Tampereen yliopisto

Kasimir Luostarinen

KYBERRISKIT JA NIIDEN HALLINTAPROSESSI

Case Yritys Oyj.

Johtamisen ja talouden tiedekunta
Kandidaatintutkielma
Helmikuu 2021

TIIVISTELMÄ

Kasimir Luostarinen: Kyberriskit ja niiden hallintaprosessi – Case Yritys Oyj.
Kandidaatintutkielma
Tampereen yliopisto
Kauppatieteiden tutkinto-ohjelma
Helmikuu 2021

Digitalisaatio ja teknologian kehittyminen ovat mahdollistaneet yritysten liiketoimintaa tehostavia menetelmiä ja muokanneet erilaisten toimialojen toimintaympäristöjä pysyvästi. Megatrendit tulevat korostamaan teknologian roolia entisestään yritysten liiketoiminnassa ja informaatioteknologian rooli tulee muuttumaan liiketoimintaa tukevasta liiketoiminnan kannalta kriittiseksi välineeksi arvon luomisessa. Uudenlaiset mahdollisuudet tuovat kuitenkin myös uudenlaisia riskejä ja uhkia yritysten liiketoimintaan. Kyberriskit on viime vuosina tunnistettu yritysten merkittävimmiksi liiketoiminnan riskeiksi ja riskienhallinnassa niiden hallitsemiseen on alettu kiinnittää entistä enemmän huomiota. Kyberriskien vaikutukset yritysten liiketoimintaan ovat erityisesti taloudellisia. Kyberriskien suorien rahallisten menetysten lisäksi yrityksille voi syntyä lukuisia erilaisia välillisiä kustannuksia, kuten kuluja oikeudenkäynneistä, vahingonkorvausvaatimuksia tai sakkoja. Taloudellisten menetysten lisäksi kyberriskit aiheuttavat yrityksille myös merkittäviä mainehaittoja. Yritykset tarvitsevat kyberriskien hallintaan oikeanlaisia ja luotettavia riskienhallinnan menetelmiä, työkaluja ja prosesseja. Kyberriskien hallintaprosessin nostamisella riittävälle tasolle, aktiivisella riskikentän arvioinnilla ja prosessin kehittämisellä yritykset voivat suojautua kyberriskeiltä mahdollistaen liiketoiminnallisten tavoitteiden saavuttamisen sekä liiketoiminnan jatkuvuuden.

Tämän tutkimuksen keskiössä ovat kyberriskit ja niiden hallintaprosessi, joita tarkastellaan Helsingin pörssiin listatun case-yrityksen näkökulmasta. Tutkimuksen tavoitteena on tutustua case-yrityksen kyberriskien hallintaprosessiin, sen vaiheisiin ja kyberriskien merkitykseen yritykselle. Tutkielmassa luodaan kokonaiskuva case-yrityksen kyberriskien hallintaprosessista, mutta tarkemmin tarkastellaan kyberriskien tunnistamista, arviointia sekä kyberriskien hallintakeinoja. Tutkimus on luonteeltaan kvalitatiivinen tutkimus. Tutkimusmetodina on tapaustutkimus eli case-tutkimus ja empiirinen aineisto koostuu case-yrityksen asiantuntijoiden haastattelusta. Tutkimushaastattelun lajina käytetään puolistrukturoitua teemahaastattelua ja empiirisen aineiston analyysissä käytetään teoriaohjaavaa sisällönanalyysiä.

Tutkimuksen tulokset vahvistavat kyberriskien tunnistettua kasvavaa merkitystä vaikutuksineen yritysten liiketoiminnalle. Tulokset tuovat myös esiin yritysten liiketoimintojen kasvavan roolin kyberriskien merkityksen kasvaessa. Kyberriskien integroituessa entistä tiiviimmäksi osaksi päivittäistä liiketoimintaa, tulee vastuu kyberriskien hallinnasta kuulua koko yrityksen henkilöstölle. Tietoisuuden lisääminen organisaation sisällä on avaintekijöitä kasvavien kyberriskien hallinnassa. Tulosten mukaan kyberriskien hallintaprosessin tulee olla jatkuva prosessi, jossa kyberriskien tunnistamista, arviointia ja hallintakeinojen arviointia tulee toteuttaa säännöllisesti. Kyberriskien hallintaprosessi noudattaa tyypillisiä riskienhallintaprosessin vaiheita ja sen vaiheet ovat menetelmineen tehokkaita myös kyberriskien hallinnassa, tietyt kyberriskien luonteen mukaiset ominaispiirteet huomioiden.

Avainsanat: kyberriskit, kyberturvallisuus, kyberuhka, riski, riskienhallinta, riskienhallintaprosessi

SISÄLLYSLUETTELO

1 JOHDANTO

1.1 Aihealueen esittely

Digitalisaatio ja teknologian kehittyminen ovat mahdollistaneet yritysten liiketoimintaa tehostavia menetelmiä ja muokanneet erilaisten toimialojen toimintaympäristöjä pysyvästi. Megatrendien myötä teknologian rooli tulee korostumaan entisestään yritysten liiketoiminnassa ja tulevaisuudessa informaatioteknologian rooli tulee muuttumaan liiketoimintaa tukevasta liiketoiminnan kannalta kriittiseksi välineeksi yritysten arvon luomisessa. Uudenlaiset mahdollisuudet ovat kuitenkin myös tuoneet yritysten riskikenttään uudenlaisia uhkia sekä haavoittuvuuksia liiketoimintaan. Kyberriskeillä tarkoitetaan informaatioteknologiasta aiheutuvia taloudellisen tappion, maineen vahingoittumisen tai muun häiriön riskejä, jotka aiheuttavat yritykselle vahinkoa (Institute of Risk Management 2014, 10). Luonteeltaan kyberriskit ovat alati muuttuvia, joiden voidaan ajatella kehittyvän yhtäaikaisesti teknologian parina. Uudenlaisten teknologisten innovaatioiden avulla kyetään luomaan entistä parempia hallintamenetelmiä kyberriskeille, mutta vastaavasti ne myös mahdollistavat uudenlaisia tapoja kyberriskien kehittymiselle ja luovat uudenlaisia alustoja kyberhyökkäyksille.

Kyberriskit on viime vuosina tunnistettu yritysten merkittävimmiksi liiketoiminnan riskeiksi ja riskienhallinnassa niiden hallintaan on alettu kiinnittää entistä enemmän huomiota. Myös kybervakuutukset ovat kehittyneet ja yleistyneet myös Suomessa yritysten riskienhallintakeinona kyberriskejä vastaan. Vakuutusyhtiö Allianz on nostanut ensimmäistä kertaa kyberriskit maailman merkittävimmäksi globaaliksi yritysten liiketoiminnan riskiksi vuonna 2020. Vastaavasti vuonna 2013 kyberriskit sijoittuivat samassa tutkimuksessa vasta sijalle 15. Tietoisuus kyberriskeistä ja niihin liittyvistä uhista on viime vuosina kasvanut yritysten lisääntyneestä riippuvuudesta IT-järjestelmiä ja dataa kohtaan sekä monista korkean profiilin tapahtumista johtuen, joissa kyberriskit ovat aiheuttaneet yrityksille massiivisia tappioita. (Allianz 2020, 8.) Allianz Risk Barometer on vuosittain ilmestyvä raportti yritysten merkittävimmistä liiketoiminnan

riskeistä, jonka tulokset perustuvat globaalisti tuhansien riskienhallinnan ammattilaisten näkemyksiin (Allianz 2020, 3).

Kyberriskien vaikutukset yritysten liiketoimintaan ovat toteutuessaan erityisesti taloudellisia. Suorien rahallisten menetysten, kuten liiketoiminnan keskeytymisen lisäksi, yrityksille syntyy kyberriskeistä välillisiä kustannuksia, jotka voivat kohota korkeiksi esimerkiksi pitkien oikeudenkäyntien, sakkojen ja vahingonkorvausten maksamisen seurauksena. EU:n yleisen tietosuoja-asetuksen GDPR:n mukaisten tietosuojaloukkausten seurauksena yritys voi joutua maksamaan 20 miljoonan euron suuruiset sakot tietomurron seurauksena. Sakon suuruus voidaan suurempien yritysten kohdalla asettaa myös jopa 4 prosentin suuruiseksi vuosittaisesta liikevaihdosta. (Evans 2019, 32.) Yritysten kerätessä ja säilöessä entistä enemmän dataa, riskit tietojen vuotamisesta ovat entistä suurempia ja kalliimpia. Toteutuessaan kyberriskit aiheuttavat taloudellisten menetysten lisäksi yrityksille myös merkittäviä mainehaittoja.

Liiketoiminnan siirtyessä enemmän verkkoon ja liiketoiminnan ollessa jatkuvasti enemmän teknologiasta riippuvaista, kyberriskit vaikuttavat globaalisti niin suuriin, kuin pieniin yrityksiin. Covid-19-pandemian voidaan ajatella kiihdyttävän liiketoiminnan sähköistymisen trendiä entisestään. Yritykset tarvitsevat jatkuvasti muuttuvien kyberriskien hallintaan oikeanlaisia ja luotettavia riskienhallinnan menetelmiä, työkaluja ja prosesseja. Kyberriskien hallintaprosessin nostamisella riittävälle tasolle, aktiivisella riskikentän arvioinnilla ja prosessin kehittämisellä yritykset voivat suojautua kyberriskeiltä mahdollistaen liiketoiminnallisten tavoitteiden saavuttamisen sekä liiketoiminnan jatkuvuuden.

Kyberriskeihin ja kyberilmiöön liittyvää tutkimusta on tehty viime vuosina enenevissä määrin aiheiden muuttuessa entistä ajankohtaisemmiksi. Suomessa on valtiotasolla tutkittu etenkin kyberturvallisuutta. Kyberilmiön noususta kertoo myös se, että Suomeen on perustettu esimerkiksi kyberturvallisuuskeskus ja laadittu kyberturvallisuusstrategia. Yritysten kyberriskien hallintaan liittyvä tutkimus painottuu pitkälti vieraskieliseen tutkimukseen. Esimerkiksi kyberriskien hallintaa ovat tutkineet Gordon, Loeb & Sohail (2003) jo 2000-luvun alussa sekä Knowles, Prince, Hutchison, Disso & Jones (2015). Opinnäytetasolla kyberriskien hallintaa on tutkinut esimerkiksi Tia-Liisa Roikola Pro gradu -tutkielmassaan vuonna 2017. Tutkielmassa suomalaisten yritysten kyberriskeiltä

varautumista tutkitaan erityisesti kybervakuutuksen näkökulmasta. Harri Suoninen tutkii Pro gradu -tutkielmassaan 2018 kyberuhkia ja kyberrikollisuutta yritysten liiketoiminnalle. Varsinaista yritysten kyberriskien hallintaprosessiin liittyvää tutkimusta ei opinnäytetasolla kuitenkaan ole aiemmin tehty. Lisäksi tutkimuksen kohdeyrityksenä on markkina-arvoltaan keskisuuri pörssiyhtiö, vastaavanlaista case-yritystä ei ole tutkittu aiemmin kyberriskien hallintaan liittyen.

Tämän tutkimuksen tärkeyttä voidaan perustella kyberriskien ajankohtaisuudella ja merkittävyydellä, joka tulee korostumaan tulevaisuudessa entisestään. Kyberriskit ovat nousseet yritysten merkittävimmiksi liiketoiminnan riskeiksi ja niiden hallintaprosessia tutkimalla voidaan yritysten riskienhallintaa kehittää entisestään suojaamalla liiketoiminnan jatkuvuutta kyberriskeiltä.

