoman ja aineellisen omaisuuden, joka on vaarassa vahingoittua kyberavaruudesta tulevien uhkien seurauksena. Kyberturvallisuus on laajempi käsite kuin tietoturvallisuus, joka sisältää ainoastaan tiedon luottamuksellisuuden, eheyden ja saatavuuden. (von Solms & van Niekerk, 2013, 97-98.)

*Korvauskäsittelyllä* tarkoitetaan tässä tutkielmassa koko korvausprosessia alkaen asiakkaan yhteydenotosta ja päättyen joko korvauksen maksamiseen tai hylkäämiseen. Korvauskäsittely tapahtuu vakuutusyhtiön korvauspalvelussa. (Finanssiala Ry, 2021.) Korvauspalvelulla viitataan tässä tutkielmassa ainoastaan vapaaehtoisten henkilövakuutusten korvauspalveluun. *Vapaaehtoisilla henkilövakuutuksilla* tarkoitetaan tässä tutkimuksessa vapaaehtoisia tapaturma- sairaus ja matkustajavakuutuksia.

## 1.4 Tutkimusmenetelmät ja -aineistot

Eskolan ja Suorannan mukaan ”Hyvä tutkimus lähtee teoriasta ja jälleen palaa siihen”. Tutkimus eroaa selvityksestä siten, että se sisältää aineiston ja teorian vuoropuhelua. (Eskola & Suoranta, 1998, 59-61.) Tässä tutkimuksessa ei pyritä todistamaan olemassa olevaa teoriaa todeksi, vaan laadulliselle tutkimukselle tyypillisesti perehdytään teoriaan ja pyritään selittämään tutkittavaa ilmiötä sen avulla, sekä tuomaan esiin uusia seikkoja (Hirsjärvi, Remes & Sajavaara, 2009, 161). Samalla tehdään teoriaan peilaten päätelmiä empiirisestä aineistosta. Laadullisen tutkimuksen tekemiseen vaaditaan kaksi erilaista teoriaa: taustateoria, jonka pohjalta tutkittavaa aineistoa voidaan tarkastella ja tulkintateoria, joka määrittelee mihin kysymyksiin ja näkökulmiin tutkija hakee aineistosta vastauksia (Eskola & Suoranta, 1998, 60).

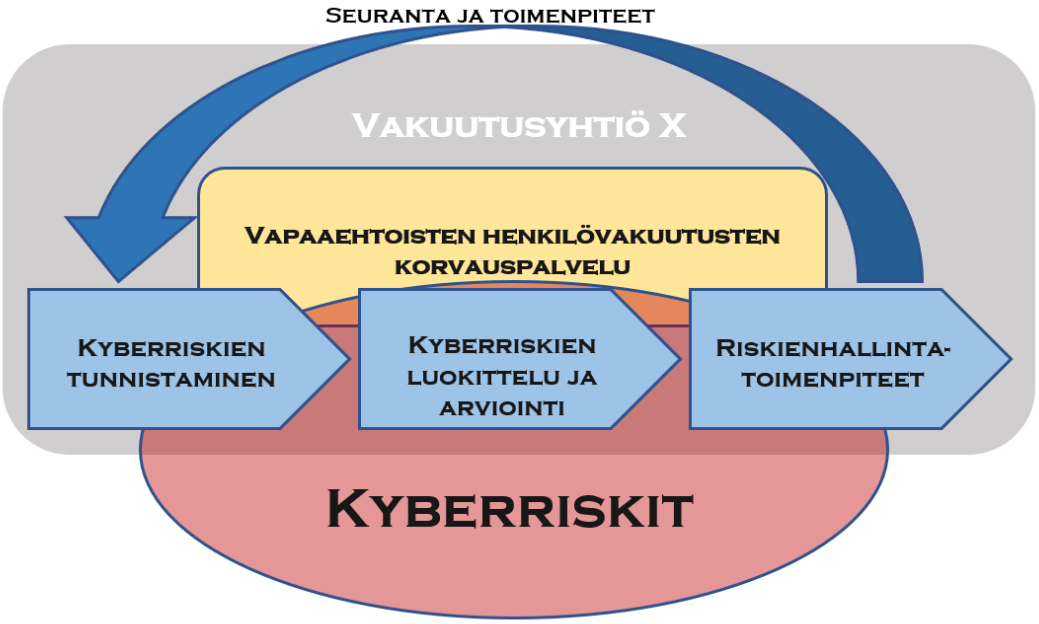
Tämän tutkielman taustateorian muodostavat kyberriskien ja riskienhallinnan käsitteet ja tulkintateoriana toimii vapaaehtoisten henkilövakuutusten korvauspalvelun näkökulma. Tutkimuksen taustateoriassa teoreettisena aineistona käytetään kyberriskeihin, riskienhallintaan ja vakuuttamiseen liittyvää kirjallisuutta, tieteellisiä artikkeleita, aikaisempia tutkimuksia ja raportteja. Lisäksi analyysissa hyödynnetään vakuutussopimuslakia, vakuutusyhtiölakia, rikoslakia ja Euroopan Unionin yleistä tietosuoja-asetusta, jotka vaikuttavat oleellisesti vakuutusyhtiön oikeuksiin ja velvollisuuksiin asiakkaiden tietojen käsittelyssä.

Tämä tutkimus on kvalitatiivinen tapaustutkimus. Tapaustutkimuksessa, eli case -tutkimuksessa tutkimus kohdistuu yhteen case -yritykseen, tässä tapauksessa anonyymiin keskinäiseen vahinkovakuutusyhtiöön. Kvalitatiiviselle tutkimukselle ominaista on kontekstuaalisuus, tulkinta ja tutkittavan ilmiön ymmärtäminen. Kvalitatiivisessa tutkimuksessa tutkimuksen asetelma saattaa muuttua jonkin verran tutkimusprosessin edetessä. (Hirsjärvi & Hurme, 2015, 21-26.) Laadullisen tutkimuksen analyysi voi olla teoreettista tai empiiristä. Tässä tutkimuksessa käytetään sekä empiiristä että teoreettista analyysia, vaikkakin tutkimuksen pääpaino on empiirisessä analyysissä. Empiirisessä analyysissa aineiston keräämis- ja analysointimetodit ovat oleellisia, kun taas teoreettisessa analyysissa tarkkaa metodia ei ole. Teoreettisessa analyysissa perehdytään olemassa olevaan aineistoon ja pyritään selittämään tutkittavaa ilmiötä sen avulla, kun taas empiirisessä analyysissa päätelmiä tehdään itse kerätyn aineiston perusteella. (Tuomi & Sarajärvi, 2018, 19-22.)

Empiirisen osuuden aineisto hankittiin kahden asiantuntijahaastattelun avulla. Haastateltavat ovat kyberriskeihin ja riskienhallintaan erikoistuneita asiantuntijoita. Haastattelut suoritettiin puolistrukturoituina teemahaastatteluina (lyhyemmin teemahaastattelu). Puolistrukturoidussa teemahaastattelussa on valmiit kysymykset ja teema-alueet, jotka ovat kaikille haastateltaville samat. Valmiita vastausvaihtoehtoja, tarkkaa muotoa tai järjestystä teemahaastattelussa ei kuitenkaan ole, vaan kysymysten järjestys ja sanamuoto saattaa vaihdella ja haastateltavalla on mahdollisuus vastata haastattelukysymyksiin omin sanoin. Teemahaastattelussa korostuu vahvasti vuorovaikutuksen ja kommunikaation merkitys, sekä haastattelijan objektiivisuus. (Hirsjärvi & Hurme, 2015, 47-50.) Haastattelukysymykset toimitettiin haastateltaville ennen haastattelua, jotta heillä oli aikaa perehtyä aiheeseen ja valmistautua tulevaan haastatteluun. Haastattelusta kerätty empiirinen aineisto toimii tutkimuksen primaariaineistona. Teemahaastattelurunko on liitteenä tutkimuksen lopussa. (Liite 1)

## 1.5 Tutkielman rakenne ja teoreettinen viitekehys

Tämä tutkimus koostuu viidestä pääluvusta ja niiden alaluvuista. Ensimmäisessä pääluvussa, *(Johdanto*) kerrotaan yleisesti tutkittavasta ilmiöstä ja tutkimuksen taustasta, esitellään tutkimusongelmat ja rajaukset, sekä keskeiset käsitteet, tutkimusmenetelmät ja -aineisto, teoreettinen viitekehys ja aiheesta aiemmin tehdyt tutkimukset. Toisessa pääluvussa (*Korvausprosessi*) kuvaillaan vapaaehtoisten henkilövakuutusten korvauskäsittelyn prosessin eri vaiheet ja käsitellään lainsäädännön vaikutuksia korvausprosessiin ja henkilötietojen käsittelyyn. Kolmannessa pääluvussa (*Kyberriskit ja riskienhallinta*) perehdytään syvällisemmin kyberriskeihin, niiden erityispiirteisiin ja riskienhallintaan käsitteenä, sekä esitellään erilaisia riskienhallintastrategioita. Neljännessä pääluvussa (*Kyberriskit vapaaehtoisten henkilövakuutusten korvauspalvelussa*) tunnistetaan kyberriskejä ja niiden hallintakeinoja vapaaehtoisten henkilövakuutusten korvauspalvelussa, esitellään ja analysoidaan haastatteluista kerätty empiirinen aineisto, sekä keskeiset tulokset. Viidennessä pääluvussa (*Yhteenveto ja johtopäätökset*) vastataan tutkimuskysymyksiin, arvioidaan tutkimuksen luotettavuutta ja tehdään jatkotutkimusehdotuksia. Tutkielman lopussa on lähdeluettelo ja liitteet.




Kuvio 1 Teoreettinen viitekehys

Teoreettisessa viitekehyksessä (Kuvio 1) yhdistyvät tutkimuksen teoria ja empiria. Teoreettinen viitekehys on rakennettu siten, että kaiken taustalla on tutkimuksen case - vakuutusyhtiö. Koko vakuutusyhtiö on kuviossa haaleammalla värillä, sillä ilmiötä tutkitaan vakuutusyhtiön korvauspalvelun näkökulmasta, joka on merkitty Case vakuutusyhtiön sisälle kirkkaammalla värillä. Korvauspalvelun näkökulma toimii myös tutkielman tulkintateoriana. Kyberriskit ja kyberriskien hallinta muodostavat tutkimuksen taustateorian. Kyberriskit sivuavat kuviossa korvauspalvelua ja koko vakuutusyhtiötä. Kyberriskit ovat osittain päällekkäin vakuutusyhtiön ja korvauspalvelun käsitteen kanssa ja osittain näiden ulkopuolella, mikä symboloi sitä, että osa kyberriskeistä on lähtöisin vakuutusyhtiön ulkopuolelta ja osa kyberriskeistä taas on sisäisiä riskejä. Kyberriskien hallintaprosessi alkaa kuvion mukaisesti riskien tunnistamisesta, jota seuraa riskien luokittelu ja arviointi. Kun riskit on luokiteltu ja niiden vakavuudet ja todennäköisyydet arvioitu, määritellään riskeille sopivat riskienhallintatoimenpiteet. Kyberriskejä ja näiden hallintaa seurataan ja arvioidaan jatkuvasti ja tarvittaessa toimenpiteisiin tehdään muutoksia. Nuoli symboloi kuviossa riskienhallinnan jatkuvuutta.

# 2 KORVAUSPROSESSI

## 2.1 Vapaaehtoiset henkilövakuutukset ja korvauskäsittely

*Henkilövakuutuksella* tarkoitetaan vakuutustuotetta, jonka vakuutusturvan kohteena on ihminen. Henkilövakuutuksella voidaan hankkia turvaa henkilöriskien, kuten kuoleman, sairauden, tapaturman ja työkyvyttömyyden varalle. Suomessa lakisääteistä sosiaalivakuutusta voidaan täydentää *vapaaehtoisilla henkilövakuutuksilla*. (Jokela, Lammi, Lohi & Silvola, 2013, 17.) Case -yrityksessä käsiteltäviä vapaaehtoisia henkilövakuutuksia ovat vapaaehtoinen tapaturma-, sairaus- ja matkustajavakuutus.

*Korvauskäsittelyyn* kuuluu vahinkoilmoitusten vastaanottaminen ja vahinkotapahtuman luominen järjestelmälle vahinkoilmoitukselta saatuihin tietoihin perustuen, korvauspäätöksen tekemisen kannalta tarpeellisen lisätiedon hankkiminen, korvauspäätöksen tekeminen ja korvauksen maksaminen tai epääminen, sekä ratkaisun ilmoittaminen ja sen perustelu asiakkaalle. (Finanssiala Ry, 2021.) Vakuutussopimuslain kymmenennen luvun pykälän 69 mukaan korvauksen hakija on velvollinen antamaan vakuutuksenantajalle korvauskäsittelyä varten tarpeelliset asiakirjat ja tiedot.