1.2 Tutkielman tavoite, tutkimuskysymykset ja rajaukset

Tämän tutkielman keskiössä ovat kyberriskit ja niiden hallintaprosessi, joita tarkastellaan case-yrityksen näkökulmasta. Tutkielman case-yritys on Helsingin pörssiin listattu yritys, jota tutkimalla pyritään ymmärtämään kyberriskien hallintaprosessia ja niiden merkitystä yritykselle. Tutkielman tavoitteena on tutustua kohdeyrityksen kyberriskien hallintaprosessiin, sen vaiheisiin ja kyberriskien merkitykseen yritykselle. Tutkielmassa luodaan kokonaiskuva case-yrityksen kyberriskien hallintaprosessista, mutta tarkemmin tarkastellaan kyberriskien tunnistamista, arviointia sekä kyberriskien hallintakeinoja. Tiettyjen vaiheiden tarkemman tarkastelun avulla vältetään pelkistetty koko prosessin yleinen kuvaus, joka voisi kandidaatintutkielman rajoitteet huomioon ottaen jäädä sisällöltään suppeaksi. Tutkielmassa pyritään saamaan vastaukset yrityksen asiantuntijoita haastattelemalla seuraaviin tutkimuskysymyksiin.

1) Millainen merkitys kyberriskeillä on kohdeyritykselle, miksi?
2) Miten kohdeyritys tunnistaa, arvioi ja hallitsee kyberriskejä?

Ensimmäisen tutkimuskysymyksen avulla pyritään selvittämään, millainen merkitys kyberriskeillä on kohdeyritykselle. Merkityksellä tarkoitetaan tässä yhteydessä ensinnäkin sitä, millaisena riskinä kohdeyritys kokee yleisesti kyberriskit. Kysymyksen

avulla pyritään saamaan vastauksia siihen, millaisia kyberriskejä yritys näkee liiketoiminnassaan, millaisena kyberriskit nähdään yrityksen liiketoiminnan kannalta, kuinka merkittäviä kyberriskit ovat suhteessa muihin riskeihin ja toisaalta suhteessa toisiinsa. Toisena, kysymyksen avulla kartoitetaan syitä kyberriskien koetulle merkitykselle.

Toisen tutkimuskysymyksen avulla keskitytään hallintaprosessin vaiheisiin, joissa kyberriskejä tunnistetaan, arvioidaan ja pyritään hallitsemaan riskienhallintakeinoin. Tutkimuskysymyksen tavoitteena on selvittää, miten kohdeyritys tunnistaa kyberriskejä, miten yritys arvioi kyberriskejä sekä se, millaisia ovat hallintakeinot kyberriskien torjumiseksi. Lisäksi arvioidaan nykyisten hallintakeinojen riittävyyttä kyberriskien hallinnassa.

Tutkielman ollessa case-tutkimus, rajaa se jo itsessään tarkastelun ainoastaan kyseiseen kohdeyritykseen. Rajauksina tutkielmassa keskitytään otsikon ja tutkimuskysymysten mukaisesti vain yrityksen kyberriskeihin ja niiden hallintaprosessiin. Yrityksen muihin riskeihin ja riskienhallintaan viitataan, kun se katsotaan tarpeelliseksi, mutta niiden tarkempi tarkastelu jää tutkielman ulkopuolelle. Huomioitavaa on kuitenkin se, että tutkielmassa esitellään yrityksen riskienhallinnan toteuttaminen yleisellä tasolla, jotta kyberriskien hallintaprosessia olisi helpompaa arvioida kokonaisvaltaisesti tätä tietoa vasten.

1.3 Tutkimusmenetelmät ja aineisto

Tämä tutkimus on luonteeltaan kvalitatiivinen eli laadullinen tutkimus. Kvalitatiivisen tutkimuksen lähtökohtana on todellisen elämän kuvaaminen, johon sisältyy ajatus siitä, että todellisuus on moninainen. Kvalitatiivisessa tutkimuksessa pyritään tutkimaan kohdetta mahdollisimman kokonaisvaltaisesti. (Hirsjärvi, Remes & Sajavaara 2007, 157.) Tässä tutkielmassa kvalitatiivisella tutkimusmenetelmällä tutkittavasta ilmiöstä on mahdollista saada syvällisempää tietoa. Lisäksi laadulliselle tutkimusmenetelmälle tyypillinen sanallinen tutkimusaineisto on kvantitatiivisia menetelmiä sopivampi tutkielman tavoitteiden saavuttamiseksi ja tutkimuskysymyksiin vastaamiseksi. Tutkimuksen tarkoitusta voidaan luonnehtia neljän piirteen perusteella, joita ovat

kartoittava, selittävä, kuvaileva sekä ennustava (Hirsjärvi ym. 2007, 134). Tätä tutkielmaa voidaan pitää pääasiassa kartoittavana, kyberriskien ja niiden hallintaprosessin ollessa vähemmän tutkittu aihe etenkin suomenkielisen tutkimuksen osalta. Tutkielmassa on myös kuvailevia piirteitä.

Yrityksen valikoiduttua tutkielman tutkittavaksi kohteeksi, tutkimusmetodiksi on valittu tapaustutkimus eli case-tutkimus. Tapaustutkimuksella tarkoitetaan tutkimusta, jossa tutkitaan yhtä tai enintään muutamaa tietyllä tarkoituksella valittua tapausta. Kauppatieteiden tutkimuksessa tapaus on yleensä yritys tai yrityksen osa. Tapaus voi olla myös toiminnallinen, kuten prosessi tai jokin yrityksen rakenteellinen ominaisuus. (Koskinen, Alasuutari & Peltonen 2005, 154.) Tässä tutkielmassa tapauksena on kohdeyritys. Tapauksena voidaan ajatella myös olevan yrityksen toiminnallinen prosessi, eli tässä tutkielmassa kyberriskien hallintaprosessi.

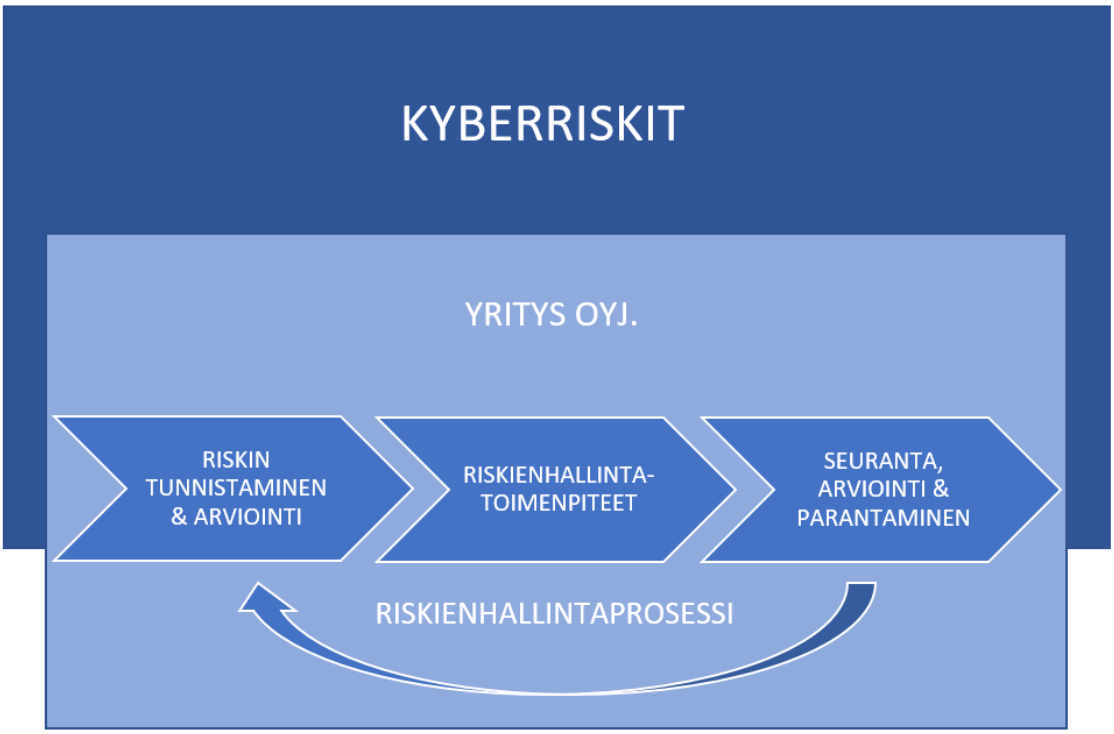
Tutkimuksen empiirinen aineisto koostuu kahden kohdeyrityksen asiantuntijan haastattelusta. Haastattelu on hyvin joustava aineiston keruumenetelmä, joka sopii moniin erilaisiin tutkimustarkoituksiin (Hirsjärvi & Hurme 2008, 34). Tutkimushaastattelun lajina käytettiin tutkielmassa puolistrukturoitua teemahaastattelua. Tavallisesti haastattelulajeja erotellaan sen mukaan, miten strukturoitu haastattelutilanne on. Ääripäät ovat täysin strukturoitu haastattelu, jossa ennalta laaditut kysymykset esitetään tietyssä järjestyksessä sekä strukturoimaton avoin haastattelu, jossa haastattelijalla on mielessään vain tietty aihe tai alue. Teemahaastattelu on lomake- ja avoimen haastattelun välimuoto, jolle on tyypillistä, että haastattelun aihepiirit ovat tiedossa, mutta kysymysten järjestys ja tarkka muoto vaihtelee. (Hirsjärvi ym. 2007, 203.) Teemahaastattelu valikoitui tutkimushaastattelun lajiksi sen joustavuuden takia. Tarkasti strukturoitua haastattelulajia käyttäessä paljon tutkielman kannalta olennaisia tietoja olisi voinut jäädä tulematta ilmi. Vastaavasti täysin avoin strukturoimaton haastattelu olisi voinut johtaa sekavampaan poukkoilevaan haastatteluun, jonka analysointi olisi jälkeenpäin ollut hankalampaa. Tutkimushaastattelun haastattelurungon asettelu teemoittain mahdollisti loogisen haastattelun kulun ja mahdollisti täydentävien lisäkysymysten esittämisen aihe kerrallaan. Tutkimushaastattelu oli lisäksi parihaastattelu. Parihaastattelu on yksi ryhmähaastattelun alalajeista (Hirsjärvi ym. 2008, 61). Ryhmähaastattelun haastateltavat valitaan siten, että heidän keskustelunsa arvellaan maksimoivan informaatiomäärän ja mielipidekirjon (Koskinen ym. 2005, 124).

Parihaastattelun ja haastateltavien valinta tehtiin juuri informaatiomäärän maksimoimiseksi ja haastateltavien keskustelun synnyttämän lisäinformaation takia. Teemahaastattelun ja parihaastattelun käyttö mahdollisti haastateltaville vuorovaikutuksen ja toisten vastausten täydentämisen omista näkökulmistaan. Lisää tutkimushaastattelun toteuttamisesta luvussa 4.2 aineiston kuvaus.

Tutkimuksen kerätyn aineiston analyysissä käytetään teoriaohjaavaa sisällönanalyysiä. Sisällönanalyysin menetelmällä voidaan analysoida tutkittavaa aineistoa systemaattisesti ja objektiivisesti. Analyysimenetelmällä pyritään saamaan tutkittavasta ilmiöstä kuvaus tiivistetyssä ja yleisessä muodossa. (Tuomi & Sarajärvi 2018, 87.) Teoriaohjaavassa sisällönanalyysissä on teoreettisia kytkentöjä siten, että teoria voi toimia analyysin apuna, mutta analyysi ei pohjaudu suoraan teoriaan (Tuomi ym. 2018, 81). Tässä tutkimuksessa teoriaohjaavuus on toteutettu siten, että aineistoa analysoidaan aineistolähtöisesti, mutta aineiston ryhmittelyä ohjaa teoria. Lisäksi lopussa aineiston perusteella tehdyt havainnot sidotaan tiiviimmin teoriaan.

1.4 Tutkimuksen rakenne ja viitekehys

Tutkielman teoreettista viitekehystä havainnollistetaan seuraavan sivun kuvion (kuvio 1) muodossa. Teoreettinen viitekehys rakentuu kyberriskien ja riskienhallintaprosessin käsitteiden ympärille. Viitekehyksen käsitteet muodostavat myös tutkielman teorialuvut, eli pääluvut kaksi ja kolme. Viitekehyksessä on näkyvissä myös tutkielman kohdeyritys, joka kuvaa tutkielman näkökulman tulevan case-yrityksen kautta. Kyberriskit on asetettu viitekehyksen taustalle ilmiönä, jonka sisällä tarkastellaan riskienhallintaprosessia ja sen vaiheita. Kyberriskit ovat taustalla siitä syystä, että ne ovat tutkielman johtava teema, joka rajaa hallintaprosessin tarkastelun yksinomaan kyberriskeihin. Riskienhallintaprosessi on esitetty viitekehyksessä pelkistetyimmässä muodossaan jaoteltuna kolmeen eri prosessin vaiheeseen. Prosessin vaiheiden alapuolelle sijoitettu nuoli kuvaa riskienhallintaprosessin jatkuvaa luonnetta.



Kuvio 1 Tutkimuksen teoreettinen viitekehys

Tutkielma rakentuu viidestä pääluvusta ja niiden alaluvuista. Tässä johdannon pääluvussa on johdateltu tutkielman aiheeseen, asetettu tavoitteet, esitelty menetelmät ja muut tutkielman kannalta olennaiset raamit. Pääluvut kaksi ja kolme ovat tutkielman teorialukuja. Ensimmäinen teorialuku kyberriskeistä toimii tutkielman taustateoriana ja toinen teorialuku riskienhallintaprosessista tutkielman tulkintateoriana. Kyberriskien pääluvussa lähdetään liikkeelle riskin käsitteestä, jonka jälkeen perehdytään tarkemmin kyberriskeihin, niiden luonteeseen ja vaikutuksiin yrityksen liiketoiminnalle. Pääluku riskienhallintaprosessista jakautuu neljään alalukuun, joissa ensimmäisessä käsitellään prosessia yleisellä tasolla ja seuraavissa käydään prosessin vaiheet tarkemmin läpi kolmeen osaan jaoteltuna. Teorialukuja seuraavassa pääluvussa siirrytään tutkielman empiiriseen osioon, jossa esitellään tarkemmin kohdeyritys ja aineiston hankinta ennen tutkimustuloksia. Tutkielman viimeisessä pääluvussa vastataan tutkielman tutkimuskysymyksiin ja verrataan aineiston perusteella saatuja tutkimustuloksia teoriaan. Luku sisältää myös tutkielman arviointia ja mahdollisia jatkotutkimuskohteita.

2 KYBERRISKIT

2.1 Riski

Yleiskielessä sanalla riski tarkoitetaan vaaraa tai uhkaa, joka pitää sisällään ajatuksen siitä, että jotain epäedullista voi tapahtua henkilölle tai jonkun omaisuudelle (Juvonen, Koskensyrjä, Kuhanen, Ojala, Pentti, Porvari & Talala 2014, 8). Riski on yleisesti helposti ymmärrettävä käsite ja sen merkitys henkilön tai yrityksen liiketoiminnan kannalta on hahmotettavissa menetyksen aiheuttavan negatiivisen tapahtuman realisoituessa. Kirjallisuudessa riskille löytyy kuitenkin useita toisistaan poikkeavia määritelmiä asiayhteydestä ja kontekstista riippuen.

Riskin käsitteelle löytyy useita erilaisia määritelmiä ja lähestymistapoja. Yleisesti riskiin kuitenkin ajatellaan liittyvän epävarmuutta ja sen liittyvän ei-toivottuun tapahtumaan. Vaughanin (1997, 8) mukaan riski määritellään kirjallisuudessa vaihtelevasti tappion mahdollisuutena, tappion todennäköisyytenä, epävarmuutena, todellisena hajontana odotetuista tuloksista ja jokaisen odotetusta poikkeavan lopputuleman todennäköisyytenä. Vaughan (1997, 8) määrittelee itse riskin olevan olosuhde, jossa on mahdollisuus haitalliselle poikkeamalle odotetusta ja toivotusta lopputuloksesta. Riskiin liittyy tappion mahdollisuus ja sen todennäköisyys vaihtelee yhden ja nollan välillä. Vaikka riskin todennäköisyyttä ei pystytä määrittämään, on sen haitallisen tuloksen todennäköisyyden oltava nollan ja yhden välillä.

Riskillä voidaan sen toteutuessa nähdä olevan myös positiivinen vaikutus. Riski voi olla mahdollisuus, ei pelkkä uhka. Riski on epävarmuuden vaikutus tavoitteisiin, vaikutus voi olla negatiivista, positiivista tai molempia (ISO 2018). Yrityksen riskienhallinnassa riski on helppo ajatella myös liiketoimintamahdollisuudeksi. Esimerkiksi liiketoimintaympäristöön tai regulaation liittyvät riskit voidaan nähdä myös mahdollisuutena saavuttaa kilpailuetua alan muihin yrityksiin nähden. Koska riskille on olemassa monia erilaisia määritelmiä, on tärkeää, että yritys valitsee itselleen parhaiten omiin tarkoituksiin sopivan määritelmän. Riski organisaation kontekstissa määritellään

yleensä kaikeksi, mikä vaikuttaa yrityksen tavoitteiden saavuttamiseen. (Hopkin 2018, 16.)

Nykyisessä kansainvälisessä käytännössä riskit luokitellaan satunnaisen luonteen perusteella usein seuraavasti: dynaaminen tai staattinen, spekulatiivinen tai puhdas, subjektiivinen tai objektiivinen sekä hajautuva tai systemaattinen. Jaottelussa dynaamisilla riskeillä tarkoitetaan riskien muuttumista suhdanteiden ja olosuhteiden mukaan, kun vastaavasti staattiset riskit pysyvät muuttumattomina. Puhdas riski sisältää vain ei-toivotun tapahtuman mahdollisuuden, mutta spekulatiiviset riskit sisältävät hyödyllisen tapahtuman mahdollisuuden. Subjektiivinen riski on epävarmuutta, joka perustuu persoonan henkiseen tilaan. Objektiivinen riski on tappion suhteellista vaihtelua odotetun tappion ympärillä. Hajautuvaa riskiä voidaan hallita hajauttamalla, kun taas systemaattisen riskin suuruuteen ei hajauttamalla voida vaikuttaa. (Koskinen, Ahteensivu, Havakka & Kulmala 2018, 16.)

Riskien luokittelusta ja riskilajeista on useita erilaisia määritelmiä riskin käsitteen tavoin. Edellä esitetty jaottelu korostaa riskin moninaista luonnetta. Yrityksen liiketoiminnan näkökulmasta kuitenkin erilainen jaottelu voi olla tarpeen apuna riskienhallinnassa ja riskien tunnistamisessa. Riskien luokittelun avulla riskit saadaan yhteismitallisemmiksi, parannetaan riskitietoisuutta organisaatiossa ja lisätään ymmärrystä riskien keskinäisistä suhteista. (Ilmonen, Kallio, Koskinen & Rajamäki 2016, 76.) Ilmosen ym. (2016, 76) Mukaan yksi vakiintuneimmista tavoista on luokitella riskit neljään eri riskilajiin: strategisiin riskeihin, taloudellisiin riskeihin, operatiivisiin riskeihin sekä vahinkoriskeihin.

Strategiset riskit liittyvät organisaation pitkän aikavälin strategisiin tavoitteisiin ja päätöksenteon epävarmuustekijöihin (Ilmonen ym. 2016, 77). Organisaation kohtaamat strategiset riskit voivat olla ulkoisia tai sisäisiä. Ulkoiset strategiset riskit voivat liittyä esimerkiksi toimintaympäristön muutoksiin ja sisäiset strategian toimeenpanon epäonnistumiseen. Operatiiviset riskit ovat organisaation päivittäisiin toimintoihin liittyvien välittömien tai välillisten vahinkojen riskejä. Operatiiviset riskit voivat olla seurausta yrityksen riittämättömistä tai epäonnistuneista sisäisistä prosesseista, henkilöstöstä, järjestelmistä tai ulkoisista tapahtumista. (Ilmonen ym. 2016, 78.) Taloudelliset riskit ovat tyypillisesti kaksipuolisia riskejä. Valuuttakurssit ja korot voivat

vaihdella yrityksen kannalta edulliseen tai haitalliseen suuntaan. Taloudelliset riskit voidaan jakaa edelleen rahoitusriskeiksi ja perusliiketoiminnan riskeiksi. Riskin alle sisältyvät maksuvalmius-, luotto-, markkina-, korko-, osake- ja hyödykemarkkinoiden hintariskit. (Knüpfer, Puttonen 2018, 219.) Vahinkoriskit kuvaavat vahingonvaaraa. Tyypillisiä vahinkoriskejä ovat omaisuusriskit ja keskeytysriskit. Vahinkoriskillä tarkoitetaan yksipuolista riskiä (Knüpfer ym. 2018, 219). Vahinkoriskeihin ei liity positiivista voitonmahdollisuutta ja riski mielletään poikkeuksetta negatiiviseksi.

2.2 Kyberriskien määritelmä ja luonne

Kyberriskille ei ole olemassa yhtä vakiintunutta määritelmää, mutta pääsääntöisesti kyberriskinä voidaan pitää mitä tahansa informaatioteknologiasta aiheutuvaa vikaa tai häiriötä, joka aiheuttaa yritykselle vahinkoa. Kyberriskillä tarkoitetaan taloudellisen menetyksen, maineen vahingoittumisen tai muun häiriön riskiä, joka johtuu informaatioteknologiaan liittyvästä viasta (Institute of Risk Management 2014, 10). Kyberriskille löytyy myös informaatioteknologian riskiä tai informaatioteknologiasta aiheutuvaa riskiä suppeampia määritelmiä. Kyberriski on liiketoiminnan häiriötä ja taloudellista tappiota aiheuttava tapahtuma, joka tapahtuu elektronisesti ja siihen liittyy tahallisuutta (Mukhopadhay, Chatterjee, Saha, Mahanti & Sadhukhan 2011, 11). Tahallinen tapahtuma voi tarkoittaa esimerkiksi hakkerin aiheuttamaa tietovuotoa tai muuta kyberrikollisuuteen liittyvää toimintaa. Mukhopadhayn ym. (2011, 11) mukaan tahallinen tapahtuma voi realisoitua myös esimerkiksi yrityksen työntekijän toimesta, joten määritelmä sisältää ulkoisten tapahtumien lisäksi myös sisäiset tapahtumat.