Kuvio 2 Korvausprosessin eteneminen (Mukaillen Finanssiala Ry, 2021)

Kuviossa 2 on havainnollistettu korvausprosessin etenemistä. Korvauskäsittely tapahtuu vakuutusyhtiön *korvauspalvelussa*, johon asiakas voi olla yhteydessä esimerkiksi verkkopalvelun kautta tai puhelimitse. Vapaaehtoisten henkilövakuutusten korvauskäsittelyssä korvausprosessi on muihin vakuutuslajeihin nähden poikkeava, sillä terveystiedoilla on keskeinen rooli korvattavuuden päättelyssä. Tämän vuoksi

vapaaehtoisten henkilövakuutusten korvauspalvelussa käsitellään ja säilytetään paljon arkaluontoisia terveystietoja, mikä jo itsessään tekee korvauspalvelusta potentiaalisen kohteen kyberhyökkäyksille. Korvausprosessi lähtee liikkeelle vahinkoilmoituksen tekemisestä. Asiakas voi tehdä vahinkoilmoituksen puhelimitse, verkkopalvelussa, postitse tai kasvotusten kivijalkakonttorilla. Vahinkoilmoituksen vastaanottamisen jälkeen siirrytään vahingon korvattavuuden tarkastamiseen. Jos korvattavuudessa on epäselvyyttä, voidaan asiakasta pyytää toimittamaan korvauskäsittelyyn esimerkiksi potilaskertomustekstit tai lääkärintodistus. (Finanssiala Ry, 2021.)

Vahingon korvattavuutta saattavat arvioida vakuutusyhtiössä korvauskäsittelijöiden lisäksi esimerkiksi vakuutuslääkäri ja korvausasiantuntijat. Kun korvattavuus on selvitetty, asiakkaalle tulee joko maksaa korvaus tai ilmoittaa kielteisestä päätöksestä. Lisäksi asiakkaalle tulee aina toimittaa vakuutusyhtiön ratkaisusta korvauspäätös. Hyvän vakuutustavan mukaan kielteiset tai asiakkaan vahinkoilmoituksesta eriävät korvauspäätökset tulee perustella asiakkaalle huolellisesti. Vakuutusyhtiön tulee toimittaa korvauksenhakijalle päätös korvattavuudesta kuukauden kuluessa tarvittavien tietojen saamisesta. Kuviossa 2 korvausprosessin viimeinen vaihe on muutoksenhaku, joka toisinaan saattaa olla ajankohtainen, jos asiakas on saamaansa korvauspäätökseen tyytymätön. Muutoshakemus tehdään ensin päätöksen tehneelle korvauskäsittelijälle. Mikäli tämä ei tuota haluttua lopputulosta, asiakas voi tehdä muutoshakemuksen tuomioistuimen, vakuutuslautakunnan tai kuluttajariitalautakunnan käsiteltäväksi. (Finanssiala Ry, 2021.)

## 2.2 Henkilötietojen käsittely

Henkilötietojen käsittelyä koskevalla lainsäädännöllä on suuri vaikutus vakuutusalaan, sillä vakuutusyhtiön toiminta on hyvin pitkälti tietojen käsittelyä. Tietosuojalainsäädäntö uudistui toukokuussa 2018, kun EU:n yleinen tietosuoja-asetus (EU 2016/679) tuli jäsenvaltioissa suoraan sovellettavaksi. Tietosuoja-asetuksen tarkoituksena oli ajantasaistaa tietosuojaa koskeva sääntely vastaamaan paremmin nykyaikaista teknologiaa ja digitaalisia palveluita. Lähtökohtana tietosuojalainsäädännössä on yksilön oikeus elää ilman ulkoisten tahojen puuttumista hänen yksityiselämäänsä. Tähän kuuluu henkilön oikeus tietää ja päättää itseään koskevien tietojen käsittelystä. Lähtökohtaisesti tämä tarkoittaa, että henkilötietojen käsittelyn on perustuttava henkilön suostumukseen. Tietosuoja-asetuksessa ja kansallisessa tietosuojalaissa määritellään poikkeukset tähän.

Vakuutusyhtiössä henkilötietojen käsittelyn tulee kuitenkin poikkeuksetta olla perusteltua, lainmukaista ja läpinäkyvää. (Luukkonen, Mäntyniemi, Pekonen-Ranta, Raulos & Santavirta, 2018, 251.)

Tietosuoja-asetuksen (2016/679) mukaan henkilötiedoilla tarkoitetaan kaikkia tietoja, jotka koskevat tunnistettua tai tunnistettavissa olevaa henkilöä, eli rekisteröityä. Henkilötietoja ovat esimerkiksi nimi, osoite, tulot, kulttuurinen profiili ja potilastiedot. (Tietosuoja-asetus 2016/679, 4§.) Vakuutusyhtiössä henkilötietoja ovat lisäksi kaikki henkilön vakuutussopimuksiin liittyvät vakuutus- ja korvaustiedot. (Luukkonen ym., 2018, 253.) Rekisterinpitäjällä tarkoitetaan: ”luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.” Tässä tutkielmassa rekisterinpitäjällä viitataan case -vakuutusyhtiöön. Henkilötiedon käsittelijällä tarkoitetaan: ”luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.” (Tietosuoja-asetus 2016/679, 4§.)

Rekisterillä tarkoitetaan jäsenneltyä henkilötietoa sisältävää tietojoukkoa. Vakuutusyhtiössä on vakuutustoimintaa varten käytössä esimerkiksi asiakas-, korvaus-, vakuutus- ja perintärekistereitä. Lisäksi korvauskäsittelyssä syntyvät vahinkokansiot, joihin kuuluvat esimerkiksi asiakkaiden toimittamat terveystiedot, ovat osa korvaustoiminnan rekisteriä. (Luukkonen ym., 2018, 253-254.) Rekisteriä muodostuu vakuutusyhtiössä vakuutussopimuksia tehdessä ja korvauspalvelussa vahinkotapahtumien myötä. Laajamittainen terveystietoja sisältävä rekisteri ja vahinkotapahtumien myötä syntyvä vahinkorekisteri muodostavat vapaaehtoisten henkilövakuutusten korvauspalvelussa suuren potentiaalin kyberriskeille.

Vakuutusyhtiölle alkaa kertyä rekisteriä vakuutuksenottajista ja vakuutetuista jo ennen vakuutuksen myöntämistä. Vakuutussopimuslain neljännen luvun pykälän 22 mukaan vakuutuksenottajan ja vakuutetun tulee antaa vakuutusyhtiön esittämiin kysymyksiin oikeat ja täydelliset vastaukset, joilla saattaa olla merkitystä vakuutusyhtiön vastuun arvioimisessa. Vapaaehtoisten henkilövakuutusten kannalta oleellisia ovat tiedot vakuutetun terveydentilasta. Vakuutetun olemassa olevat sairaudet ja aiemmat vammat kartoitetaan jo ennen vakuutuksen myöntämistä terveysselvityksen avulla. Jos vakuutuksenottaja tai vakuutettu on laiminlyönyt tiedonantovelvollisuuttaan tai antanut

vakuutuksentarjoajalle virheellistä tietoa, vakuutussopimus ei vakuutussopimuslain neljännen luvun pykälän 23 mukaan sido vakuutuksenantajaa.

Henkilötietojen käsittelyksi vakuutusyhtiössä luetaan kaikki henkilötietoihin kohdistuvat toimenpiteet, kuten tietojen kerääminen, käyttö, tallentaminen, säilyttäminen, muokkaaminen, poistaminen, siirtäminen ja luovuttaminen. Käsittely voi olla joko automaattista tai manuaalista. (Luukkonen ym., 2018, 253.) Henkilön terveydentilaa koskevat tiedot on tietosuojalainsäädännössä luokiteltu arkaluontoisiksi tiedoiksi, joiden käsittely on lähtökohtaisesti kielletty. Vakuutusyhtiössä voidaan kuitenkin käsitellä asiakkaiden terveystietoja, mikäli näiden käsittely on tarpeen vakuutusyhtiön vastuun selvittämiseksi. (Luukkonen ym., 2018, 254-255.)

Tietosuoja-asetuksessa (2016/679) määritellään edellytykset sille, milloin tietojen käsittely yrityksessä on sallittua. Tietosuoja-asetus edellyttää, että tietoja käsitellään asianmukaisesti ja lainmukaisesti tiettyä laillista tarkoitusta varten, ja että vain tätä tarkoitusta varten tarvittavia tietoja käsitellään. (Tietosuoja-asetus 2016/679, 5§.) Henkilötietojen käsittelyä yrityksessä valvoo tietosuojavastaava, joka yrityksen tulee nimittää, mikäli yrityksessä käsitellään henkilötietoja laajamittaisesti, valvotaan yksilöitä tai käsitellään erityisiä tietoryhmiä. (Tietosuoja-asetus 2016/679, 37§.) Vakuutusyhtiön on nimettävä tietosuojavastaava, koska vakuutusyhtiössä käsitellään arkaluontoisia tietoja. (Luukkonen ym., 2018, 258.)

Vakuutusyhtiön työntekijöillä on vakuutusyhtiölain (18.7.2008/521) luvun 30 ensimmäisen pykälän mukaan vaitiolovelvollisuus koskien asiakkaiden arkaluontoisia tietoja. Tähän kuuluvat esimerkiksi taloudellista asemaa, terveydentilaa ja muita henkilökohtaisia oloja koskevat tiedot tai liikesalaisuudet. Korvauskäsittelijä ei saa ilmaista näitä tietoja sivulliselle taholle, ellei asiakas erikseen anna suostumustaan tähän. Vakuutusyhtiö saa kuitenkin vakuutusyhtiölain luvun 30 kolmannen pykälän mukaan luovuttaa tietoja salassapitovelvollisuudesta huolimatta joissain tapauksissa muun muassa toisille vakuutusyhtiöille, ulosotto-, vero-, tai sosiaaliviranomaisille ja alan lautakunnalle

Rekisteröidylle tulee taata ilmainen pääsy omiin henkilötietoihinsa. Yrityksen on siis rekisteröidyn pyynnöstä kerrottava, mikäli hänen henkilötietojaan käsitellään, mikä on tietojen käsittelyn tarkoitus, mitä tietoja käsitellään ja kenelle tietoja luovutetaan. Lisäksi

rekisteröidylle on annettava helposti saatavassa muodossa jäljennös niistä henkilötiedoista, joita hänestä käsitellään. (Tietosuoja-asetus 2016/679, 15§.) Rekisteröidyllä on myös oikeus vastustaa tietojensa käsittelyä. Mikäli yrityksellä ei ole oikeutettua etua, joka syrjäyttää rekisteröidyn edun, tulee henkilötietojen käsittely lopettaa tämän pyynnöstä. (Tietosuoja-asetus 2016/679, 21§.) Lisäksi rekisteröidyllä on oikeus tulla unohdetuksi, mikä tarkoittaa sitä, että rekisterinpitäjän tulee rekisteröidyn pyynnöstä poistaa häntä koskevat tiedot. (Tietosuoja-asetus 2016/679, 17§.)

Rekisterinpitäjän tulee toteuttaa asianmukaiset tekniset ja organisatoriset toimenpiteet, joiden avulla voidaan varmistua siitä, että ainoastaan tietyn tarkoituksen kannalta tarpeellisia henkilötietoja käsitellään. Lisäksi rekisterinpitäjän on uusin tekniikka ja toteuttamiskustannukset, sekä käsittelyn luonne, asiayhteys, tarkoitus ja riskien todennäköisyys huomioiden toteutettava tehokkaasti erilaisia tietosuojaperiaatteita suojatakseen rekisteröityjen oikeuksia ja vastatakseen tietosuoja-asetuksen vaatimuksia. (Tietosuoja-asetus 2016/679, 25§.) Vakuutusyhtiön on otettava tietosuoja huomioon kaikessa järjestelmä- ja sovelluskehityksessä, sekä tuotteiden ja palveluiden kehityksessä. Lisäksi henkilötietojen suojaamisesta on huolehdittava kaikissa käsittelyn vaiheissa. (Luukkonen ym., 2018, 258.)

Tietosuoja-asetuksessa velvoitetaan, että rekisterinpitäjän on ilmoitettava mahdollisesta tietoturvaloukkauksesta tietosuojaviranomaisille 72 tunnin kuluessa siitä, kun loukkaus on tullut tietoon. Tietoturvaloukkauksesta on kyse, jos yrityksen vastuulla olevia tietoja on vahingossa tai laittomasti päätynyt valtuuttamattomille vastaanottajille, tai jos niihin pääsy on estetty tai tietoja muutettu. Mikäli tietoturvaloukkaus aiheuttaa todennäköisesti korkean riskin rekisteröidyn oikeuksille tai vapauksille, rekisterinpitäjän tulee ilmoittaa tästä myös rekisteröidylle. (Tietosuoja-asetus 2016/679, 34§.)

Rekisterinpitäjä tai henkilötietojen käsittelijä on vastuussa korvaamaan tietosuoja-asetuksen rikkomisesta henkilölle aiheutuneet aineelliset tai aineettomat vahingot. Rekisterinpitäjä tai henkilötietojen käsittelijä on kuitenkin vapautettava vastuusta siinä tapauksessa, että se pystyy osoittamaan olevansa syytön aiheutuneeseen vahinkoon. (Tietosuoja-asetus 2016/679, 82§.) Säädösten laiminlyönnistä tai rikkomuksesta voi seurata sakkoja maksimissaan 20 miljoonaa euroa tai 4 prosenttia yrityksen liikevaihdosta. Lisäksi seurauksena voi olla myös muita korjaavia toimenpiteitä, kuten henkilötietojen käsittelyn lopettaminen. (Tietosuoja-asetus 2016/679, 83§.)