Kyberriskin määritelmään voidaan tahallisten tapahtuminen lisäksi lisätä toisissa määritelmissä myös tahattomat tapahtumat. Kyberriskit koostuvat tahallisista ja tahattomista tapahtumista, jotka ovat vain riskien osajoukko riskeistä, joille kyberjärjestelmät altistuvat (Refsdal, Solhaug & Stølen 2015, 34). Esimerkiksi luvaton pääsy yrityksen arkaluontoisiin tietoihin voi aueta ulkopuolisille tahallisen hyökkäyksen seurauksena tai tahattoman yrityksen työntekijän inhimillisen virheen seurauksena. Kyberjärjestelmiin kohdistuvalla riskien osajoukolla Refsdal ym. (2015, 33) tarkoittavat sitä, että kyberriskit koostuvat vain kyberuhkien aiheuttamista riskeistä, esimerkiksi palvelunestohyökkäyksistä. Kyberjärjestelmiin liittyy myös kyberuhkien ulkopuolelle

jääviä riskejä. Esimerkiksi luonnonkatastrofin aiheuttamat kyberjärjestelmän häiriöt eivät määritelmässä kuulu kyberriskeihin, koska taustalla ei ole tahallista tai tahatonta kyberuhkaa.

Kyberuhka on mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku, joka kohdistuu kybertoimintaympäristöön ja toteutuessaan vaarantaa siitä riippuvaisen toiminnon (Turvallisuuskomitea 2018, 25). Yleisesti kyberuhkien määritelmiin liitetään tapahtuman mahdollisuus ja uhan aiheutuvan digitaalisen maailman ilmiöistä. Kyberuhat rinnastetaan usein tahalliseen pahantahtoiseen toimintaan, jonka taustalla on esimerkiksi rikollisessa mielessä toimiva henkilö tai organisaatio. Esimerkiksi myös Evansin (2019, 101) määritelmän mukaan kyberuhka on tahallinen vihamielinen yritys vahingoittaa tietokoneverkkoa ja järjestelmiä. Kuitenkin suuri osa kyberuhista on myös tahattomia. Kyberuhkia voivat olla järjestelmät, jotka kaatuvat ohjelmointivirheiden tai laitteiston vanhentumisen seurauksena. Refsdal ym. (2015, 29) nostavatkin kyberuhan määritelmässä esille myös uhkien tahattomuuden luonteen. Kyberriskien tapaan kyberuhat voivat olla yrityksen sisäisiä, ulkoisia, tahallisia tai tahattomia.

Kyberuhkien ohella keskeinen kyberriskeihin liittyvä termi on kyberturvallisuus. Kyberturvallisuus on tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Lisäksi kyberturvallisuuteen kuuluvat toimenpiteet, joilla voidaan ennakoivasti hallita ja tarvittaessa sietää erilaisia kyberuhkia ja niiden vaikutuksia. (Turvallisuuskomitea 2018, 25.) Turvallisuuskomitean laatiman kyberturvallisuuden sanaston määritelmään kuuluu myös kybertoimintaympäristön tavoitetila, mutta usein kyberturvallisuuteen viitataan kyberuhilta suojautumisen ja kyberriskien hallinnan yhteydessä. Evansin (2019, 100) mukaan kyberturvallisuus on kokonaisuus tekniikoita, prosesseja ja käytäntöjä, jotka on suunniteltu suojaamaan verkkoja, tietokoneita, ohjelmia ja dataa hyökkäyksiltä sekä luvattomalta käytöltä.

Kyberriskit ovat luonteeltaan hyvin moninaisia ja niitä on vaikea osoittaa yksittäiseen riskiluokkaan. Yhteen riskiluokkaan jakaessa kyberriskit luokitellaan kuitenkin yleisimmin operatiivisiksi riskeiksi. Cebulan & Youngin (2010, 10) mukaan kyberriskit määritellään operatiivisiksi riskeiksi, joilla on vaikutuksia tiedon tai tietojärjestelmien saatavuuteen, eheyteen tai luottamuksellisuuteen. Moninaisuuden lisäksi kyberriskit ovat luonteeltaan hyvin globaaleja ja nopeasti muuttuvia. Kyberriskien nopeasti lisääntyvä

monimutkaisuus ja entistä lamauttavampi vaikutus liiketoimintaan edellyttävät jatkuvaa huomiota ja vaativat erilaisia resursseja sekä priorisointia kuin muut yrityksen kohtaamat riskit tänä päivänä. Kyberriskeistä tekee uniikin niiden nopeus, laajuus sekä monimutkaisuus perinteisiin liiketoiminnan riskeihin verrattuna. (Ruan 2019, 76-77.) Nopeudella Ruan (2019, 77) viittaa nopeasti kehittyvään teknologiaan, joka mahdollistaa uudenlaiset ja jatkuvasti muuttuvat kyberhyökkäykset. Esimerkiksi esineiden internetin ja tekoälyn lisääntyminen ja kehittyminen luovat jatkuvasti myös uudenlaisia kyberriskejä, jotka vaativat dynaamisia nopeasti mukautuvia riskienhallintakeinoja (Ruan 2019, 77). Laajuudella voidaan tarkoittaa kyberriskien rajat ylittävää globaalia luonnetta, mutta myös datan räjähdysmäisen kasvun aiheuttamaa kyberuhkien lisääntymistä entistä laajemmaksi riskikentäksi. Dataa on entistä enemmän saatavilla ja se on tarkempaa sekä entistä personoidumpaa. Yksityisyyden ja datan käytön ongelmien lisäksi riskit niiden väärinkäytöstä kasvavat. (Ruan 2019, 77.) Monimutkaisuudella Ruan (2019, 77) tarkoittaa kyberriskien koostuvan laajemmin monista muista tekniikan ulkopuolisista tekijöistä kuten poliittisista ja inhimillisistä uhista, kuin perinteiset liiketoiminnan riskit.

2.3 Kyberriskien lähteet ja erilaiset kyberuhat

Kyberriskien luonteen mukaisesti niiden muodostumiselle on olemassa useita erilaisia syitä ja lähteitä. Cebula ym. (2010, 2) mukaan kyberriskien lähteet voidaan jakaa neljään pääluokkaan: 1) ihmisten toimenpiteet, 2) Järjestelmävirheet, 3) sisäisten prosessien epäonnistuminen ja 4) ulkoiset tapahtumat. Kyberriskit voivat kuitenkin muodostua myös useamman lähteen summana. Riski voi laukaista riskin toisessa pääluokassa. Esimerkiksi ohjelmiston häiriö, joka johtuu virheellisistä asetuksista, voi olla seurausta ihmisten tahattomasta tai tahallisesta toiminnasta. (Cebula ym. 2010, 2.) Kyberriskien lähteisiin jaottelu auttaa ymmärtämään kyberriskeihin liittyviä riskitekijöitä. Lähteet tunnistamalla niiden arviointi ja hallintakeinojen valinta on helpompaa riskienhallinnan näkökulmasta.

Cebula ym. (2010, 3) jakavat ihmisten toiminnasta johtuvat kyberriskien lähteet tahattomiin, tahallisiin ja toteuttamatta jätettyihin toimenpiteisiin. Suuri osa kyberriskeistä voidaan jakaa lähteeltään tähän luokkaan. Kyberhyökkäykset ja muut tahalliset vahingonteot voidaan poikkeuksetta lukea ihmisten toimenpiteistä lähtöisiksi. On kuitenkin hyvä huomioida, että tahalliset vahingonteot ja vahingoittamisyritykset

voivat seurata muun pääluokan lähteen kyberriskin seurauksena. Esimerkiksi tietotekniikan suojauksen kaatuminen tai ohjelmistovirhe voi johtaa tahalliseen vahingoittavaan toimenpiteeseen, joka hyödyntää muuta realisoitunutta riskiä. Cebulan ym. (2010, 3) mukaan ihmisten tahattomat toimenpiteet ovat yleensä organisaation sisäisiä ja ne voidaan jakaa erehdyksiin, virheisiin ja laiminlyönteihin. Ihmisten tahallisten toimenpiteiden alaluokka kuvaa toimia, jotka ovat tahallisia ja niiden tarkoituksena on tuottaa vahinkoa. Tahallisiin tekoihin kuuluvat petokset, sabotaasit, varkaudet ja vandalismi. Toteuttamatta jätettyjen toimenpiteiden alaluokalla kuvataan toimimattomuutta toimenpiteitä vaativissa tilanteissa. Toimimattomuuden syyt jaetaan taitojen, tiedon ja ohjauksen puutteeseen sekä vastaavan henkilön saatavuuteen tietyllä hetkellä.

Järjestelmävirheiden luokka kuvaa laitteiston, ohjelmistojen ja järjestelmien virheitä, jotka ovat normaalista poikkeavia ja odottamattomia. Laitteistosta lähtöisin olevat kyberriskit liittyvät fyysisiin laitteiston vikoihin, kuten kapasiteettiin, suorituskyvyn puutteeseen, ylläpitoon ja vanhentuneisuuteen. Ohjelmistoista aiheutuvat kyberriskit ovat kaiken tyyppisten ohjelmistojen aiheuttamia riskejä, mukaan lukien käyttöjärjestelmät ja sovellukset. Ohjelmistojen viat voivat seurata ohjelmiston osien yhteensopimattomuudesta, vääränlaisista asetuksista, muutosten hallinnan epäonnistumisesta, ohjelmoinnin virheistä tai ohjelmistosovellusten puutteellisesta testauksesta. Järjestelmien aiheuttamat kyberriskit ovat lähtöisin järjestelmien odottamattomista toimimattomuuksista. (Cebula ym. 2010, 4-5)

Sisäisten prosessien epäonnistuminen kyberriskien lähteenä kuvaa odottamattomia vikoja prosessien suorittamisessa. Epäonnistuminen voi johtua prosessien suunnittelun ja toteuttamisen epäonnistumisesta, prosessien puutteellisesta hallinnasta ja puutteellisten tukitoimien seurauksena. Neljännen pääluokan, ulkoisten tapahtumien aiheuttamat kyberriskit ovat yleisesti organisaation kontrollin ulkopuolisia asioita. Ulkoisten tapahtumien ajoitusta ja esiintymistä on vaikea ennakoida. Luokan kyberriskien lähteenä voivat olla luonnonkatastrofit, lainsäädännölliset ongelmat, liiketoiminnalliset ongelmat sekä ulkopuoliset palveluntarjoajat. (Cebula ym. 2010, 6.)