# 3 KYBERRISKIT JA RISKIENHALLINTA

## 3.1 Erilaisia kyberriskejä ja kyberriskin erityispiirteitä

Ilmonen ym. mukaan "Kaikkeen liiketoimintaan liittyy aina riski; liiketoiminta on pohjimmiltaan riskin ottamista" (Ilmonen, Kallio, Koskinen & Rajamäki, 2016, 10). Liiketoiminnassa riski ei kuitenkaan ole ainoastaan negatiivinen käsite, vaan riskinotolla yritys pyrkii usein saavuttamaan esimerkiksi taloudellista voittoa. Kuten johdannossa jo aiemmin mainittiin*, kyberriskillä* voidaan viitata mihin tahansa informaatioteknologian toimimattomuudesta aiheutuvaan taloudellisen tappion riskiin, liiketoiminnan häiriöön tai maineriskiin (Institute of Risk Management, 2014, 8).

Kyberriskien merkitys kasvaa jatkuvasti ja niistä tulee koko ajan suurempi uhka niin yrityksille kuin yhteiskunnallekin. Kyberriskin käsitteessä yhdistyvät kaksi näkökohtaa: tekninen ja taloudellinen. Kyberriskit koskettavat laajasti monia eri aloja ja ovat globaali uhka, mutta siitä huolimatta niille ei ole vieläkään löydetty yhtenäistä yleisesti hyväksyttyä määritelmää. Tämä voi johtua osittain siitä, että kyberriskit ovat nousseet esiin tieteelliseen keskusteluun melko äskettäin ja osittain siitä, että kyberriskit ovat monimutkaisia ja nopeasti muuttuvia riskejä, joihin on vaikea varautua. (Strupczewski, 2021, 1-2.)

Kyberriskille on olemassa useita erilaisia määritelmiä. Bierner ym. mukaan kyberriski voidaan määritellä kolmen parametrin funktiona. *Vaikutus* ilmaisee, kuinka suuren vahingon riski voi aiheuttaa, *uhka* kertoo riskin todennäköisyydestä ja *haavoittuvuus* kertoo, ovatko olemassa olevat tietoturvatoimenpiteet tehokkaita. (Biener, Eling, & Wirfs, 2015, 134.) National Association of Insurance Commissioners sen sijaan määrittelee kyberriskin käsitteen seuraavasti: Kyberriski kattaa kaikki verkkotoimintaan liittyvät riskit, kuten henkilötietojen tallentamisen internetiin tai verkkotapahtumien suorittamisen, jotka voivat johtaa yrityksen maineen vahingoittumiseen, taloudelliseen tappioon tai liiketoiminnan häiriöön (NAIC, 2018).

*Tietomurrossa* on kyse siitä, että ulkopuolinen taho pääsee käsiksi yrityksen arkaluontoisiin tai suojattuihin tietoihin tahallisesti murtautumalla yrityksen tietokantoihin tai järjestelmiin. Tietomurrossa tiedostoja voidaan joko tarkastella tai levittää ilman lupaa. Tietomurrosta saattaa seurata yritykselle suuria kustannuksia tai

välillisesti esimerkiksi mainehaittaa. Pahimmassa tapauksessa tietomurto saattaa jopa uhata yrityksen toiminnan jatkuvuutta. Tietomurto tapahtuu yleisimmin joko teknologian puutteiden tai käyttäjän puutteellisen toiminnan vuoksi. (Long, Fang & Danfeng, 2017, 1-2.) Vuonna 2016 yksittäisen tietomurron keskimääräiseksi kustannukseksi arvioitiin 2,1-3,8 miljoonaa dollaria (Eling & Schnell, 2016, 477). Suomen rikoslain (19.12.1889/39) luvun 38 kahdeksannen pykälän mukaan tietomurto on rangaistava teko.

*Tietovuoto* eroaa tietomurrosta siten, että siinä kyseessä ei ole varsinaista hyökkäystä, vaan tieto päätyy vahingossa vääriin käsiin. Toisinaan tietovuodolla viitataan myös ulkopuolelta käsin tehtyyn tietomurtoon, mutta tässä tutkimuksessa tietovuodolla viitataan tahattomasta väärinkäytöksestä johtuvaan tietojen vuotamiseen. Tietovuoto saattaa tapahtua esimerkiksi silloin, kun tietoa käsitellään tai säilytetään yrityksessä huolimattomasti tai yrityksen tietoturvatoimet ovat muuten puutteelliset. (Skrop, 2015, 113.) Vaikka tietomurto ja tietovuoto eroavatkin toisistaan syntytapansa mukaan, on molemmissa kyse siitä, että tietoa joutuu vääriin käsiin.

*Kiristyshaittaohjelma* on vahingollinen koodi, jonka rikollinen pyrkii asentamaan yrityksen tietokoneelle, järjestelmiin tai tiedostoihin. Kiristyshaittaohjelman avulla tiedostoista tai järjestelmistä tehdään käyttökelvottomia ja näiden uudelleenavaamisesta yritykseltä kiristetään lunnaita. Kiristyshaittaohjelma saattaa päätyä vakuutusyhtiön järjestelmiin esimerkiksi sähköpostissa olleen liitetiedoston välityksellä. Kiristyshaittaohjelmien varalta on ensisijaisen tärkeää, että vakuutusyhtiöllä on tiedoista varmuuskopiot. (Thakkar, 2015, 123.)

*Palvelunestohyökkäyksellä* tarkoitetaan mitä tahansa sellaista hyökkäystä verkkopalveluun tai järjestelmään, jolla pyritään estämään asiakkaiden pääsy palvelimelle. Palvelunestohyökkäys saattaa ilmetä esimerkiksi siten, että palvelinta ylikuormitetaan tarkoituksellisesti valtavalla määrällä tietoa. (Mahjabin, Xiao, Sun & Jiang, 2017, 2.)

## 3.2 Kyberriskien luokittelu

Riskien luokitteluun voidaan käyttää useita erilaisia malleja. Eräs yleinen tapa luokitella riskejä on jakaa ne neljään riskilajiin: strategisiin riskeihin, operatiivisiin riskeihin, taloudellisiin riskeihin ja vahinkoriskeihin. Vaihtoehtoisesti riskit voidaan jakaa vain kolmeen eri luokkaan, jolloin vahinkoriskit sisällytetään osaksi operatiivisia riskejä.

Riskien luokittelun avulla riskien analysointi ja niiden keskinäisten suhteiden hahmottaminen helpottuu. (Ilmonen ym., 2016, 76-77.)

*Strategiset riskit* vaikuttavat yrityksen strategisten tavoitteiden toteuttamiseen. Tähän kuuluvat esimerkiksi liiketoiminnan kehittymiseen liittyvät riskit, liiketoimintaympäristön riskit ja markkinariski. *Taloudellisiin riskeihin* kuuluvat yrityksen varallisuuteen liittyvät riskit, kuten likviditeettiriskit, korkoriskit ja valuuttariskit. *Operatiivisiin riskeihin* kuuluvat yrityksen sisäisten prosessien, järjestelmien tai ihmisten riittämättömästä tai virheellisestä toiminnasta aiheutuvat riskit. Esimerkiksi informaatioteknologiaan liittyvät riskit ja keskeytysriski kuuluvat tähän kategoriaan. *Vahinkoriskeihin* kuuluvat esimerkiksi työterveys- ja turvallisuusriskit, henkilöstöriskit ja ympäristöriskit. (Ilmonen ym., 2016, 77.)

Taulukko 1 Kyberriskien luokittelu niiden lähteiden mukaan (Cebula & Young, 2010, 3)

| 1. IHMISTEN TOIMINTA | 2. JÄRJESTELMIEN JA TEKNOLOGIOIDEN HÄIRIÖT | 3. EPÄONNISTUNEET SISÄISET PROSESSIT | 4. ULKOISET TEKIJÄT |
|---|---|---|---|
| **1.1 TAHATON** | **2.1 LAITTEISTO** | **3.1. PROSESSIN** | **4.1 KATASTROFIT** |
| 1.1.1 Erehdys | 2.1.1 Kapasiteetti | **SUUNNITTELU JA** | 4.1.1 Sääilmiöt |
| 1.1.2 Virhe | 2.1.2 Suorituskyky | **TOTEUTUS** | 4.1.2 Tulipalot |
| 1.1.3 Laiminlyönti | 2.1.3 Ylläpito | 3.1.1 Prosessin kulku | 4.1.3 Tulvat |
| | 2.1.4 Vanhentuminen | 3.1.2 Prosessin | 4.1.4 Maanjäristykset |
| **1.2 TAHALLINEN** | | dokumentointi | 4.1.5 Levottomuudet |
| 1.2.1 Petos | **2.2 OHJELMISTO** | 3.1.3 Roolit ja vastuu | 4.1.6 Pandemia |
| 1.2.2 Sabotaasi | 2.2.1 Yhteensopivuus | 3.1.4 Ilmoitukset ja | |
| 1.2.3 Varkaus | 2.2.2 Kokoonpanon hallinta | varoitukset | **4.2. LAILLISET KYSYMYKSET** |
| 1.2.4 Ilkivalta | 2.2.3 Muutosten hallinta | 3.1.5 Informaation kulku | 4.2.1 Lakien noudattaminen |
| | 2.2.4 Turvallisuusasetukset | 3.1.6 Ongelmien | 4.2.2 Uusi lainsäädäntö |
| | 2.2.5 Koodauskäytännöt | laajentuminen | 4.2.3 Oikeudenkäynnit |
| | 2.2.6 testaus | 3.1.7 Palvelutasosopimukset | |
| | | 3.1.8 Tehtävien jakaminen | |
| **1.3 TOIMETTOMUUS** | **2.3 JÄRJESTELMÄT** | **3.2 PROSESSIN HALLINTA** | **4.3 LIIKETOIMINTAONGELMAT** |
| 1.3.1 Taidot | 2.3.1 suunnittelu | 3.2.1 Seuranta | 4.3.1 Toimittajan |
| 1.3.2 Tiedot | 2.3.2 Vaatimukset | 3.2.2 Mittarit | epäonnistuminen |
| 1.3.3 Ohjeistus | 2.3.3 Integraatio | 3.2.3 Kausittainen arviointi | 4.3.2 Markkinaolosuhteet |
| 1.3.4 Saatavuus | 2.3.4 Monimutkaisuus | 3.2.4 Prosessin omistajuus | 4.3.3 Taloudelliset olosuhteet |
| | | **3.3 TUKIPROSESSIT** | **4.4 PALVELURIIPPUVUUDET** |
| | | 3.3.1 Rekrytointi | 4.4.1 Hyödykkeet |
| | | 3.3.2 Rahoitus | 4.4.2 Hätäpalvelut |
| | | 3.3.3 Koulutus | 4.4.3 Polttoaine |
| | | 3.3.4 Hankinta | 4.4.4 Kuljetus |

Yksi vakiintunut tapa kyberriskien luokitteluun on jakaa kyberriskit taulukon 1 mukaisesti neljään eri pääluokkaan: ihmisen toimintaan, järjestelmien ja teknologian häiriöihin, epäonnistuneisiin sisäisiin prosesseihin ja ulkoisiin tekijöihin. Luokittelussa ihmisten toiminta tai sen puute voi tahallisesti tai tahattomasti vaikuttaa kyberturvallisuuteen. Järjestelmien tai teknologioiden häiriöllä tarkoitetaan vikaa laitteistossa, ohjelmistossa tai tietojärjestelmässä. Epäonnistuneilla sisäisillä prosesseilla

tarkoitetaan sisäisen liiketoimintaprosessin ongelmia, joilla on vaikutus kyberturvallisuuden kehittämiseen, toteuttamiseen tai ylläpitämiseen. Ulkoisilla tekijöillä tarkoitetaan organisaation hallinnan ulkopuolisia tekijöitä, kuten katastrofeja, juridisia kysymyksiä, liiketoimintakysymyksiä ja palveluntarjoajan riippuvuuksia. Kyberriskit voidaan jakaa pääluokista edelleen useaan alaluokkaan taukukon 1 mukaisesti. (Cebula & Young, 2010, 3-7.)

Taulukossa 1 vapaaehtoisten henkilövakuutusten korvauspalvelun kannalta oleellisia riskien lähteitä ovat etenkin ihmisen toiminta, järjestelmien ja teknologioiden häiriöt sekä epäonnistuneet sisäiset prosessit. Ihmisen toiminnassa inhimilliset virheet ja osaamattomuus altistavat kyberriskeille vapaaehtoisten henkilövakuutusten korvauspalvelussa, jossa korvauskäsittely ja tietojen säilytys on pitkälti sähköisten järjestelmien varassa. Riittävä koulutus ja tiedotus kyberriskeistä ja henkilöstön kyberturvallisuusosaamisen ylläpitäminen on keskeisessä roolissa kyberriskien hallinnassa, ja puutteet tässä sisäisessä koulutusprosessissa saattavat olla osasyynä kyberriskien realisoitumiselle. Koska sähköiset järjestelmät ovat oleellinen osa sekä korvauskäsittelyä että asiakkaan vuorovaikutusta korvauspalvelun kanssa, ovat järjestelmien ja teknologioiden häiriöt korvauspalvelun toiminnalle suuri uhka.

## 3.3 Kyberriskien hallinta

Vakuutusalan riskienhallinta poikkeaa muun yritystoiminnan riskienhallinnasta, sillä vakuutusalaa koskee tyypillisesti voimakas sääntely. Vakuutusalan riskienhallinnan haasteita lisää myös markkinoiden kompleksisuus, sillä vakuutusyhtiöiden toiminta-alue monimutkaistuu jatkuvasti. Ala kehittyy nopeasti ja kilpailukyvyn säilyttämiseksi vakuutusyhtiöiden on poistettava käytöstä vanhoja toimintoja ja teknologioita ja omaksuttava nopeasti uusia toimintatapoja. (Kivisaari & Kahola, 2017, 90-91.) Teknologian kehitys ja nopeasti muuttuva ympäristö, sekä vakuutusalan tietointensiivisyys tekevätkin vakuutussektorista alttiin kyberriskeille. Tämä luo myös riskienhallinnalle poikkeuksellisia vaatimuksia.