Erilaiset kyberuhat kehittyvät ja muuntautuvat jatkuvasti teknologian kehittyessä. Euroopan unionin kyberturvallisuusvirasto ENISA on raportissaan nimennyt

merkittävimmät kyberuhat vuoden 2019 tammikuusta vuoden 2020 huhtikuuhun ja tehnyt yhteenvedon tarkasteluajanjakson kyberuhkien trendeistä sekä vaikutuksista tulevaisuuteen. ENISA (2020a, 7) nimeää merkittävimmiksi kyberuhiksi: 1) haittaohjelmat, 2) verkkohyökkäykset, 3) verkkourkinnan, 4) verkkosovelluksiin kohdistuvat hyökkäykset, 5) spämmin, 6) palvelunestohyökkäykset, 7) identiteettivarkaudet, 8) tietomurrot, 9) sisäpiiriuhat, 10) bottiverkot, 11) fyysiset varkaudet ja vahingoittamiset, 12) tietovuodot, 13) kiristysohjelmat, 14) kybervakoilun ja 15) kryptovaluuttojen louhinnan. Kolmeksi merkittävimmäksi trendiksi kyberuhissa ENISA (2020a, 10) nimeää teknologian kehityksen, Covid-19-pandemian ja sosiaalisen median. Seuraavaan teknologian aikakauteen siirtyminen laajentaa kyberuhkien kenttää yhä laajemmaksi. Pandemian jälkeen seuraa uusi sosiaalinen ja taloudellinen normi, joka on entistä riippuvaisempi turvallisesta ja luotettavasta kyberympäristöstä. Sosiaalisen median alustojen käyttö kyberhyökkäyksissä on uudenlainen, yleistyvä ja vakava uhka. (ENISA 2020a, 10)

Kyberuhkia voidaan jakaa erilaisiin luokkiin, mutta niille ei ole yhtä vakiintunutta tapaa. Institute of Risk Management (2014, 47) jakaa kyberuhat kolmeen erilaiseen luokkaan ja edelleen alaluokkiin. Ensimmäinen luokka liittyy datan muokkaamiseen ja luotettavan tiedon tuhoamiseen. Toinen luokka sisältää kyberuhat, jotka estävät datan ja palveluiden käytettävyyttä. Kolmannen luokan kyberuhat liittyvät luottamuksellisen datan hyväksikäyttöön erilaisilla tavoilla, esimerkiksi kybervakoilu ja identiteettivarkaudet. (Institute of Risk Management 2014, 47.) Kyberuhkien luokittelua vaikeuttaa se, että monilla niistä on hyvin samankaltaisia ominaisuuksia. Kolmessa seuraavassa kappaleessa on määritelty tarkemmin merkittäviä kyberuhkia niiden yleisyyden, taloudellisen sekä yhteiskunnallisen vaikutuksen perusteella.

Haittaohjelmat ovat tietokoneohjelmia, jotka on tarkoitettu vahingoittamaan tietokonejärjestelmiä ja häiritsemään niiden käytettävyyttä. Haittaohjelmat on jatkuvasti luokiteltu yhdeksi merkittävimmistä kyberuhista yrityksille, valtioille ja yksilöille (Choo 2011, 721). Myös edellä esitetyssä Euroopan unionin kyberturvallisuusviraston tuoreessa raportissa haittaohjelmat nostettiin merkittävimmäksi riskiksi. Haittaohjelmiin kuuluu viruksia, matoja, kiristysohjelmia, vakoiluohjelmia ja kryptovaluuttaa louhivia ohjelmia. Haittaohjelmien yleisiä tavoitteita ovat tieto- ja identiteettivarkaudet, vakoilu ja palveluiden käytettävyyden häirintä. (ENISA 2020b, 2.)

Palvelunestohyökkäykset ovat tietoverkkohyökkäyksiä, joilla pyritään kuormittamaan ja siten lamaannuttamaan jokin palvelu tai tietojärjestelmä. Palvelunestohyökkäykset ovat usein hajautettuja palvelunestohyökkäyksiä, eli ne toteutetaan yhtä aikaa useammista eri lähteistä niiden torjumisen vaikeuttamiseksi. Hajautettuun hyökkäykseen käytetään usein hyökkääjän haltuun ottamaa bottiverkkoa. (Kyberturvallisuuskeskus 2018, 31.) Palvelunestohyökkäykset ovat yleisiä kyberuhkia ja niitä kohdistetaan esimerkiksi finanssisektorin palveluntarjoajiin. Palvelunestohyökkäyksien motiivina voi olla rahan kiristäminen tai häirintä. Evansin (2019, 16) mukaan palvelunestohyökkäyksistä aiheutuva taloudellinen tappio muodostuu yrityksille yleensä prosessitasolla, kun yritys ei pysty harjoittamaan liiketoimintaa keskeytymisen vuoksi.

Tietomurrot ovat tapahtumia, joissa kopioidaan, lähetetään, varastetaan tai käytetään luvattomasti arkaluontoista ja yksityistä tietoa. Tietomurtoihin liittyy usein taloudellisia tietoja esimerkiksi luottokorttitietoja, henkilökohtaisia terveystietoja, muita arkaluontoisia henkilökohtaisia tietoja tai yritysten liikesalaisuuksia. Suurin osa tietomurroista kohdistuu haavoittuviin, heikosti suojattuihin ja jäsentelemättömiin dokumentteihin ja tiedostoihin. (Ruan 2019, 136.) Tietomurrot saivat suurta näkyvyyttä Suomessa loppuvuodesta 2020 Psykoterapiakeskus Vastaamon tietomurron seurauksena, kun suuri määrä arkaluontoisia terveystietoja joutui hyökkäyksen kohteeksi. Tapaus nosti esille kyberturvallisuuden ja henkilötietojen vahvemman suojaamisen jatkuvasti digitalisoituvassa yhteiskunnassa.

2.4 Kyberriskien vaikutukset

Kyberriskien vaikutukset ovat merkittäviä koko yhteiskunnan tasolla. Kyberhyökkäykset koskevat yritysten lisäksi myös valtioita. Kyberriskien globaalit rajat ylittävän luonteen vuoksi yksittäiset hyökkäykset voivat kohdistua niihin myös samanaikaisesti. Yksittäinen kyberhyökkäys voi vaikuttaa kymmeniin, satoihin tai jopa tuhansiin instituutioihin yhtäaikaisesti (Ruan 2019, 76). Yritysten riskienhallinnan ohella valtiot ovat alkaneet kiinnittää entistä enemmän huomiota niitä uhkaaviin kyberriskeihin. Esimerkiksi myös Suomi on laatinut oman kyberturvallisuusstrategiansa. Kyberturvallisuusstrategia asettaa keskeisimmät kansalliset tavoitteet kybertoimintaympäristön kehittämiseksi ja siihen

liittyvien elintärkeiden toimintojen turvaamiseksi (Turvallisuuskomitea 2019, 4). Kyberriskien yhteiskunnallisesti laajoista vaikutuksista huolimatta, seuraavissa kappaleissa keskitytään tutkimuksen aihepiirin mukaisesti niiden vaikutuksiin yrityksien näkökulmasta.

Kyberriskien vaikutukset ovat yrityksille ennen kaikkea taloudellisia. Kyberriskit aiheuttavat yrityksille suoria rahallisia menetyksiä, oikeudenkäyntikuluja, operationaalisia kuluja sekä sakkoja lainsäädännöllisten asetusten rikkomuksista, esimerkiksi tietosuoja-asetuksen rikkomisesta tietomurron yhteydessä (Evans 2019, 16). Liiketoiminnan keskeytymiseen liittyy suuria taloudellisia menetyksiä. Kyberriskit ovat entistä lamauttavampia ja toiminnan keskeytyminen voi yrityksen riskienhallinnan tasosta riippuen olla hyvin pitkäkestoinen. Liiketoiminnan keskeytyminen voi olla seurausta esimerkiksi palvelunestohyökkäyksestä tai haittaohjelmasta, joka lamauttaa liiketoiminnan kannalta tärkeiden laitteiden toimintakyvyn. Liiketoiminnan keskeytymisestä seuraavien vaikutusten lisäksi myös lainsäädännölliset sanktiot voivat taloudellisesti olla hyvin suuria.

Tieto- ja yksityisyydensuojan sääntelyn tiukentumisen ja entistä suurempien joukkokanteiden seurauksena tietomurtojen kustannukset ovat merkittävässä kasvussa. Yritykset keräävät entistä enemmän henkilökohtaista dataa, jonka seurauksena tietomurrot ovat entistä suurempia. Hotelliketju Marriott joutui vuonna 2018 tietomurron kohteeksi, joka koski yli 300 miljoonan asiakkaan henkilötietoja. Yritystä vastaan nostettiin lukuisia kanteita oikeudessa ja Iso-Britannian tietosuojaviranomainen asetti yritykselle 100 miljoonan punnan sakot GDPR-tietosuojalain rikkomuksesta. (Allianz 2020, 11.) GDPR:n ansiosta tietomurtojen uhrina olevien asiakkaiden on entistä helpompaa hakea vahingonkorvauksia oikeusteitse (Allianz 2020, 13).

Taloudellisten vaikutusten osalta on otettava huomioon myös kolmansista osapuolista aiheutuvat riskit. Yritykset käyttävät liiketoiminnassaan hyödykseen entistä enemmän kolmansia osapuolia ja eri toimintojen ulkoistamisen trendi on kiihtymässä. Kolmansien osapuolien ongelmat kyberturvallisuudessa voivat siirtyä suoraan yritykselle. (Evans 2019, 25.)

Taloudellisten vaikutusten lisäksi kyberriskien aiheuttamat mainehaitat voivat olla yrityksille vahingollisia. Tieto yrityksen altistumisesta kyberhyökkäykselle leviää verkossa nopeasti ja voi saada huomattavan suuren mediahuomion. Mainehaitat voivat olla pitkäkestoisia heikentäen asiakkaiden luottamusta yritystä kohtaan. Mainehaittojen taloudelliset vaikutukset voivat myös olla merkittäviä. Maineriski kasvattaa taloudellista riskiä kahdella tavalla, liikevaihto pienenee menetetyn myynnin seurauksena ja yrityksen osakekurssin laskuna. Esimerkiksi yhdysvaltalaisen tavaratalon Targetin myynti laski tietomurron jälkeisen ensimmäisen vuoden aikana neljänteen vuosineljännekseen mennessä 46%. (Evans 2019, 24.)

Kyberriskeillä on liiketoimintaan myös monia muita epäsuoria vaikutuksia. Kyberriskien aiheuttamat oikeudenkäynnit vievät taloudellisten panosten lisäksi arvokkaita työtunteja muun liiketoiminnan palauttamisesta normaalille tasolle. Liiketoiminnan jatkaminen voi lisäksi vaikeutua kriittisen datan katoamisen seurauksena tai liikesalaisuuksien vuotona kilpailijoiden nähtäville. Asiakkaiden menettämisen lisäksi yritys voi menettää myös työntekijöitään. Esimerkiksi suuren mediahuomion saaneen tietomurron jälkeen työntekijät voivat pitää yrityksessä työskentelyä vahingollisena heidän urakehityksensä kannalta. (Institute of Risk Management 2014, 32.) Kyberriskien toteutumisen syynä voi olla puutteellinen riskienhallinta ja varautuminen. Liiketoiminnan normaalille tasolle palauttamisen ohella yrityksen tulee panostaa kyberturvallisuuden parantamiseen ja teknisiin investointeihin. Välillisiä taloudellisia vaikutuksia yritykselle voi syntyä myös vakuutusmaksujen kasvamisesta sekä vieraan pääoman saatavuuden vaikeutumisesta. Pahimmillaan kyberriskit voivat vaikuttaa yrityksiin lopettamalla koko liiketoiminnan.

3 RISKIENHALLINTAPROSESSI

3.1 Riskienhallintaprosessi yleisesti

Riskienhallinnan onnistumiseksi ja yrityksen strategisten tavoitteiden saavuttamiseksi yritys tarvitsee systemaattisen tavan toteuttaa toimenpiteitä riskien hallitsemiseksi. Riskienhallintaprosessi on systemaattinen tapa, jolla riskejä arvioidaan, hallitaan ja raportoidaan. Riskejä ei pidä arvioida irrallisina vaan suhteessa poikkeamiin ja tapahtuneisiin vahinkoihin. (Ilmonen ym. 2016, 95.) Prosessi on yrityksen määrittämien periaatteiden systemaattista soveltamista sen eri vaiheisiin, joiden avulla riskejä pyritään hallitsemaan. Prosessi kattaa kaikki riskien hallitsemiseen liittyvät toimenpiteet. Ilmosen ym. (2016, 130) mukaan riskienhallintaprosessin tarkoituksena on lisätä ymmärrystä riskeistä, jotta voidaan tehdä toimenpiteitä ja päätöksiä riskien hallitsemiseksi ja toteuttaa päätetyt hallintakeinot keskeisimmille riskeille.