*Riskienhallinta* on suunniteltu ja jäsennelty prosessi, jonka tarkoituksena on tunnistaa, luokitella ja arvioida riskejä, sekä hallita ja kontrolloida niitä. Riskienhallintaa tulisi toteuttaa niin, että siihen käytetyt resurssit, kuten aika ja raha olisivat tasapainossa siitä saatavien hyötyjen kanssa. Riskienhallinta on jatkuva prosessi, jota toteutetaan projektin alusta loppuun saakka. Jotta riskienhallinnasta saataisiin irti täysi potentiaali, tulisi sitä

toteuttaa jo projektien aikaisimmilla tasoilla, eli käytännössä jo suunnitteluvaiheessa. Riskienhallinnan tarkoituksena ei ole poistaa kaikkia yrityksen kohtaamia riskejä, vaan tunnistaa ja arvioida niitä ja varautua kuhunkin riskiin niiden vaatimalla tavalla. (Srinivas, 2019, 3.)

Kyberriskien hallinnan toteuttamisessa oleellista on riskianalyysi, jossa arvioidaan jokaiselle kyberriskille todennäköisyys ja vakavuus, sekä määritellään kyseiselle riskille sopivat riskienhallintakeinot. Riskienhallintakeinoihin kuuluvat tyypillisesti riskin välttäminen, riskin pienentäminen, riskin pitäminen ja riskin siirtäminen. Kun riskit on arvioitu ja riskienhallintastrategia on tehty, tulee riskienhallintatoimenpiteitä seurata ja raportoida tarkasti. Samalla riskienhallinnan toimivuutta tulee arvioida ja kehittää tarpeen mukaan. (Ilmonen ym., 2016, 99.)

Rohmeyer ja Bayuk ovat listanneet teoksessaan "Financial Cybersecurity Risk Management: Leadership Perspectives and Guidance for Systems and Institutions" riskienhallintakeinoja erilaisille kyberriskeille. Myös heidän mukaansa tyypillisimmät riskienhallintakeinot kyberriskeille ovat karkeasti luokiteltuna riskin välttäminen, pienentäminen, siirtäminen ja pitäminen. Rohmeyerin ja Bayukin mukaan mahdollisesti vältettävissä oleva riski on esimerkiksi vanhan teknologian kanssa kamppaileminen. Vaikka uudet järjestelmät voivat tuoda mukanaan uusia riskejä, voi vanhojen järjestelmien kanssa jatkuva kamppailu itse asiassa olla riskialttiimpi tai kalliimpi vaihtoehto kuin uuteen nykyteknologian tasolla valmiiksi toimivaan järjestelmään siirtyminen. (Rohmeyer & Bayuk, 2019, 106.)

Joitakin kyberriskejä, kuten erilaisten järjestelmien haavoittuvuuksia voidaan pienentää esimerkiksi palomuureilla tai järjestelmien kovennuksilla. Järjestelmän kovennuksella tarkoitetaan järjestelmän toiminnan rajaamista niin, että siitä poistetaan kaikki ylimääräisten toimintojen mahdollisuudet. Lisäksi järjestelmien haavoittuvuuksista seuraavia kyberriskejä voidaan hallita monivaiheisella tunnistautumisella, käyttöoikeuksien rajaamisella, haittaohjelmasuodattimilla, virustorjuntajärjestelmillä, suojatulla yksityisellä verkkoyhteydellä, järjestelmien haavoittuvuuksien kartoituksella, sekä kiintolevyjen, verkon ja tietojen salaamisella. (Rohmeyer & Bayuk, 2019, 107-108.)

Kyberriski voidaan siirtää esimerkiksi niissä tapauksissa, että omasta yhtiöstä ei löydy riittävästi osaamista sähköisten palveluiden tuottamiseen ja koodaamiseen. Tämä

tarkoittaa käytännössä ulkoisten palveluntuottajien hyödyntämistä, jolloin vastuu kyberriskistä siirretään sopimuksellisesti tälle kolmannelle osapuolelle. Toinen vaihtoehto kyberriskin siirtämiselle on kybervakuutus, jonka yritys voi ottaa sen varalta, että se joutuu esimerkiksi vakavan tietomurron kohteeksi. Kybervakuutuksesta on mahdollista saada korvausta esimerkiksi liiketoiminnan katkoksista aiheutuneista kuluista, järjestelmien kunnostuksen kustannuksista ja vahingonkorvausmenoista. (Rohmeyer & Bayuk, 2019, 111-112.)

Kyberriskit, jotka eivät ole todennäköisyydeltään tai suuruusluokaltaan kovin merkittäviä, voidaan mahdollisesti pitää itsellä ilman erillisiä toimenpiteitä. Kaikkia riskejä tulee kuitenkin seurata, sillä etenkin kyberriskien tapauksessa nämä saattavat muuttaa nopeasti muotoaan vakavammiksi. Joissain tapauksissa riskin pitämisen syynä voi olla se, ettei sille käytännössä löydy selkeitä riskienhallintatoimenpiteitä. Voi myös olla, että riskin vaikutukset arvioidaan sen verran pieniksi, että tulisi yritykselle kalliimmaksi tehdä sen eteen riskienhallintaatoimenpiteitä. On syytä muistaa, että juuri kyberriskin nopeasti muuttuvan luonteen ja epäselvien vaikutusten vuoksi kyberriskin hallitsematta jättäminen on kuitenkin aina itsessään riski. (Rohmeyer & Bayuk, 2019, 114.)

Nykyään vakuutusyhtiöissä on pitkiä toimitusketjuja, joissa kyberriskien hallinta on haastavaa. On vaikeaa hahmottaa riskejä, kun mukana on useita osapuolia, joiden riskit saattavat olla salakavalasti yhteydessä toisiinsa. Jonkin pieneltä vaikuttavan kyberriskin salliminen tällaisessa riskialttiissa toimitusketjussa saattaa realisoituessaan aiheuttaa arvaamattomia seurauksia ja eskaloitua paljon suuremmaksi, kuin olisi osattu odottaa. Esimerkiksi yhden toimitusketjun jäsenen pääsy vakuutusyhtiön sisäverkkoon saattaa johtaa siihen, että rikollinen pääsee hyökkäämään yrityksen järjestelmiin tämän ulkopuolisen toimittajan tai alihankkijan kautta. (Rohmeyer & Bayuk, 2019, 114.)

# 4 KYBERRISKIT VAPAAEHTOISTEN HENKILÖVAKUUTUSTEN KORVAUSPALVELUSSA

## 4.1 Aineiston kuvaus

Tutkimuksen empiirinen aineisto kerättiin kahden asiantuntijahaastattelun avulla. Haastattelut toteutettiin puolistrukturoituina teemahaastatteluina Microsoft Teams -videopuheluiden välityksellä keväällä 2021. Haastateltavat valittiin tutkimukseen, koska heillä on kattavasti kokemusta ja tietoa kyberriskeistä ja näiden parissa työskentelystä. Haastatteluissa keskityttiin tarkoituksenmukaisesti kyberriskeihin ja kyberriskien hallintaan vakuutusyhtiön ja korvauspalvelun näkökulmasta.

Molemmat haastateltavista toimivat asiantuntijatehtävissä kyberturvallisuuden parissa. Haastateltavien nimiä tai yksilöiviä tietoja ei mainita tässä tutkimuksessa tietojen arkaluontoisuuden vuoksi. Myös case -vakuutusyhtiö esitetään tutkimuksessa anonyymina, sillä tutkimukseen on saatu käytettäväksi sen kyberturvallisuuden hallintaan liittyviä materiaaleja, joiden käsittelyn yhteydessä yhtiö ei tahdo nimeään mainittavan. Tutkimuksen seuraamisen helpottamiseksi haastateltavat on nimetty kirjaimin A ja B.

Haastateltava A toimii tietoturvajohtajana tutkimuksen case -vakuutusyhtiössä. Hänellä on kaupallinen pohjakoulutus ja yli kymmenen vuoden kokemus tietoturvallisuuden ja kyberriskien parissa työskentelystä. Hän on saanut tunnustusta muun muassa kyberriskeihin liittyvistä innovaatioista ja ollut kehittämässä yhtiön tietoturvallisuutta monipuolisesti. Haastateltava A:lla on siis hyvin laaja näkemys kyberriskeistä ja näiden hallinnasta vakuutusyhtiössä.

Haastateltava B toimii johtavana asiantuntijana suomalaisessa organisaatiossa. Hänellä on noin kahdenkymmenen vuoden kokemus kyberturvallisuudesta. Taustalla hänellä on juristin koulutus. Lisäksi hänellä on tietoturvaosaamisesta CISM (Certified Information Security Manager) ja CISSP (Certified Information Systems Security Professional) sertifioinnit. Työkokemusta hänellä on niin valtion viroista kuin finanssialan yrityksistäkin kyberturvallisuuden parissa. Myös haastateltava B:llä on siis laaja tietämys kyberriskeistä ja näiden hallinnasta erityisesti finanssialan yrityksissä.

Teemahaastattelulle on tyypillistä, että kysymysten järjestys saattaa vaihdella eri haastateltavien kesken, ja että haastattelun joihinkin aiheisiin voidaan perehtyä

syvällisestikin. Lisäksi aiheesta saattaa nousta haastattelussa esiin myös muita seikkoja. (Hirsjärvi & Hurme, 2015. 47-50.) Teemahaastattelurunko oli sama molemmille haastateltaville. Haastattelurunko koostui kahdesta eri teemasta. Ensimmäinen teema käsitteli kyberriskejä vakuutusyhtiössä ja korvauspalvelussa ja toinen kyberriskien hallintaa vakuutusyhtiössä. Haastattelukysymysten avulla etsittiin vastauksia tutkimukselle asetettuihin tutkimuskysymyksiin, eli millaisia kyberriskejä vapaaehtoisten henkilövakuutusten korvauspalvelussa on, ja miten korvauspalvelussa tunnistettuja kyberriskejä voidaan hallita.

Aineiston analyysissa pyritään hyödyntämään teorian luomaa pohjaa ja kvalitatiiviselle tutkimukselle ominaisesti ymmärtämään tutkittavaa ilmiötä. Teoria on ollut osana haastattelukysymysten luomisessa, mikä tukee hyvin teorian ja empirian yhdistämistä tutkimuksessa. Haastateltavat vastasivat haastattelurungon kysymyksiin kattavasti, mutta keskustelu haastattelutilanteessa oli kuitenkin teemahaastattelulle ominaisesti sen verran vapaata, että esiin nousi kattavasti myös sellaisia seikkoja ja näkökulmia, joita ei ollut teemahaastattelurungossa otettu huomioon.

Haastattelurunkoja (Liite 1) tehtiin yhteensä yksi. Haastattelut suoritettiin yksilöhaastatteluina videoyhteyden välityksellä. Haastatteluissa painotukset eri teemojen ja kysymysten käsittelyissä vaihtelivat sen mukaan, paljonko tietämystä haastateltavalla aiheesta oli. Haastattelut tallennettiin ja litteroitiin sähköisesti sanatarkasti tekstimuotoon. Litteroinnin jälkeen aineistoja vertailtiin keskenään ja pyrittiin löytämään näistä yhtäläisyyksiä ja eroavaisuuksia. Seuraavassa alaluvussa analysoidaan haastatteluista kerättyä empiiristä aineistoa. Aineiston käsittely on jäsennelty selkeyden vuoksi haastattelurungon teemoja mukaillen.

## 4.2 Kyberriskit vapaaehtoisten henkilövakuutusten korvauspalvelussa

### 4.2.1 Kyberriskien syntymekanismit ja syyt

Teemahaastattelun ensimmäinen kysymys keskittyi siihen, kuinka suurena uhkana kyberriskit koetaan nyt ja tulevaisuudessa. Molemmat haastateltavat olivat yksimielisiä siitä, että kyberristit ovat tällä hetkellä vakuutusyhtiössä hyvin merkittävä riski. Haastateltava A:n mukaan kyberriskien merkityksellisyys on kasvamassa, ja etenkin viime kuukausien tapahtumat, kuten koronavirus ja Vastaamon tietomurto ovat lisänneet

kyberturvallisuuden näkyvyyttä entisestään. Haastateltava A painottaa myös, että tulevaisuudessa kyberriskit ovat osana myös sellaisilla osa-alueilla, joilla niihin ei ole aikaisemmin törmätty. Hänen mukaansa kyberilmiön ymmärtämisen tuleekin olla läsnä jokaisen tekemisessä, jotta kyberriskejä voidaan tunnistaa ja ennaltaehkäistä myös tulevaisuudessa.

Haastateltava B on sitä mieltä, että kyberriskit ovat tällä hetkellä yksi ehdottomasti merkittävimpiä riskejä tietointensiivisillä toimialoilla, kuten vakuutussektorilla. Hänen mukaansa kyberriskit ovat melko geneerisiä, ja siten vakuutusyhtiö kokonaisuudessaan ja sen korvauspalvelu kohtaavat pitkälti samanlaisia kyberriskejä. Haastateltava B:n mukaan kyberriskeistä tekee kasvavan uhan se, että riippuvuus tiedosta ja teknologiasta kasvaa jatkuvasti, kun palveluketjut, arvoketjut ja hankintaketjut digitalisoituvat ja tulee uutta teknologiaa, kuten esimerkiksi 5G ja tekoäly. ”Kaikki alkaa olla toisiinsa paitsi ristiin kytkeytynyttä myös ristiin riippuvaista, ja se lisää ehdottomasti riskien määrää”, hän sanoo. Haastateltava B:n mukaan kyberriskit jatkavat tulevaisuudessa kasvuaan ja monet sellaisistakin riskeistä, jotka ovat aikaisemmin olleet reaalimaailman riskejä, siirtyvät kybermaailmaan.

Molemmat haastateltavat mainitsevat merkittävinä tunnistettuina kyberriskeinä vakuutusyhtiössä ja korvauspalvelussa huijaus- ja tietojenkalastelusähköpostit, sekä esimerkiksi Microsoftin IT tuen nimissä tehdyt huijaussoitot. Suureksi kyberriskiksi koettiin myös sisäiset uhat ja väärinkäytökset, joissa yrityksen työntekijä tahallisesti tai huolimattomuuttaan käyttää järjestelmiä väärin ja aiheuttaa näin esimerkiksi tietovuodon tai häiriön järjestelmien toimintaan. Haastateltava A nosti lisäksi esiin myös palveluiden ja järjestelmien haavoittuvuudet, joita havaitaan ja korjataan case -vakuutusyhtiössä jatkuvasti. Mikäli näiden havainnointi tai korjaaminen laiminlyötäisiin, voisi seurauksena olla katkoksia ja häiriöitä työnteossa. Jos rikollinen tahon havaitsee haavoittuvuuden järjestelmässä, voi pahimmassa tapauksessa seurauksena olla tietomurto yrityksen järjestelmiin.

Erityisesti korvauspalveluun liittyvänä riskinä haastateltava A nosti esiin asiakkaan tai asiakkaaksi tekeytyvän rikollisen tahon, joka voisi esimerkiksi liitetiedoston mukana saada ujutettua yrityksen järjestelmään kiristyshaittaohjelman. Tämän seurauksena kaikki työasemassa olevat tiedostot, verkkolevyt ja ohjelmat voitaisiin kryptata sellaiseen muotoon, ettei niitä saisi auki kuin maksamalla lunnaat tai palauttamalla nämä

varmuuskopioista. Toinen korvauspalveluita koskeva kyberriski on haastateltava A:n mukaan se, että hakkeri pääsee yrityksen sisäverkkoon ja onnistuu esimerkiksi muuttamaan asiakkaiden tilinumeroita niin, että korvaukset maksetaankin asiakkaiden sijaan rikollisen tilille.

Haastateltava B nosti esiin myös palvelunestohyökkäykset, joissa yritetään valtavalla tietomäärällä kuormittamalla tai muilla tavoin estää asiakkaiden pääsy palveluihin. Lisäksi hän sanoi, että yksi merkittävä ja kasvava riski ovat pitkiin alihankkijaketjuihin liittyvät toimitusketjuhyökkäykset. Ulkoiset palveluntuottajat tarvitsevat usein pääsyn yrityksen sisäverkkoon ja järjestelmiin. Seurauksena myös rikolliset voivat päästä näihin yrityksen palveluntuottajien kautta. Palveluntuottajien suojaukset eivät välttämättä ole samalla tasolla kuin vakuutusyhtiössä, joten potentiaali kyberriskille on suuri.

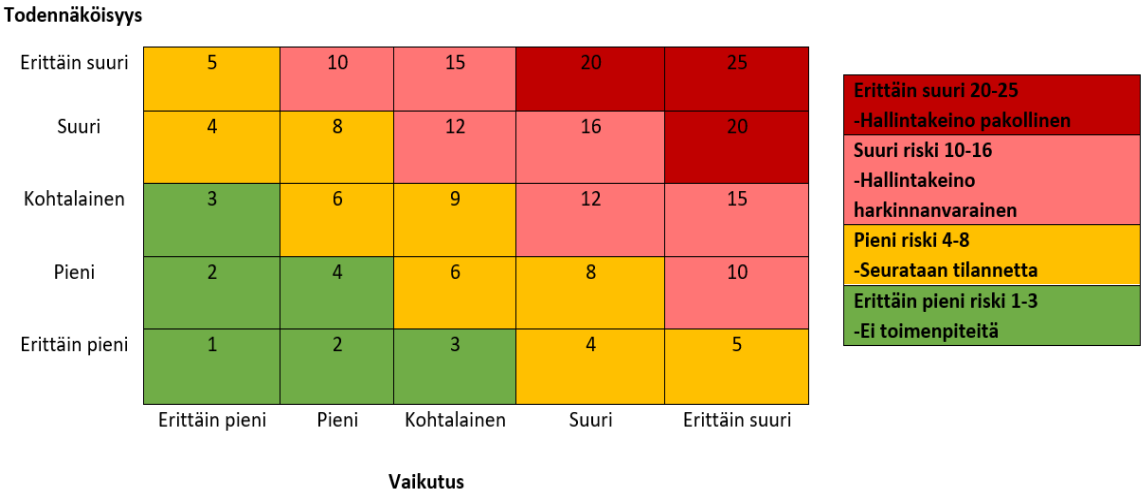
### 4.2.2 Kyberriskien arviointi ja priorisointi

Kyberriskien arvioinnissa haastateltavien näkemykset erosivat toisistaan jonkin verran. Haastateltava A kertoi haastattelussa kyberriskien arvioinnista case -vakuutusyhtiön näkökulmasta. Kyberriskejä seurataan case -vakuutusyhtiössä arvioimalla jatkuvasti tuotannossa olevia sovelluksia ja järjestelmiä ja niiden turvallisuutta, sekä erilaisten palveluntuottajien toimintaa. Yhtiössä koodaus on kokonaan ulkoistettu, joten ulkoisten ICT -palveluntuottajien toiminnan seuranta, valvonta ja arviointi ovat tärkeä osa kyberriskien hallintaprosessia.

Kyberturvallisuus koostuu haastateltava A:n mukaan luottamuksellisuudesta, eheydestä ja saatavuudesta. Kyberriskien hallintaa ja arviointia toteutetaan vakuutusyhtiössä näiden kolmen käsitteen kautta. Haastateltava A otti tästä esimerkiksi vakuutusyhtiön asiakastietojärjestelmän riskien arvioinnin. Järjestelmälle tehdään riskikartoitus, jossa pohditaan sen sisältämiä ja kohtaamia uhkia näiden kolmen käsitteen kautta. Kyseinen asiakastietojärjestelmä on keskeinen osa case -vakuutusyhtiön korvauskäsittelyä. Uhkana järjestelmässä on havaittu, että sen käyttö joko estyy kokonaan tai hidastuu, jolloin asiakkaita ei pystytä palvelemaan. Tähän voi olla syynä esimerkiksi virhe järjestelmän omassa toiminnassa tai koodauksessa, tai ulkopuolelta tullut hyökkäys. Seurauksena järjestelmän käyttö joka tapauksessa estyy, ja samalla estyy myös korvauskäsittely ja asiakkaiden palvelu. Tässä on kyse riskistä asiakastietojärjestelmän saatavuudessa.

Eheys liittyy järjestelmän datan oikeellisuuteen. Uhkana järjestelmän eheydessä on havaittu, että asiakastietojärjestelmän sisältämät tiedot ovat osittain ristiriidassa niiden järjestelmien kanssa, joista se hakee tietoa. Tällainen haavoittuvuus tiedoissa voi syntyä virheestä jossain vaiheessa järjestelmien välistä kommunikaatiota. Luottamuksellisuutta pidetään haastateltava A:n mukaan kyberturvallisuuden tärkeimpänä elementtinä, koska siihen liittyvät keskeisesti tietoturva ja tietosuoja. Esimerkiksi liian laajat työntekijöiden käyttöoikeudet ovat haavoittuvuus. Haastateltava A:n mukaan on tärkeää varmistaa, että työntekijöillä on käyttöoikeudet vain niihin järjestelmien osiin, joita he todella tarvitsevat työssään. Muuten seurauksena saattaa olla esimerkiksi käyttäjän huolimattomuudesta tai osaamattomuudesta johtuva virhe, tai pahimmassa tapauksessa tahallinen väärinkäyttö.

Taulukko 2 Riskimatriisi (Mukaillen Case -vakuutusyhtiö, 2021)




Haastateltava A kertoo, että kyberriskejä arvioidaan case- vakuutusyhtiössä ”Heat Mapin”, eli riskimatriisin avulla. Taulukossa 2 on esitetty riskimatriisi case - vakuutusyhtiöltä saatuja materiaaleja mukaillen. Riskit sijoittuvat riskimatriisiin sen mukaan, mikä niiden toteutumisen todennäköisyys ja vaikutus on. Riskeille muodostetaan niiden todennäköisyyden ja vaikutuksen perusteella riskiluku, joka kuvastaa riskin suuruutta. Taulukon oikeassa yläkulmassa punaisella alueella ovat kaikkein vakavimmat ja todennäköisimmät riskit, joille riskienhallintakeino on pakollinen. Vasemmassa alakulmassa taas on vihreä alue, jolla olevat riskit eivät välttämättä vaadi riskienhallintatoimenpiteitä.

Haastateltava B:n mukaan kyberriskien arviointi on edelleen lähinnä kvalitatiivista. Hän ei pidä riskien arvioimista todennäköisyyden ja vakavuuden lukujen perusteella luotettavana, koska hänen näkemyksensä mukaan voi olla hankalaa antaa vahingon vaikutukselle tai todennäköisyydelle luotettavia arvoa. Myös haastateltava B nostaa kyberturvallisuuden tärkeimpinä osa-alueina esiin samat elementit, jotka haastateltava A mainitsi: Luottamuksellisuuden, eheyden ja saatavuuden.

Lisäksi haastateltava B kertoo, että kyberriskien arvioinnissa on tärkeää pohtia riskin kokonaiskustannusta. Kyberriskin kokonaiskustannus muodostuu ensinnäkin riskienhallinnan aiheuttamista kustannuksista. Kustannuksia saattaa syntyä myös suoraan kyberrikoksen, esimerkiksi tietomurron seurauksena, kun menetetään tietoja tai rahaa. Välittömien kulujen lisäksi haastateltava B nostaa esiin välilliset kustannukset: ”Yrityksen kilpailukyky tai maine saattaa kärsiä ja sen toiminta saattaa hidastua pitkäksikin ajaksi. Lisäksi tilanteen hoitaminen tietomurtoa edeltäneelle tasolle on kallista ja vie paljon työtunteja, jotka ovat pois jostain muusta työn tekemistä.”

Haastateltava B painottaa, että työlläkin on vaihtoehtoiskustannus, joka tulisi huomioida kyberriskejä arvioidessa. Vaikka tietoja ei katoaisi haittaohjelman seurauksena, kuluu tilanteen selvitykseen ja haittaohjelman poistamiseen silti paljon resursseja. Jos asiakkaiden henkilötietoja on päässyt vääriin käsiin, joudutaan tietovuodon uhreille mahdollisesti maksamaan korvauksia ja viranomaisille seuraamusmaksuja. Nämä välilliset kustannukset aliarvioidaan haastateltava B:n mukaan usein, vaikka ne saatavat todellisuudessa olla kaikkein suurin kulkuerä.

### 4.2.3 Kyberriskien seuraukset ja vastuut

Kyberriskien seurauksiin liittyen molemmat haastateltavat nostivat esiin syksyllä 2020 sattuneen Psykoterapiakeskus Vastaamon tietomurron, jonka seurauksena yritys ajautui konkurssiin. Tällä he havainnollistivat, että kyberriskien seuraukset todella voivat jopa uhata yrityksen toiminnan jatkuvuutta. Haastateltava A painotti, että nimenomaan yrityksen maineella on suuri merkitys sen toiminnan jatkuvuuden kannalta. Esimerkiksi tietomurto voi helposti horjuttaa yrityksen mainetta ja asiakkaiden luottamausta yritykseen pitkäksikin aikaa.

Haastateltava A mainitsi kyberriskien seuraukseksi myös suuret lunnaat, joita yritykset saattavat joutua maksamaan kiristäjille. Mikäli yrityksen järjestelmään saadaan asennettua kiristyshaittaohjelma, eikä yrityksellä ole tiedoista varmuuskopioita, voi lunnaiden maksaminen olla ainoa ratkaisu selvitä tilanteesta. Lisäksi hän nosti esiin erilaiset vahingonkorvausvastuut, joita kyberriskeistä voi seurata. Jos esimerkiksi tietosuojavaltuutettu havaitsee, että yrityksen kyberturvallisuus ei ole hyvän tavan mukaista, voi seurauksena aiheutua GDPR:n tietosuoja-asetuksen mukaisesti enintään neljän prosentin sanktio yrityksen globaalista liikevaihdosta.

Haastateltava B nostaa tärkeimpänä seikkana esiin, että kyberriskit ovat epälineaarisia. ”Pienestä työntekijän virheestä ei välttämättä seuraa pieni vahinko, vaan seuraukset voivat olla hyvinkin merkittäviä. Toisaalta suurikin vahinko saatetaan saada nopeasti hallintaan ja näin välttyä seurauksilta”, hän sanoo. Haastateltava B:n mukaan kyberriskien kohdalla riskin todellisen suuruuden arvioiminen voi olla vaikeaa, sillä kyberriskeillä voi olla paljon välillisiä seurauksia ja pitkän aikavälin vaikutuksia.