Riskienhallintaprosessin tulee kattaa kaikki riskien hallitsemisen vaiheet, niinpä prosessi jakautuu useampaan vaiheeseen. Vaughanin (1997, 34) mukaan prosessin jakaminen eri osiin on hyödyllistä riskien analysoinnin kannalta, mutta käytännössä vaiheet sulautuvat yhteen riskienhallinnassa. Riskienhallintaprosessiin on olemassa useita vaihtoehtoisia prosessimalleja, mutta niiden sisältö on hyvin lähellä toisiaan. Erot liittyvät lähinnä prosessin vaiheiden lukumääriin. Ilmonen ym. (2016, 96) jakaa prosessin pelkistetyimmillään kolmeen osaan: riskien tunnistamiseen ja arviointiin, riskienhallintapäätökseen ja sen toimenpiteiden suorittamiseen sekä riskienhallintatoimenpiteiden arviointiin, seurantaan ja tarkastamiseen. Hänen mukaansa olisi kuitenkin tavoitteellisen johtamisen elementit huomioidakseen syytä laajentaa prosessi viiteen vaiheeseen.

Vaughan (1997, 34) jakaa prosessin kuuteen vaiheeseen: 1) tavoitteiden määrittäminen, 2) riskien tunnistaminen, 3) riskien arviointi, 4) vaihtoehtojen arviointi ja hallintakeinojen valinta, 5) valintojen toteuttaminen sekä -6) arviointi ja kehittäminen. Lam lähestyy prosessia riskien ymmärtämisen kautta. Lamin (2014, 36) mukaan riskienhallinta on

ihmisten johtamaa toimintaa, joten yrityksen riskienhallinnan prosessi voidaan havainnollistaa tavoilla, joilla ihmiset hallitsevat riskejä jokapäiväisessä elämässään. Hänen mukaansa riskienhallintaprosessi voidaan jakaa riskitietoisuuden lisäämiseen, riskien mittaamiseen ja riskien hallitsemiseen.

Riskienhallinnan ja sen prosessin tueksi yritys voi käyttää apunaan viitekehyksiä tai standardeja. Riskienhallinnan standardien mukainen riskienhallintaprosessi sisältää pääsääntöisesti edellisessä kappaleessa esitettyjen prosessimallien keskeisimmät vaiheet. Prosessin lisäksi standardit sisältävät tyypillisesti riskienhallinnan järjestämisen tueksi periaatteita ja käytäntöjä organisointiin. Ilmosen ym. (2016, 30) mukaan standardien suurin hyöty on niiden luoma yhteinen riskienhallintasanasto ja metodologia yritykselle, joka mahdollistaa systemaattisen, ymmärrettävän ja toistettavan lähestymistavan riskienhallintaan. Kansainvälisesti yleisiä yritysten käytössä olevia standardeja ovat esimerkiksi ISO 31000 ja COSO ERM.

Riskienhallinnan toimintojen kehittämisessä ja prosessin luomisessa olennaista on riskienhallintapolitiikka, joka asettaa yrityksen riskienhallinnan keskeisimmät tavoitteet. Riskienhallintapolitiikka on tavallisesti yrityksen hallituksen määrittämä. Politiikassa voidaan määritellä riskienhallinnan periaatteita ja vastuita sekä kuvata riskienhallinnan merkitystä strategian toteutumiselle. Riskienhallintapolitiikka voi myös selkeyttää riskienhallintaprosessin vaiheita ja määritellä toimintatapoja eri prosessin vaiheisiin. Vaughanin (1997, 98) mukaan riskienhallintapolitiikan tarkkuus vaihtelee huomattavasti ja joissain tapauksissa politiikkaan on dokumentoitu tiukat säännöt, joiden mukaan on toimittava tilanteesta riippumatta. Muissa tapauksissa politiikka sisältää yleisisiä toimintaohjeita, jotka antavat harkinnanvaraa operatiiviseen toimintaan ja riskienhallintaan (Vaughan 1997, 98).

Yrityksen riskinkantokyvyn määrittäminen voidaan ottaa osaksi riskienhallintapolitiikkaa. Vaughanin (1997, 100) mukaan äärimmäisten riskien välttämiseksi on määriteltävä raja, mihin asti yritys sietää riskien aiheuttamaa tappiota. Rajan asettaminen on yksi vaikeimmista päätöksistä riskienhallintapolitiikan muotoilussa (Vaughan 1997, 100). Riskinkantokyvyn määrittäminen on keskeistä riskienhallinnan strategian kannalta ja sen määrittäminen on välttämätöntä riskienhallintaprosessin vaiheiden toteuttamiseksi. Esimerkiksi riskien arvioimisen jälkeen riskinkantokykyyn

vertaaminen auttaa yritystä valitsemaan oikeat keinot hallita riskiä riskinkantokyvyn puitteissa. Ilmosen ym. (2016, 11) mukaan riskinkantokyky määritellään tavallisesti vastaukseksi kysymykseen, kuinka paljon yritys kestää taloudellista menetystä vuodessa, millä tarkoitetaan yleensä suurinta mahdollista negatiivista muutosta yrityksen liiketoiminnan mittareihin, jonka yritys voi hyväksyä.

Riskinkantokyky määrittelee pitkälti yrityksen riskinottohalun. Riskinottohalu määrittää sen, kuinka paljon yritys on valmis ottamaan liiketoiminnassaan riskiä. Riskinottohalu liittyy läheisesti strategiaan ja siinä korostuu riskinkantokykyyn verrattuna riskin positiivinen puoli ja liiketoimintamahdollisuudet. Organisaation tulee määritellä riskinottohalunsa tai se, kuinka paljon riskiä on otettava saavuttaakseen osakkeenomistajien ja sidosryhmien tavoitteet (Fraser & Simkins 2010, 113). Fraserin ym. (2010, 114) mukaan riskinottohalulla on kaksi ulottuvuutta, joista toinen keskittyy markkinoiden keskimääräiseen ja odotettuun tilanteeseen ja toinen äärimmäisiin ja pahimpiin mahdollisiin tilanteisiin. Keskimääräisten ja äärimmäisten tilanteiden arviointi auttaa yrityksen lopullisen riskinottohalun tason määrittämistä.

3.2 Riskien tunnistaminen ja arviointi

Riskiarviointi muodostaa keskeisen riskienhallintaprosessin vaiheen, joka seuraa toimintaympäristön määrittelyä ja riskienhallinnan tavoitteiden asettamista. Riskien tunnistaminen ja luokittelu muodostavat riskiarvioinnin vaiheen riskienhallintaprosessiin, joka sisältää riskien tunnistamista, arviointia ja luokittelua, jotta saadaan määriteltyä merkittävimmät organisaatiota, projekteja ja strategiaa koskevat riskit (Hopkin 2018, 119). Riskienhallintaprosessin vaiheeseen sisältyy vaihteleva määrä pienempiä vaiheita eri prosessimalleissa. Pääsääntönä kuitenkin se, että riskit tunnistetaan, niitä arvioidaan ja niiden merkitystä yritykselle ja liiketoimintoihin arvioidaan.

Lamin (2014, 399) mukaan riskiarvioinnin tavoitteena on tunnistaa, kvantifioida ja priorisoida organisaation riskejä, jotta voidaan mahdollistaa tietoon perustuvien liiketoiminta- ja riskienhallintapäätösten tekeminen. Riskianalyysin termillä voidaan viitata prosessin vaiheeseen, jossa arvioidaan kokonaisvaltaisesti riskin luonnetta ja sen suuruutta. Eroja kuitenkin löytyy ja esimerkiksi Juvonen ym. (2016, 20) määrittelee

riskianalyysin tietoiseksi riskien tunnistamisen ja arvioinnin prosessiksi, joka on riskienhallinnan tärkein yksittäinen osa.

Riskien tunnistamisen tavoitteena on havaita merkittävät liiketoimintaa uhkaavat riskit. Keskeistä on myös tunnistaa riskien lähteet ja tapahtumat, joiden kautta riski voi realisoitua. Riskien tunnistamisessa on tyypillistä, että yritys käyttää ulkopuolisia palveluita riskien tunnistamiseen. Esimerkiksi riskikartoitukset yhteistyössä vakuutusyhtiön kanssa ovat yleisiä. Riskien tunnistamisen ulkoistaminen kokonaan ei kuitenkaan ole välttämättä järkevä vaihtoehto yritykselle. Vaghanin (1997, 107) mukaan ulkopuoliset tahot tarjoavat arvokasta palvelua riskien tunnistamiseen, mutta ulkopuolisella ei ole kokonaisvaltaista näkemystä yrityksestä ja sen liiketoiminnasta. Organisaation on myös itse osallistuttava riskikartoitukseen, jotta paras ymmärrys yrityksen riskeistä saavutetaan (Vaughan 1997, 107). Riskien tunnistaminen on myös jatkuva toimenpide, kun uusia liiketoimintaa uhkaavia riskejä syntyy yrityksen toimintaympäristöön.

Yrityksen kyky tunnistaa riskejä ja niiden muodostumista on tärkeää riittävän riskienhallinnan ylläpitämiseksi. Yrityksen riskien tunnistamisen tueksi Ilmonen ym. (2016, 110-111) esittelevät neljä riskien tunnistamismenetelmää: toteutuneisiin riskeihin perustuva tunnistamismenetelmä, tarkistuslistoihin (check-list) perustuva tunnistamismenetelmä, ryhmätyönä tehtävä riskien tunnistaminen (risk workshop) sekä induktiiviset päättelymenetelmät. Riskien tunnistamisen jälkeen tunnistetuista riskeistä on hyvä muodostaa riskirekisteri ja riskikartta, jotka ovat helposti ymmärrettävissä ja joita on mahdollista päivittää tarpeen mukaan säännöllisin väliajoin. Riskien tunnistamisen tulee olla hyvin ja selkeästi määritelty prosessi. Tämän avulla varmistetaan se, että riskien tunnistamisen lisäksi ne myös rekisteröidään asianmukaisesti. (Sweeting 2011, 112.)

Riskien tunnistamisen jälkeen tunnistettuja riskejä tulee arvioida niiden todennäköisyyden ja vakavuuden kannalta sekä arvioida niiden merkitystä liiketoiminnalle. Vaughanin (1997, 36) mukaan arviointiin sisältyy mahdollisen tappion määrän ja todennäköisyyden määrittäminen, jonka jälkeen riskit on niiden merkityksen perusteella mahdollista priorisoida. Riskin vaikutusten ja todennäköisyyden arviointiin voidaan riskin luonteesta riippuen käyttää kvalitatiivisia tai kvantitatiivisia arviointimenetelmiä. Myös niiden yhdistelmiä voidaan käyttää.

Kvalitatiivisten arviointimenetelmien avulla pyritään sanallisesti arvioimaan ja selittämään riskin vaikutukset liiketoiminnalla. Kvantitatiivinen arviointimenetelmä perustuu matematisoituun malliin, jonka avulla riskin taloudellisen tappion määrää on mahdollista arvioida. Esimerkiksi keskeytysriskin aiheuttama tappio liiketoiminnalle on mahdollista laskea. Riskin suuruuden määrittämiseksi sen todennäköisyyttä ja vakavuutta mitataan tavallisesti numeroidulla asteikolla yhdestä viiteen. Todennäköisyyden kohdalla pienempi luku tarkoittaa epätodennäköisempää riskin realisoitumista ja suurempi luku todennäköisempää. Vastaavasti vakavuutta arvioidessa pienempi luku tarkoittaa merkityksettömämpää riskiä ja suurempi luku liiketoiminnan kannalta vakavampaa.