Molemmat haastateltavat ovat yksimielisiä siitä, että sopimuksilla on vastuun jakamisessa tärkeä rooli. Haastateltava A:n mukaan case -vakuutusyhtiössä asiakkaiden tietoja käsitellään paljon ulkopuolisissa yrityksissä ja vastuuta on pyritty siirtämään sopimuksellisesti tietoturva- ja tietosuojaliitteiden avulla heille. Näin tietoturvaloukkauksen sattuessa sanktiot eivät tule maksettavaksi vakuutusyhtiölle, vaan tietojen käsittelystä vastuussa olevalle yhteistyökumppanille. Haastateltava B painottaa, että vaikka työn tekemistä voikin ulkoistaa, viimekätistä vastuuta ei voida. Jos vakuutusyhtiön alihankkija tekee virheen ja siitä aiheutuu ongelmia asiakkaille, kohdistuvat seuraukset kuitenkin aina ensin vakuutusyhtiöön. Vasta tämän jälkeen selvitetään, voidaanko alihankkijalta saada tapahtuneesta korvauksia.

## 4.3 Kyberriskien hallintakeinot

Haastattelun toinen teema keskittyi tunnistettujen kyberriskien hallintaan vakuutusyhtiössä. Haastateltava A kertoi riskienhallintakeinoista case -vakuutusyhtiön näkökulmasta. Hän nosti tärkeimmäksi riskienhallintakeinoksi uhkamallinnukset, joita tehdään case -vakuutusyhtiössä jopa sata vuodessa. Uhkamallinnuksissa tunnistetaan case -vakuutusyhtiötä uhkaavia kyberriskejä, arvioidaan näiden todennäköisyyttä ja vaikutusta ja suunnitellaan näille riskienhallintakeinoja.

Haastateltava A mainitsi riskienhallintakeinoina myös työasemien ja järjestelmien maksimitasoisen suojauksen teknologian avulla ja tietoturvavalvomon, joka tarkkailee vakuutusyhtiön kohtaamia kyberriskejä jatkuvasti ja on valmiina reagoimaan näihin lyhyellä varoitusajalla. Lisäksi hän nosti esiin ”Security Coach” -mallin, jonka avulla uusien tuotteiden ja järjestelmien kehitystä valvotaan koko niiden kehitysprosessin ajan. Tuotteiden valvonta jo kehitysprosessin aikana on haastateltava A:n mukaan tärkeä osa kyberriskien hallintaa, koska on paljon työläämpää ja kalliimpaa korjata järjestelmien virheitä ja vasta siinä vaiheessa, kun järjestelmät on jo kehitetty valmiiksi.

Haastateltava B:n mukaan kyberriskien hallinta lähtee liikkeelle siitä, että yritys tuntee oman infrastruktuurinsa ja sen toiminnan hyvin. Kyberriskien hallintakeinona hän mainitsee tehtävien eriyttämisen. Tällä hän tarkoittaa, että kriittiset työketjut tulisi pilkkoa niin, ettei yksi ihminen pysty hoitamaan kaikkea alusta loppuun samoilla valtuuksilla. Hän painottaa, että käyttövaltuudet ovat todella tärkeitä kyberriskien hallinnassa. Käyttövaltuuksien tulisi aina vastata henkilöiden työtehtäviä, eikä ylimääräisiä valtuuksia tulisi antaa kenellekään sellaisiin järjestelmiin, palveluihin tai ohjelmistoihin, joihin heillä ei ole tarpeen päästä.

Haastateltava B otti riskienhallintakeinona esiin myös järjestelmien koventamisen. Tällä hän tarkoittaa, että järjestelmien toiminta tulisi rajata ainoastaan siihen mihin niitä käytetään ja estää kaikki ylimääräiset toiminnot. Haastateltava B:n mukaan ulkoistamiseen ja hankintaan liittyvät menettelyt tulisi arvioida erityisen huolellisesti. Ulkoistamisprosessissa tulisi aina pohtia, että vaikka jokin asia voitaisiin ulkoistaa, kannattaako tämä. Hänen mielestään yrityksen kannattaa elää strategiansa mukaisesti ja pitää itsellään ne järjestelmät ja toiminnot, joissa sen tulevaisuuden kilpailuedun nähdään olevan.

Haastateltava B:n mukaan tärkein termi kyberriskien hallinnassa on *defense in depth*, eli puolustuksen syvyys. Tällä hän tarkoittaa, että kriittiset toiminnot ja järjestelmät eivät saa olla vain yhden suojauksen varassa. Jos jokin suojaus murretaan, sen takaa pitäisi löytyä vielä vähintään toinen suojaus. Moninkertaisella suojauksella pystytään mahdollisesti pysäyttämään kyberhyökkäys tai ainakin hidastamaan sen etenemistä ja samalla antamaan aikaa vastatoimenpiteisiin.

Molemmat haastateltavat olivat sitä mieltä, että yksittäisen työntekijän rooli kyberriskeiltä suojautumisessa on todella tärkeä. Haastateltava A:n mukaan kyberturvallisuus on parhaimmillaan silloin, kun ihminen ja teknologia ovat sopivassa suhteessa keskenään. Hänen mukaansa kyberriskien hallinnassa korostuu työntekijöiden koulutus ja jatkuva ajan tasalla pitäminen, sekä tiedottaminen kyberriskeistä. Myös haastateltava B on sitä mieltä, että kyberturvallisuus on yhteispeliä tekniikan ja ihmisten kanssa. Hän sanoo, että työntekijä kuvataan usein heikoimpana osapuolena kyberturvallisuudessa, mutta siitä huolimatta tähän mennessä juuri ihmiset ovat pystyneet torjumaan ja havaitsemaan kohtaamiaan uhkia hyvin. Haastateltava B:n mukaan myös kohdennetut hyökkäykset ja kalastelut, kuten huijauslaskut ja toimitusjohtajahuijaukset lisääntyvät koko ajan ja muuttuvat yhä taitavammiksi, ja tämä tekee yksittäisen työntekijän roolista kyberuhkien havaitsemisessa yhä tärkeämmän.

Lopuksi haastateltavilta kysyttiin, mitä kyberriskejä ei pystytä hallitsemaan. Molemmat haastateltavat mainitsivat, että kyberriskien hallinta aiheuttaa vakuutusyhtiölle suuria kustannuksia. Suurten kustannusten vuoksi joitain kyberriskejä ei pystytä hallitsemaan tai niiden hallintaan ei pystytä panostamaan riittävästi. Haastateltava A:n mukaan hallitsemattomissa olevia kyberriskejä ovat erilaiset neljännen teollisen vallankumouksen mukanaan tuomat uhat, kuten 5G -teknologia, tekoäly, pilvilaskenta, kryptovaluutat ja erilaiset lohkoketjut. Molemmat haastateltavat ottivat esiin myös Microsoftin valtavat pilvialustat, joiden taustalla tapahtuvia uhkia ja haavoittuvuuksia on käytännössä mahdotonta hallita. ”Näitä tulevaisuuden uhkia voidaan vain seurata ja yrittää jatkuvasti rakentaa jotain niiden ympärille, etteivät kyberriskit pääsisi eskaloitumaan näissä ympäristöissä”, haastateltava A sanoo.

## 4.4 Tutkimustulokset

Tässä alaluvussa esitellään tutkimuksen keskeiset tutkimustulokset. Tutkimusaineisto analysoitiin huolellisesti ja ongelmalähtöisesti. Empiiristä aineistoa peilattiin analyysissa tutkielman taustateoriaan ja tehtiin päätelmiä tämän pohjalta. Tutkimustulokset koottiin yhtenäiseksi kokonaisuudeksi taulukkoon (Taulukko 3). Taulukon kokoamisessa on sovellettu taustateoriassa esiteltyä Cebulan & Youngin (2010) oppien mukaista kyberriskien luokittelua.

Taulukko 3 Kyberriskien luokittelu korvauspalvelussa

| Kyberriskin syntylähde | Riski | Seuraukset | Hallintakeinot |
|---|---|---|---|
| **Ihmisten toiminta** | Tahaton virhe (Vahinko, osaamisen puute tai erehdys) | Tietojen joutuminen vääriin käsiin, järjestelmien vioittuminen, korjauskustannukset, mainehaitta | Käyttöoikeuksien rajaaminen minimiin, kyberosaamisen kehittäminen ja ylläpitäminen, ohjeistus, haittaohjelmasuodattimet, järjestelmien koventaminen |
| | Tahallinen väärinkäytös | | |
| **Järjestelmien haavoittuvuudet** | Virheet koodauksessa tai aukko järjestelmän suojauksessa | Järjestelmien käyttö ja korvauskäsittely estyy, syntyy korjauskustannuksia, asiakkaiden luottamus järjestelmiin kärsii, tietoja voi joutua vääriin käsiin, mainehaitta | Järjestelmien ja tietoteknisten suojamuurien jatkuva seuranta, kehittäminen ja korjaaminen, tietoturvavalvomo, järjestelmien koventaminen, virustorjuntaohjelmat ja haittaohjelmasuodattimet, varmuuskopiot |
| | Puutteellinen seuranta/ havainnointi | | |
| **Ulkoiset tekijät** | Kiristyshaittaohjelma | Asiakaspalvelu estyy, työnteko pysähtyy, korjauskustannukset, mainehaitta, verkkopalvelun käyttö vähenee | Virustorjuntaohjelmat, haittaohjelmasuodattimet, varmuuskopiot, tuplasuojaukset järjestelmissä, tietoturvavalvomo, jatkuva havainnointi ja ennakointi, uhkamallinnukset |
| | Palvelunestohyökkäys | Lunnaat, tietojen tuhoutuminen tai joutuminen vääriin käsiin, mainehaitta, korjauskustannukset, vahingonkorvausmenot ja muut välilliset kustannukset | |
| | Tietomurto | | |

Taulukkoon 3 on koottu case -vakuutusyhtiön vapaaehtoisten henkilövakuutusten korvauspalvelun kohtaamat keskeisimmät kyberriskit, näiden seuraukset ja hallintakeinot. Kyberriskit on luokiteltu taulukossa niiden syntylähteiden mukaan ihmisen toimintaan, järjestelmien haavoittuvuuksiin ja ulkoisiin tekijöihin. Ihmisen toiminnasta aiheutuvat kyberriskit on jaettu tahattomiin virheisiin ja tahallisiin väärinkäytöksiin. Seurauksena ihmisen toiminnasta voi aiheutua tietojen joutumista vääriin käsiin, järjestelmien vioittumista ja välillisenä seurauksena esimerkiksi korjauskustannuksia sekä mainehaittaa.

Korvauspalvelun työntekijällä on jo valmiiksi pääsy yrityksen sisäverkkoon, eli hän on jo ohittanut yrityksen tärkeimmän suojamuurin. Riskit, joita sähköiset järjestelmät eivät pysty seulomaan, siirtyvät korvauspalvelussa korvauskäsittelijän vastuulle. Työntekijöiden kyberturvallisuusosaamiseen, tietotekniseen osaamiseen, ja ohjeistukseen panostaminen on vakuutusyhtiössä sekä taustateorian että empiirisen aineiston perusteella ensisijaisen tärkeä riskienhallintakeino. On myös tärkeää, että työntekijöiden käyttöoikeudet on rajattu vain niihin järjestelmien osiin, joita he todella tarvitsevat työssään. Mitä laajempi pääsy järjestelmiin henkilöillä on, sitä suurempi riski on myös järjestelmien ja tietojen väärinkäytökselle.

Järjestelmien haavoittuvuudet voidaan taulukon 3 mukaisesti jakaa edelleen koodauksessa oleviin virheisiin ja aukkoihin järjestelmien suojauksessa, sekä puutteellisesta seurannasta aiheutuviin haavoittuvuuksiin. Häiriöt ja virheet sähköisissä järjestelmissä ovat merkittävä kyberriski, koska korvauspalvelun toiminta on lähes kokonaan sähköisten kanavien ja järjestelmien varassa. Korvauspalvelussa verkkopalvelulla on keskeinen rooli, sillä jos asiakas tekee korvaushakemuksen verkkopalvelussa, säästyy korvauskäsittelijöiltä enemmän aikaa monimutkaisempaa päätöksentekoa vaativiin tehtäviin.

Tekniset häiriöt tai asiakkaiden epäluottamus verkkopalveluun johtavat siihen, että asiakkaat alkavat käyttää sähköisten järjestelmien sijaan enemmän kivijalkakonttoreita tai puhelinpalvelua. Samalla vähemmälle käytölle jäävät ne järjestelmät, joihin on panostettu vakuutusyhtiössä paljon. Tärkeimmäksi riskienhallintakeinoksi järjestelmien haavoittuvuuksien ennaltaehkäisyssä havaittiin järjestelmien ja tietoteknisten suojamuurien jatkuva seuranta, kehittäminen ja korjaaminen, erilaiset virustorjuntaohjelmat ja haittaohjelmasuodattimet, sekä tiedostojen varmuuskopiointi.

Ulkoisten tekijöiden aiheuttamat kyberriskit on taulukossa 3 jaettu kiristyshaittaohjelmiin, palvelunestohyökkäyksiin ja tietomurtoihin. Tietomurto korvauspalveluun voi olla erityisen vakava siksi, että korvauspalveluun liittyy paljon asiakkaiden arkaluontoisia terveystietoja. Tietomurto ja kiristyshaittaohjelmat voivat olla seurausta järjestelmissä olevista aukoista tai haavoittuvuuksista, tai esimerkiksi korvauspalvelun työntekijälle lähetetystä huijaussähköpostiviestistä.

Korvauspalveluun kohdistuneen tietomurron seurauksena tietoja saatetaan varastaa, poistaa tai muuttaa. Rikolliset saattavat havitella rahaa esimerkiksi muuttamalla asiakkaiden tilinumeroita omikseen. Välillisenä seurauksena vakuutusyhtiölle voi aiheutua mainehaittaa, vahingonkorvausvastuita, järjestelmien kunnostuksesta ja tietojen palauttamisesta aiheutuvia kustannuksia, sekä katkoksia liiketoiminnassa. Merkittäviä verkkopalvelun kohtaamia ulkoisia kyberriskejä ovat palvelunestohyökkäykset, joissa verkkopalvelua ylikuormitetaan niin paljon, että siellä asioiminen estyy. Kyberhyökkäykset häiritsevät korvauspalvelun toimintaa ja voivat lisäksi horjuttaa asiakkaiden luottamusta sähköisiin järjestelmiin ja koko vakuutusyhtiöön. Yhtiön ulkopuolelta tulevien kyberriskien torjunnassa korostuvat järjestelmien ja tietojen suojaaminen, sekä riskien jatkuva havainnointi ja uhkamallinnukset.

# 5 YHTEENVETO JA JOHTOPÄÄTÖKSET

## 5.1 Tutkimuskysymyksiin vastaaminen

Tässä tutkimuksessa vastauksia etsittiin kahteen päätutkimuskysymykseen: ”Millaisia kyberriskejä vapaaehtoisten henkilövakuutusten korvauspalvelussa on?” ja ”Miten korvauspalvelussa tunnistettuja kyberriskejä voidaan hallita?” Päätutkimuskysymysten lisäksi tutkimuksessa selvitettiin myös, millaisia seurauksia kyberriskeillä voi olla. Empiirisen aineiston perusteella korvauspalvelussa kohdataan pitkälti samanlaisia kyberriskejä kuin case -vakuutusyhtiössä yleisestikin. Haastatteluissa korostui vahvasti, että kyberriskit tulevat muuttamaan muotoaan ja yleistymään tulevaisuudessa merkittävästi. Lisäksi kyberriskien hallinnasta tulee vaativampaa, koska teknologioiden väliset riippuvuudet lisääntyvät ja samalla myös riskeistä tulee toisistaan ristiin riippuvaisia ja hankalammin hahmotettavia. Myös niin sanottujen reaalimaailman riskien uskottiin siirtyvän tulevaisuudessa kybermaailmaan.

Vastauksena ensimmäiseen tutkimuskysymykseen merkittävimmät korvauspalvelussa tunnistetut kyberriskit ovat tietomurto, kiristyshaittaohjelmat, palvelunestohyökkäykset, ihmisen puutteellinen tai virheellinen toiminta, sekä järjestelmien haavoittuvuudet ja virheet. Nämä ovat merkittäviä kyberriskejä korvauspalvelulle, mutta myös koko vakuutusyhtiölle. Pelkästään vapaaehtoisten henkilövakuutusten korvauspalveluun liittyviä riskejä ei empiirisen aineiston perusteella löytynyt, mutta edellä mainitut riskit vaikuttavat erityisen vahvasti vapaaehtoisten henkilövakuutusten korvauspalvelussa.

Toisen tutkimuskysymyksen avulla etsittiin riskienhallintakeinoja ensimmäisen tutkimuskysymyksen avulla tunnistetuille kyberriskeille. Tämän tutkimuskysymyksen osalta riskienhallintakeinoja etsittiin koko vakuutusyhtiön, ei pelkästään korvauspalvelun näkökulmasta. Tämä oli päätetty jo teemahaastattelurunkoa rakennettaessa, mutta haastatteluista saadut tulokset vahvistivat entisestään sitä näkemystä, että korvauspalvelussa tunnistettuja kyberriskejä täytyy ehdottomasti hallita myös koko vakuutusyhtiön tasolla johtuen riskien laajuudesta ja kompleksisuudesta.

Tärkeimpinä riskienhallintakeinoina case -vakuutusyhtiön korvauspalvelussa nousivat esiin tietoturvateknologia, henkilöstön kyberosaamisen kehittäminen ja ylläpitäminen, uhkamallinnukset, käyttöoikeuksien rajaaminen ja tuplasuojaukset järjestelmissä, tietoturvavalvomo, sekä järjestelmien jatkuva seuraaminen ja kehittäminen.

Riskienhallintaprosessi case -vakuutusyhtiössä noudattaa pitkälti perinteistä riskienhallinnan asetelmaa, jossa prosessi etenee riskien tunnistamisesta riskien arviointiin ja edelleen riskienhallintakeinoihin. Case -vakuutusyhtiössä riskienhallinnassa käytetään apuna riskimatriisia, jossa kyberriskien suuruutta arvioidaan riskitulon avulla. Myös kvalitatiivisilla menetelmillä on kyberriskien arvioinnissa tärkeä rooli, sillä toisinaan riskiluvun arviointi kyberriskeille on haastavaa.

## 5.2 Johtopäätökset

Johtopäätöksenä tutkimustuloksista voidaan todeta, että case -vakuutusyhtiön vapaaehtoisten henkilövakuutusten korvauspalvelun kohtaamat kyberriskit linkittyvät hyvin pitkälti vakuutusyhtiön muihin kyberriskeihin. Tämä on osittain selitettävissä sillä, että vakuutusala ja finanssiala ovat ylipäätään tietointensiivisiä aloja, jotka toimivat kiinteästi yhteistyössä erilaisten terveydenhuollon yksikköjen kanssa. Case -vakuutusyhtiön henkilökorvauspalvelussa ja vakuutusyhtiön muissa yksiköissä käytetään myös pitkälti samoja järjestelmiä, mikä osaltaan lisää kyberriskien yleistettävyyttä vakuutusyhtiössä.

Vapaaehtoisten henkilövakuutusten korvauspalvelussa erityispiirteenä on arkaluontoisten terveystietojen käsittely ja säilytys. Case -vakuutusyhtiössä asiakkaiden terveystietoja käsitellään kuitenkin myös lakisääteisten tapaturmavakuutusten korvauspalvelussa ja liikenteen henkilövahinkojen korvauspalvelussa. Lisäksi terveystietoja käsitellään jo ennen vakuutusten myöntämistä esimerkiksi terveysselvityksiä tehtäessä. Näin ollen tämäkään erityispiirre ei täysin erota vapaaehtoisten henkilövakuutusten korvauspalvelua muusta vakuutusyhtiöstä. Kyberriskien yleistettävyys ei kuitenkaan ole negatiivinen piirre, vaikkakin riskien geneerisyys teki tutkimuskysymyksiin vastaamisesta osittain haastavaa.

Kyberriskien hallinnan kannalta on jopa suotuisaa, että kyberriskit ja niiden hallintatoimenpiteet ovat vakuutusyhtiön eri osastojen kesken samankaltaisia. Vakuutusyhtiön on tällöin helpompi noudattaa kyberriskien hallinnassa yhtenäistä linjaa ja kohdistaa riskienhallintatoimenpiteitä tasaisesti eri osastoihin. Molemmat asiantuntijat kertoivat haastatteluissa, että kyberriskien hallinta ja tietoteknisten järjestelmien ylläpitäminen on vakuutusyhtiölle kallista. Joitain kyberriskejä jätetään jopa hallitsematta siksi, että niiden hallitsemisesta aiheutuvat kustannukset nousevat yksinkertaisesti liian korkeiksi. Jos vakuutusyhtiön eri osastoissa käytettäisiin toisistaan eroavia järjestelmiä,

tai jos jokainen osasto vaatisi erilaisia kyberriskien tunnistus-, arviointi-, ja hallintamenetelmiä, nousisivat kustannukset todennäköisesti vielä korkeammiksi. Myös riskien tunnistaminen ja arviointi vaikeutuisi, kun arvioitavia kohteita olisi enemmän. Kyberriskien geneerisyys on siis todellisuudessa vakuutusyhtiölle eduksi. Voidaan jopa todeta, että kyberriskien hallinnan yhtenäistäminen on itsessään riskienhallintakeino.

Teorian ja empirian kannalta pohtien tärkeimmäksi havainnoksi case -yrityksen korvauspalvelun kohtaamista kyberriskeistä nousi, että se mikä on turvallista nyt, ei välttämättä ole sitä enää huomenna. Tämä summaa hyvin yhteen tutkimuksen taustateoriassa esitetyn näkemyksen kyberriskin nopeasti muuttuvasta luonteesta ja empiirisessä aineistossa useasti toistuvan jatkuvan riskienhallinnan käsitteen. Kyberriskien tunnistamisen, arvioinnin ja riskienhallinnan on siis oltava jatkuva prosessi, jotta vakuutusyhtiössä pystytään suojautumaan kyberriskeiltä parhaalla mahdollisella tavalla.

## 5.3 Tutkielman arviointi ja jatkotutkimusehdotuksia

Tässä alaluvussa tarkastellaan tutkimusprosessin onnistumista ja luotettavuutta. Kvalitatiivisen tutkimusmenetelmän ja teemahaastattelun avulla tutkimusaiheeseen oli mahdollista perehtyä syvällisesti pohtien. Tutkimustulosten perusteella kyberriskien tunnistaminen ja arviointi on osittain kvalitatiivista. Tämänkin vuoksi kvalitatiivinen tutkimusmenetelmä sopi tutkimusmenetelmäksi case -vakuutusyhtiössä hyvin. Tutkimus onnistui vastaamaan sille annettuihin tavoitteisiin sillä, molempiin tutkimuskysymyksiin löydettiin kattavasti vastauksia.

Tutkimustulokset olivat kuitenkin hyvin laajoja ja koskivat henkilökorvauspalvelun lisäksi myös koko case -vakuutusyhtiötä. Tutkimustulosten laajuus ja yleistettävyys hankaloittivat tutkimusprosessin toteuttamista ja tutkimuksen keskittämistä korvauspalveluun. Tutkimuksen aihe osoittautui haastavaksi juuri siksi, että kyberriskit ovat kompleksisia ja koskettavat usein koko vakuutusyhtiötä. Tutkimusaihetta olisikin mahdollisesti ollut kannattavaa rajata koskemaan esimerkiksi vain henkilötietojen käsittelyyn liittyviä kyberriskejä vakuutusyhtiössä.

Tutkimuksen luotettavuutta voidaan arvioida sen validiteetin ja reliabiliteetin perusteella. Validiteetti kertoo, kuinka hyvin valittu tutkimusmenetelmä ja käytetyt mittarit pystyvät mittaamaan tutkittavaa ilmiötä. Reliabiliteetilla taas viitataan tutkimuksen

toistettavuuteen, eli kykyyn antaa yleistettävissä olevia, ei-sattumanvaraisia tuloksia. Kvalitatiivisessa tutkimuksessa tutkielman luotettavuutta lisää muun muassa prosessin läpinäkyvyys. Tällä tarkoitetaan sitä, että tutkija raportoi tarkasti jokaisen tutkimusprosessin vaiheen ja perustelee tutkimusaineiston analyysin luokittelun, sekä tutkimuksen tulosten tulkinnan hyvin. (Hirsjärvi, Remes & Sajavaara, 2009, 231–233.)

Tutkijan objektiivisuudella on suuri merkitys kvalitatiivisen tutkimuksen luotettavuudessa ja sen arvioinnissa. Keskeistä kvalitatiivisen tutkimuksen luotettavuuden arvioinnissa onkin nimenomaan tutkimusprosessin luotettavuus. Kvalitatiivisen tutkimuksen luotettavuuden arvioinnissa käsitteitä tärkeämmäksi seikaksi nousee, millaisilla perusteilla tutkimuksen luotettavuutta on argumentoitu. (Eskola & Suoranta, 1998, 163–165.) Arvioin tämän tutkimuksen luotettavuutta tutkimusprosessin kokonaisvaltaisen onnistumisen suhteen, en ainoastaan validiteetin ja reliabiliteetin käsitteiden kautta.

Tutkielman taustateoriaan perehdyttiin huolellisesti ja keskeiset käsitteet selitettiin lukijalle mahdollisimman kattavasti. Lähteinä hyödynnettiin kyberriskeihin ja riskienhallintaan liittyviä kirjallisuuslähteitä, artikkeleja, sekä verkkojulkaisuja. Tämä osoittautui tutkimusprosessissa haastavaksi vaiheeksi, sillä kirjallisuuslähteitä ja aikaisempaa tutkimusta kyberriskeihin liittyen on saatavilla niukasti. Kyberriskin käsite on moniulotteinen ja siitä on tehty suuri määrä erilaisia tulkintoja. Siksi tutkimuksen ymmärtämisen kannalta tarkoituksenmukaisen määritelmän täsmällinen esittäminen onkin tutkimuksen luotettavuuden kannalta oleellista. Tutkimuksen taustateoriaa voidaan pitää luotettavana, sillä esitetyt väitteet on perusteltu huolellisesti ja aineistona on hyödynnetty tieteenalalla yleisesti luotettavina pidettyjä lähteitä.