Todennäköisyyden ja vakavuuden arvioinnin avulla voidaan muodostaa riskin merkitystä kuvaava riskitulo. Riskitulo saadaan kertomalla riskin vakavuus sen todennäköisyydellä. Juvosen ym. (2016, 22) mukaan riskitulossa tulee painottaa vakavuutta, sillä vakavuutta painottamalla voidaan suurin huomio kiinnittää riskejä arvioitaessa merkittävimpiin riskeihin, jotka voivat uhata toiminnan jatkuvuutta. Myös Vaughanin (1997, 36) mukaan tiettyjä riskejä, joiden vakavuus on suuri, tulee riskejä priorisoitaessa nostaa etusijalle.

Riskitulon laskeminen auttaa riskien merkityksen arviointia ja vertaamista toisiinsa. Riskit voidaan jakaa niiden liiketoiminnallisten taloudellisten vaikutusten perusteella riskin suuruutta kuvaaviin luokkiin. Vaughan (1997, 36) jakaa riskit taloudellisten vaikutusten perusteella kolmeen luokkaan: kriittisiin riskeihin, tärkeisiin riskeihin ja ei-tärkeisiin riskeihin. Riskien merkitysten arvioinnissa yritys voi peilata riskikohtaisten analyysien tuloksia strategiaan ja riskienottohaluun. Tämä helpottaa riskienhallintaprosessin seuraavaa vaihetta, riskienhallintakeinojen valintaa.

3.3 Riskienhallintatoimenpiteet

Riskien tunnistamisen ja arvioinnin jälkeen yrityksen tulee valita riskikohtaiset hallintatoimenpiteet riskien hallitsemiseksi. Toimenpiteiden valitsemisessa huomiota tulee kiinnittää riskin arviointivaiheen analyysiin ja riskin luonteeseen. Riskien arvioinnissa tunnistettujen kriittisten riskien ja priorisoinnin avulla voi olla järkevää kohdistaa eniten resursseja näille merkittävimmille riskeille. Myös yrityksen

riskinottohalu ja strategia tulee ottaa huomioon negatiivisten ja positiivisten riskien toimenpiteitä valitessa.

Ilmosen ym. (2016, 131) mukaan riskienhallintatoimenpiteet voidaan jakaa riskien kontrollointiin ja siirtämiseen, ensisijaisesti on pyrittävä riskienhallintatoimenpitein pienentämään riskin todennäköisyyttä sekä seurausta ja toissijaisesti vasta siirtää jäljelle jäävän riskin osuus kolmansille osapuolille. Riskienhallintakeinoja ovat riskin hyväksyminen, pienentäminen, poistaminen ja välttäminen sekä siirtäminen (Juvonen 2016, 101). Sweeting (2011, 413) jakaa menetelmät samankaltaisiin neljään osaan: pienentämiseen, poistamiseen, siirtämiseen ja hyväksymiseen. Menetelmien jako on hyvin samankaltainen erilaisissa prosessimalleissa. Lopullinen riskin hallintatoimenpide voi olla erilaisten menetelmien yhdistelmä. On kuitenkin tärkeää huomioida riskienhallinnan kustannusten suhde riskiin. Riskiin tulisi käyttää vain sen verran kustannuksia, kuin sen suuruus saadaan liiketoiminnan kannalta hyväksyttävälle tasolle.

Riskin poistamista kokonaan voidaan pitää parhaana mahdollisena tilanteena, mutta käytännössä poistaminen voi olla vaikea toteuttaa ja se voi tulla yritykselle kalliiksi. Juvosen ym. (2016, 25) mukaan riskin poistaminen on riskin välttämisen äärimmäinen muoto. Riskin välttäminen on ensisijainen keino merkitykseltään suurille riskeille. Riskin välttäminen aiheuttaa yritykselle menoja, jolloin johto joutuu pohtimaan kustannusten ja saavutetun hyödyn suhdetta. (Juvonen ym. 2016, 25). Riskin poistaminen voi tarkoittaa liiketoiminnosta tai investoinnista pidättäytymistä, mikä poistaa myös mahdollisen positiivisen riskin tai liiketoimintamahdollisuuden toteutumisen. Sweetingin (2011, 414) mukaan yritys voi riskin poistaakseen pidättäytyä hankkeen tai investoinnin toteuttamisesta, tai toteuttaa sen poikkeavalla tavalla. Ilmonen ym. (2016, 133) mainitsee riskien poistamisen yhteydessä nollatoleranssiriskit. Merkittävimpien henkilö-, ympäristö- ja turvallisuusriskien kohdalla riskien poistaminen mahdollisimman tarkoin on hyvin tärkeää. Riskien poistaminen vaatii optimointia kustannusten ja saavutetun hyödyn välillä. Vaikka riskin poistaminen epäonnistuu ja riskiä ei saada kokonaan poistettua, vaikutuksena riskin vakavuutta ja todennäköisyyttä onnistutaan usein pienentämään.

Riskin pienentäminen on riskin todennäköisyyden ja vaikutusten pienentämistä. Hopkinin (2018, 174) mukaan suurimpaan osaan riskeistä käytetään pienentämisen

hallintamenetelmää, jonka tarkoituksena on rajoittaa riskiä hyväksyttävälle tasolle samalla, kun yrityksen toiminta aiheuttaa riskiä. Riskin pienentämisen menetelmät voivat olla hyvin erilaisia ja usein hyväksyttävä riskin taso saavutetaan pienentämismenetelmien summana. Juvosen ym. (2016, 24) mukaan riskien pienentämistä pidetään usein merkittävimpänä riskienhallinnan keinona, joka tulee kyseeseen silloin, kun riskiä ei voida välttää tai siirtää. Esimerkkejä riskien pienentämiseen ovat esimerkiksi varautumissuunnitelmien laatiminen, henkilöstön koulutus ja liiketoiminnan kannalta tärkeiden laitteiden ja ohjelmistojen päivittäminen. Sweeting (2011, 413) lähestyy riskin pienentämistä sijoitustoiminnassa hajauttamisen ja riskien erilaisen keskinäisen korrelaation kautta, mutta lähestymistapaa voi hänen mukaansa soveltaa myös esimerkiksi yrityksen erilaisten projektien valintaan ja aloittamiseen.

Joidenkin riskien kohdalla riskin siirtäminen voi olla yrityksen kannalta paras vaihtoehto. Riskin seuraukset pyritään siirtämään toiselle osapuolelle. Hopkinin (2018, 178) mukaan riskin toteutumisen todennäköisyyden ollessa pieni, mutta vaikutusten ollessa suuria, yritys haluaa siirtää riskin. Riski voidaan siirtää toiselle osapuolelle kannettavaksi vakuuttamalla, sopimuksilla tai rahoitusratkaisuilla. Rahoitusratkaisuilla tarkoitetaan erilaisten johdannaisten ja rahastoivien ratkaisujen käyttöä riskienhallintavälineenä. (Ilmonen ym. 2016, 133.) Sopimuksien avulla riski voidaan siirtää esimerkiksi toiselle yritykselle tai alihankkijalle. Riskin siirtämisessä vakuuttaminen on yleinen tapa. Vakuutuksen avulla pystytään siirtämään riskin taloudelliset vaikutukset vakuutusyhtiölle, mutta vakuutus korvaa taloudellisia menetyksiä vain tiettyyn rajaan asti ja riskin muut vaikutukset jäävät yritykselle. Ilmosen ym. (2016, 134) mukaan parhaassakin tapauksessa yritykselle voi jäädä kustannukseksi omavastuun lisäksi maineriskejä sekä viivästyksien ja ylimääräisen työn aiheuttamia kuluja. Vahingon uhka jää vakuuttamisen jälkeen yritykselle, joten riskin siirtämisen jälkeen riski vaatii usein myös muita hallintamenetelmiä.

Riski voidaan hyväksyä ja jättää omalle vastuulle, jos riskin arvioinnin perusteella se nähdään järkeväksi. Riski voi merkitykseltään olla niin vähäinen tai epätodennäköinen, ettei yritys katso tarpeelliseksi käyttää siihen resursseja. Hopkinin (2018, 174) mukaan toimenpiteitä ei joskus tehdä, vaikka riski ei olisi siedettävä, koska joidenkin riskien hallitseminen voi olla rajallista tai riskienhallintatoimenpiteiden tekemisestä koituvat kustannukset ovat suhteettomia saavutettuun hyötyyn nähden. Toimenpiteiden tekeminen

voi aiheuttaa riskin kohdalla liikaa kuluja tai merkitykseltään pienen riskin kohdalla seuraamukset voivat taloudellisesti olla pienempiä, mitä hallintakeinoihin on käytetty taloudellisia resursseja. Riski voi myös jäädä tiedostamatta omalle vastuulle, jos yritys epäonnistuu riskien tunnistamissa ja arvioinnissa.

3.4 Riskienhallintaprosessin seuranta, arviointi ja jatkuva parantaminen

Riskienhallinnan prosessin viimeisenä vaiheena on teoriassa prosessin seuranta, arviointi ja jatkuva parantaminen. Vaiheeseen voidaan myös sisällyttää riskienhallinnan ja riskien dokumentaatiota, raportointia ja auditointia. Prosessin seurannan ja arvioimisen avulla riskienhallintaa voidaan kehittää ja sen tehokkuutta arvioida. Vaughanin (1997, 74) mukaan huolimatta siitä, että seuranta ja arviointi ovat riskienhallintaprosessin viimeinen vaihe, se on toistuva ja jatkuva toiminto. Riskienhallintaprosessin seurantaan ja arviointiin on kaksi syytä. Ensinnäkin riskit kehittyvät ja uusia riskejä syntyy, jonka seurauksena ennestään sopivia riskienhallinnan toimenpiteitä ja menetelmiä voidaan joutua kehittämään. Toisena, virheitä sattuu ja riskeille altistuminen voi jäädä huomioimatta. Toimenpiteet, jotka on valittu riskien hallitsemiseksi eivät välttämättä ole olleet sopivia tai niitä ei ole pantu käytäntöön asianmukaisella tavalla. Prosessin tarkastelu mahdollistaa havaitsemaan aikaisempia virheitä. (Vaughan 1997, 74.) Seurannan ja arvioinnin vaihe sisältää prosessin jokaisen vaiheen toimenpiteiden ja riskien käsittelyn onnistumisen arviointia tavoitteisiin peilaten, joka mahdollistaa prosessin jatkuvan parantamisen. Ilmosen ym. (2016, 105) mukaan jatkuva parantaminen on olennainen osa kokonaisvaltaista riskienhallintaprosessia.

Sweetingin (2011, 457) mukaan aikaisempien riskienhallintaprosessin vaiheiden jälkeen tulisi suorittaa jatkuvasti myös muita toimintoja, joita ovat dokumentointi, viestintä ja auditointi. Dokumentaatio viittaa prosessiin, jossa kaikki riskienhallintaprosessin vaiheet ja näkökulmat kirjataan (Sweeting 2011, 457). Dokumentaation tulisi kattaa riskien tunnistamisen ja arvioinnin vaiheen lisäksi kaikki muut prosessin vaiheet. Tämän avulla helpotetaan prosessin arviointia ja kehittämistä. Viestinnän avulla mahdollistetaan toimiva riskienhallinnan toteuttaminen ja selkeä vastuualueiden jako. Viestinnällä viitataan myös raportointiin, joka voidaan jakaa yrityksen sisäiseen ja ulkoiseen

raportointiin. Ulkoinen riskienhallintaraportointi tarkoittaa julkista ja sidosryhmäraportointia (Ilmonen ym. 2016, 202). Ulkoiseen raportointiin liittyy listatun yhtiön tapauksessa säännellympiä vaatimuksia, joiden avulla taataan riittävä informaatio kaikille ulkoisille sidosryhmille. Sisäinen raportointi tukee yrityksen riskienhallintaprosessia ja operatiivista toimintaa. Sisäiseen raportointiin liittyvät johdon riskiraportoinnit, joiden painopiste on Ilmosen ym. (2016, 202) mukaan siirtynyt riskienhallintatoimenpiteiden ja niiden vaikuttavuuden seurantaan ja tulevaisuuden arviointiin ennakoimaan, mihin suuntaan riskit kehittyvät.