Koska korvauspalvelun näkökulma toimi tutkimuksen tulkintateoriana, oli kattava perehtyminen korvauspalvelun ja vakuutusyhtiön toimintaan tarpeen. Lainsäädännöllä on oleellinen rooli siinä, kuinka kyberturvallisuutta tulisi toteuttaa vakuutusyhtiössä ja korvauspalvelussa. Tämän vuoksi vakuutusyhtiön ja korvauspalvelun toimintaa ohjaaviin juridisiin seikkoihin on syvennytty tutkimuksessa huolellisesti. Lähteinä on hyödynnetty EU:n yleistä tietosuoja-asetusta, vakuutussopimuslakia, vakuutusyhtiölakia ja rikoslakia. Tulkintateoriassa esitetyt seikat ovat tarpeellisia tutkimuksen toteuttamisen kannalta ja juridisia lähteitä voidaan pitää luotettavina.

Tutkittavan aineiston luotettavuutta voidaan kvalitatiivisessa tutkimuksessa arvioida aineiston kattavuudella, arvioitavuudella ja toistettavuudella. Kattavuudella tarkoitetaan sitä, että aineisto on analysoitu kauttaaltaan, eikä siitä ole vain poimittu satunnaisia kohtia. Arvioitavuus tarkoittaa, että lukijan tulisi olla mahdollista seurata tutkijan päättelyä analyysin edetessä. Toistettavuus viittaa siihen, että analyysissä hyödynnetyt luokittelu- ja tulkintasäännöt on esitetty sillä tavalla, että jollakin toisella tutkijalla olisi mahdollisuus päätyä samoihin lopputuloksiin näitä soveltaen. (Eskola & Suoranta, 1998, 155–156.)

Tämän tutkimuksen empiirisen aineiston analyysi on toteutettu edellä mainittuja periaatteita tavoitellen. Molemmilla haastateltavilla on vahva ammattitaito ja useiden vuosikymmenten kokemus kyberriskien parissa työskentelystä. Toinen haastateltavista pystyi lisäksi kertomaan erittäin kattavasti juuri case- vakuutusyhtiön korvauspalvelun riskeistä ja riskienhallintakeinoista. Hän myös perusteli kertomaansa vakuutusyhtiön riskienhallintamateriaalin avulla, mikä myös lisää tutkimusaineiston luotettavuutta ja tarkoituksenmukaisuutta. Haastateltavia voidaan siis pitää luotettavina lähteinä.

Haastateltavien luotettavuuden lisäksi on oleellista, että haastatteluprosessia voidaan pitää luotettavana. Kysymykset esitettiin haastateltaville mahdollisimman neutraalissa muodossa, välttäen kaikenlaista johdattelua tai oman mielipiteen esiin tuomista. Haastattelut litteroitiin sanatarkasti pian niiden toteuttamisen jälkeen, mikä myös lisää kerätyn aineiston luotettavuutta. Aineiston analyysissa käytiin läpi yksityiskohtaisesti molempien haastateltavien vastaukset ja pyrittiin löytämään näistä samankaltaisuuksia ja eroavaisuuksia, sekä tutkimuskysymyksiin vastaamisen kannalta relevantteja tuloksia. Aineiston kuvauksessa haastateltavien näkemykset tuotiin esiin erikseen, mutta myös näiden yhtäläisyyksistä ja eroavaisuuksista esitettiin kattavasti päätelmiä.

Haastattelutilanteessa kehityskohdaksi havaittiin, että haastattelukysymykset olisi voitu rajata vieläkin tarkemmin, tai vaihtoehtoisesti haastateltavien vastausten laajuutta olisi voitu haastattelutilanteessa rajoittaa suppeammaksi. Haastatteluista saatiin kerättyä kattavasti tarkoituksenmukaista empiiristä aineistoa, mutta tämän lisäksi aihetta sivuavaa tietoa nousi esiin paljon. Tämä hankaloitti tutkimusprosessissa litteroinnin tekemistä ja tärkeimpien asioiden poimimista empiirisestä aineistosta. Litterointi ja aineiston analyysi toteutettiin kuitenkin huolellisesti ja ongelmalähtöisesti, joten empiiristä aineistoa voidaan pitää luotettavana.

Vaikka molemmat haastateltavat olivat alansa asiantuntijoita ja aineistoa saatiin kerättyä kattavasti, olisi tutkimuksen luotettavuutta lisännyt entisestään se, että haastateltavia olisi ollut useampia. Etenkin useampien case -yrityksen sisäisten tahojen haastatteluista olisi voinut olla hyötyä, jotta case -yrityksen näkökulmasta olisi saatu vielä kattavampia tuloksia. Asiantuntijahaastattelu vapaaehtoisten henkilövakuutusten korvauspalvelusta olisi todennäköisesti antanut vielä selkeämpiä vastauksia korvauspalvelun näkökulmasta, mikä olisi helpottanut tutkimusprosessin toteutusta ja tutkimuskysymyksiin vastaamista.

Aikaisemmin esitettyjen perustelujen mukaisesti tätä tutkimusta voidaan pitää luotettavana ja pääosin onnistuneena kokonaisuutena, vaikka kehityskohteita nousikin esiin. Tutkimus tuo esiin uudenlaista tietoa, sillä case -yrityksen korvauspalveluun liittyvistä kyberriskeistä ja niiden hallinnasta ei ole vielä koskaan aikaisemmin tehty tutkimusta. Vaikka korvauspalveluun liittyvät kyberriskit ovatkin pitkälti samanlaisia koko vakuutusyhtiön kohtaamien kyberriskien kanssa, on tämä tutkimustuloksena uutta tietoa.

Kyberriskit ovat melko tuore ja vähän tutkittu ilmiö, ja kuten tutkimustuloksista ja taustateoriasta voidaan todeta, ovat ne myös hyvin nopeasti kehittyviä. Sekä taustateorian että tutkimustulosten perusteella kyberriskit tulevat lisäämään merkittävyyttään tulevaisuudessa kasvavalla vauhdilla, ja siksi jatkotutkimus olisikin erittäin suositeltavaa. Jatkotutkimusta olisi aiheellista kohdistaa erityisesti uusiin teknologioihin, kuten 5G:hen, tekoälyyn ja kasvaviin pilvipalveluihin, sekä näiden mukanaan tuomiin uudenlaisiin kyberriskeihin. Etenkin nämä elementit nousivat tutkimushaastatteluissa esiin haastateltavia huolettavina, sillä näihin liittyy paljon tunnistamattomia tai hallitsemattomissa olevia kyberriskejä.

# LÄHDELUETTELO

## Kirjallisuuslähteet:


Biener, C., Eling, M. & Wirfs, J. H. (2015). Insurability of Cyber Risk: An Empirical Analysis. *Geneva Papers on Risk and Insurance*, 40(1), 131–158. doi:10.1057/gpp.2014.19

Cebula, J. L. & Young, L. R. (2010). *A Taxonomy of Operational Cyber Security Risks.* Carnegie Mellon University, Software Engineering Institute.

Eling, M., McShane, M. & Nguyen, T. (2021). Cyber risk management: History and futureresearch directions. *Risk Management and Insurance Review*, 24(1), 93-125. doi: 10.1111/rmir.12169

Eling, M. & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance*? Journal of Risk Finance,* 17(5), 474–491. doi:10.1108/JRF-09-2016-0122

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

Hirsjärvi, S. & Hurme, H. (2015). *Tutkimushaastattelu: Tutkimushaastattelun teoria ja käytäntö.* Helsinki: Gaudeamus Helsinki University Press.

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2009). *Tutki ja kirjoita.* Helsinki: Tammi.

Ilmonen, I., Kallio, J., Koskinen, J. & Rajamäki, M. (2016). *Johda riskejä.* Helsinki: Finanssi- ja vakuutuskustannus FINVA.

Jokela, T., Lammi, V., Lohi, I. & Silvola, T. (2013). *Vapaaehtoinen henkilövakuutus.* Helsinki: Finanssi- ja vakuutuskustannus Oy FINVA.

Juvonen, M., Koskensyrjä, M., Kuhanen, L., Ojala, V., Pentti, A., Porvari, P. & Talala, T. (2014). *Yrityksen riskienhallinta*. Vantaa: FINVA.

Kivisaari, E. & Kahola, M. (2017). *Vakuutustalous - vakuutusyrityksen riskienhallinta, tilinpäätös ja vakavaraisuus.* Helsinki: FINVA.

Long, C., Fang, L. & Danfeng, Y. (2017). Enterprise data breach: causes, challenges, prevention, and future directions*.* Teoksessa Pedrycz, W., *Wiley interdisciplinary reviews. Data mining and knowledge discovery.* Hoboken: John Wiley & Sons.

Luukkonen, I., Mäntyniemi, L., Pekonen-Ranta, M., Raulos, V. & Santavirta, P. (2018). *Vakuutuslainsäädäntö*. Helsinki: FINVA Finanssikoulutus Oy.

Mahjabin, T., Xiao, Y., Sun, G. & Jiang, W. (2017). A Survey of distributed denial-of-service attack, prevention, and mitigation techniques. *International Journal of Distributed Sensor Networks,* 13(12), 1-33. doi: 10.1177/1550147717741463

Rohmeyer, P. & Bayuk, J. (2019). *Financial Cybersecurity Risk Management.* New York: Apress.

Skrop, A. (2015). DATALEAK: Data Leakage Detection System. *MACRo 2015*, 1(1), 113-124. doi: 10.1515/macro-2015-0011

Srinivas, K. (2019). Process of Risk Management. Teoksessa Hessami, A.G., *Perspectives on Risk, Assessment and Management Paradigms*. Lontoo: IntechOpen.

Strupczewski, G. (2021). Defining cyber risk. *Safety Science*, 135, 1-10. doi: 10.1016/j.ssci.2020.105143

Thakkar, S. (2015). Ransomware - Exploring the Electronic form of Extortion. *International Journal for Scientific Research & Development*|, 2(10), 123-126.

Tuomi, J. & Sarajärvi, A. (2018). *Laadullinen tutkimus ja sisällönanalyysi*. Helsinki: Tammi.

Von Solms, R. & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38.(1), 97–102. doi:10.1016/j.cose.2013.04.004

## Internet-lähteet:

Finanssiala Ry (2021). Hyvä vakuutustapa ja vakuutustoiminnan yleiset periaatteet. Saatavissa: < https://www.finanssiala.fi/aiheet/hyva-vakuutustapa-ja-vakuutustoiminnan-yleiset-periaatteet/#2> Viitattu 31.05.2021.

Finanssiala Ry (2021). Korvauspalvelut. Saatavissa: <https://www.finanssialalle.fi/opintomateriaalit/finanssialan-perusteet/vakuuttaminen/korvauspalvelut-2> Viitattu 23.04.2021

Institute of Risk Management (2014). Cyber Risk Executive Summary. Institute of Risk Management. Saatavissa: <https://www.cgma.org/resources/reports/downloadabledocuments/irm-cyber-risk-report-executive-summary.pdf> Viitattu 30.01.2021.

NAIC (2018). Cybersecurity Risk Management. National Association of Insurance Commissioners (NAIC). Saatavissa: <https://www.naic.org/documents/consumer_alert_cybersecurity_risk_management. htm> Viitattu 07.03.2021.

Swiss Re Institute (2019). New emerging risk insights. Saatavissa: <https://www.swissre.com/dam/jcr:5916802c-cf6b-4c67-9d42-39cf80c4b00d/SONAR%20Publication%202019_WEB_quality.pdf> Viitattu 28.01.2021.

## Oikeudelliset lähteet:

EU:n yleinen tietosuoja-asetus (GDPR) 25.5.2016
Rikoslaki 19.12.1889/39
Vakuutussopimuslaki 28.06.1994/543
Vakuutusyhtiölaki 18.7.2008/521

## Henkilölähteet:

Haastateltava A, Tietoturvajohtaja suomalaisessa vahinkovakuutusyhtiössä. Haastattelu 17.03.2021.
Haastateltava B, Kyberturvallisuuden johtava asiantuntija suomalaisessa organisaatiossa. Haastattelu 08.04.2021.

## Yrityslähteet:

Keskinäinen Vakuutusyhtiö X

# LIITTEET

## LIITE 1: TEEMAHAASTATTELURUNKO ASIANTUNTIJAHAASTATTELUIHIN

### HAASTATELTAVAN TAUSTATIETOJA

Kertoisitteko ensin, millainen on teidän koulutustaustanne, työkokemuksenne, asemanne organisaatiossa, sekä kyberturvallisuusosaamisenne?

### TEEMA 1: KYBERRISKIT VAKUUTUSYHTIÖSSÄ JA KORVAUSPALVELUSSA

- Kuinka suurena uhkana kyberriskit koetaan nyt, entä tulevaisuudessa?
- Mitkä ovat merkittävimmät tunnistetut kyberriskit vakuutusyhtiössä yleisesti ja vapaaehtoisten henkilövakuutusten korvauspalveluissa?
- Miten kyberriskejä voidaan tunnistaa ja miten niitä pyritään tunnistamaan?
- Miten kyberriskejä arvioidaan?
- Millaisia seurauksia kyberriskeillä voi olla?
- Miten vastuu jakautuu, jos kyberriski realisoituu?

### TEEMA 2: KYBERRISKIEN HALLINTA VAKUUTUSYHTIÖSSÄ

- Miten tunnistettuja kyberriskejä pyritään hallitsemaan?
- Miten kyberriskejä pyritään hallitsemaan tulevaisuudessa?
- Millainen rooli yksittäisellä työntekijällä on kyberriskeiltä suojautumisessa?
- Mitä kyberriskejä voidaan hallita ja mitä ei voida hallita?

Tuleeko mieleesi aiheesta joitain muita huomioita, tai materiaalia, josta voisi olla hyötyä tutkimuksessani?