Yritys voi toteuttaa riskienhallinnan auditointia riskienhallintaprosessin arvioimisen ja seuraamisen lisäksi. Riskienhallinnan auditointi on yksityiskohtainen ja järjestelmällinen arvio riskienhallinnasta, jonka tarkoituksena on selvittää, ovatko riskienhallinnan tavoitteet sopivia yrityksen tavoitteisiin, ovatko tavoitteiden saavuttamiseksi tehdyt toimenpiteet sopivia ja onko toimenpiteet toteutettu asianmukaisella tavalla (Vaughan 1997, 75).

4 TUTKIMUSTULOKSET

4.1 Yritysesittely

Yritys Oyj. on suomalainen elintarvikealan yritys, jonka liikevaihto on noin 1,5 miljardia euroa (2019). Yrityksen osake on ollut listattuna Nasdaq Helsinki Oy:ssä vuodesta 1991 lähtien. Yrityksen asiakasryhmiä ovat päivittäistavarakauppa, Food Service -asiakkaat ja alan teollisuus.

Yrityksen toiminta jakaantuu neljään liiketoiminta-alueeseen (Suomi, Ruotsi, Venäjä sekä Tanska & Baltia) ja kotimarkkinoiden lisäksi sillä on laajaa vientitoimintaa Yhdysvaltoihin, Koreaan ja Kiinan. Suomen liiketoiminta-alueen liikevaihto vastaa noin 70% koko konsernin liikevaihdosta ja markkina-asemaltaan yritys on useimpien päätuoteryhmiensä markkinajohtaja Suomessa. Yrityksen strategisena tavoitteena on uusiutua ja kasvaa johtavaksi pohjoiseurooppalaiseksi ruokataloksi.

4.2 Aineiston kuvaus

Tutkimuksen empiirinen aineisto kerättiin haastattelun avulla. Haastattelu toteutettiin puolistrukturoituna teemahaastatteluna. Haastattelu oli lisäksi parihaastattelu. Haastattelun tarkoituksena oli saada yleiskuva kohdeyrityksen riskienhallinnan toteuttamisesta konsernin tasolla ja saada yksityiskohtaisempi kuva yrityksen kyberriskeistä ja niiden hallintaprosessista keskittyen erityisesti tutkimuskysymysten mukaisiin vaiheisiin prosessissa. Molempien haastateltavien haastattelu toteutettiin samalla kertaa ja haastateltavat pystyivät täydentämään toistensa vastauksia ja tuomaan asioita esiin omista näkökulmistaan.

Tutkimuksen aineistoa varten haastateltiin kahta henkilöä. Haastatelluista asiantuntija A on Yritys Oyj:n Group Controller. Hän on koulutukseltaan kauppatieteiden lisensiaatti ja työskennellyt kohdeyrityksessä noin kuusi vuotta. Hänen vastuualueinaan ovat

tilintarkastus, sisäinen tarkastus, rajat ylittävä verotus sekä vakuuttaminen ja riskienhallinta. Lisäksi kohdeyrityksen julkaisema talousinformaatio kulkee hänen organisaationsa kautta. Toinen haastatelluista henkilöistä asiantuntija B on Yritys Oyj:n ICT Technical Manager. Hän on koulutukseltaan diplomi-insinööri ja työskennellyt kohdeyrityksessä noin puolitoista vuotta. Ennen kohdeyritykseen tuloa hän on työskennellyt vuoden ulkoisena konsulttina yritykselle. Hänen vastuualueinaan ovat tietoturva ja loppukäyttäjän palvelut. Haastateltavat valittiin tutkielmaan heidän toimenkuvansa ja laajan osaamisensa vuoksi erityisesti riskienhallinnan ja kyberriskien parissa. Haastateltaviin viitataan jatkossa heidän tehtävänimikkeillään.

Haastattelu toteutettiin etäyhteydellä Microsoft Teams -sovelluksen avulla ja haastattelu nauhoitettiin haastateltavien luvalla. Haastattelun aineisto saatettiin kirjalliseen muotoon litteroimalla vuorokauden kuluessa haastattelusta. Haastattelurunko lähetettiin haastateltaville henkilöille etukäteen sähköpostilla ja haastattelua varten varattiin aikaa kattavasti kahdeksi tunniksi. Haastattelun kesto oli kokonaisuudessaan noin puolitoista tuntia.

Haastattelurunkoon kuului kokonaisuudessaan neljätoista kysymystä ja runko löytyy kokonaisuudessaan liitteestä 1. Ensimmäiset kysymykset keskittyivät kohdeyrityksen konsernitason riskienhallintaan ja sen toteutukseen, jotta tutkimuksen kohdeyrityksen riskienhallinasta saataisiin mahdollisimman hyvä yleiskuva ja kyberriskien hallintaa olisi helpompi arvioida tätä tietoa vasten. Seuraavat kysymykset rakentuivat riskienhallintaprosessin vaiheiden ympärille painottaen kyberriskien tunnistamisen, arvioinnin ja hallintakeinojen vaiheita. Prosessin ympärille rakentuvien kysymysten jälkeen haastateltavilta kysyttiin kyberriskien tulevaisuuden merkityksestä ja mahdollistettiin tutkimuksen kannalta keskeisten asioiden läpikäynti, jotka eivät tulleet haastattelun aikana muuten ilmi. Haastatteluiden tiedot, joiden pohjalta aineisto rakentuu, on kerrottu haastateltavien toimesta yleisellä tasolla, jotta mitään yrityksen kannalta kriittistä tietoa ei tutkimuksen kautta tule julkiseksi. Jatkossa tässä pääluvussa lyhennetään tutkimuksen kohdeyritys Yritykseksi.

4.3 Yrityksen riskienhallinnan järjestäminen yleisellä tasolla

Group Controllerin mukaan riskienhallinnan tavoitteena on Yrityksessä tukea strategian toteutumista ja tavoitteiden saavuttamista sekä organisaation kehittymistä strategiassa määritetyssä toimintaympäristössä. Lisäksi Yritys pyrkii riskienhallinnallaan ehkäisemään epäsuotuisia tapahtumia ja suojaamaan liiketoiminnan jatkuvuutta. Politiikkatason riskienhallinnan tavoitteet asettaa Yrityksen hallitus. Hallituksen asettaman riskienhallintapolitiikan lisäksi eri organisaatiotasoilla voidaan asettaa alatavoitteita. Group Controller mainitsee alatavoitteiden asettajiksi esimerkkinä konsernin toimitusjohtajan, talousjohtajan sekä liiketoiminta-alueiden johtajat johtoryhmineen.

Hallituksen rooli riskienhallinnassa riskienhallintapolitiikan laatimisen lisäksi on valvoa politiikassa määritettyjen periaatteiden toimeenpanoa ja osallistua strategisten riskien arviointiin ja tunnistamiseen. Toimitusjohtaja vastaa riskienhallinnan asianmukaisesta järjestämisestä ja muut konsernin johtoryhmän jäsenet ovat vastuussa riskienhallinnan toimeenpanosta sekä riskien tunnistamisesta ja arvioimisesta omilla vastuualueillaan. Edelleen eri Yrityksen liiketoiminta-alueet vastaavat riskienhallinnastaan omilla alueillaan ja raportoivat riskejä. Riskiraportoinnin ylläpidosta vastaa konsernin talousjohtaja, joka raportoi tunnistetut riskit ja riskienhallinnan toimenpiteet hallitukselle Yrityksen vuosiohjelman mukaisesti.

Riskienhallintaa toteutetaan Yrityksessä vuosikellon mukaan. Pääsääntöisesti keväällä hallitus ja konsernin johto tunnistavat strategisia riskejä, jonka pohjalta syntyvä aineisto lähetetään liiketoiminta-alueille budjettiprosessiin kuuluvan riskienhallinta-aineiston kanssa. Riskienhallintaa ohjaa lisäksi riskienhallintaohjeistus, joka toimintaohjeen mukaisesti asettaa riskienhallinnalle minimitason. Group Controllerin mukaan aina tarpeen vaatiessa tehdään riskienhallinnassa minimitason ylittäviä toimenpiteitä. Group Controller korostaa myös jokaisen Yrityksen työntekijän vastuuta riskienhallinnassa. Kaikki työntekijät ovat vastuussa omaan työhönsä liittyvien riskien tunnistamisessa, arvioinnissa, ehkäisemisessä ja riskien esille tuomisesta.

Yritys käyttää riskienhallinnassaan apuna soveltuvin osin ISO31000 ja ISO31010 viitekehyksiä. Lisäksi Yritys huomio pörssiyhtiönä riskienhallinnan järjestämisessä Arvopaperimarkkinayhdistys ry:n julkaiseman hallinnointikoodi corporate governancen mukaisia vaatimuksia listayhtiöille. Group Controllerin mukaan laadittu riskikartta ohjaa myös Yrityksen riskienhallintaa ja erityisesti yhtenäistää konsernin sisäistä viestintää. Riskikartta mahdollistaa yhtenäisen riskienhallinnan kielen jakaen riskit neljään pääluokkaan ja edelleen riskien alaluokkiin.

Group Controller nostaa esiin heti haastattelun alussa myös riskin positiivisen puolen olemassa olemisen. Hänen mukaansa riskit nähdään usein negatiivisena ja epäsuotuisena asiana, mutta hän korostaa riskien olevan Yritykselle myös mahdollisuuksia. Kilpailutekijöitä ja liiketoimintamahdollisuuksia pyritään aktiivisesti tunnistamaan strategioiden ja riskikartoituksien yhteydessä.

4.4 Kyberriskien merkitys

Kysyessä kyberriskien merkittävyydestä muihin riskeihin verrattuna, nousevat ne merkittäväksi ja kuuluvat Group Controllerin mukaan Yrityksen viiden merkittävimmän riskin joukkoon. Haastateltavat mieltävät riskin vahvasti keskeytysriskiin ja pitävät sitä erityisesti keskeytysriskin riskitekijänä. Haastateltavien mukaan kyberriskit mielletään liikaa liiketoiminnasta erillisiksi riskeiksi, joiden ajatellaan helposti olevan vain teknistä tietohallinnon asiaa. Group Controller nostaa esimerkkinä esille kybervakuutuksen ja liiketoiminnan keskeytysvakuutuksen. Kyberriskin aiheuttamaa toiminnan keskeytymistä ei korvata keskeytysvakuutuksesta tai korvaussumma on hyvin rajallinen. Tästä syystä suuremmat yritykset joutuvat ottamaan kaksi erillistä vakuutusta. Haastateltavat pitävät tätä outona, sillä liiketoiminnan keskeytyminen voi johtua lopulta hyvin moninaisista eri tekijöistä, joita on vaikea erottaa toisistaan. Tämän lisäksi lähes kaikki liiketoiminta vaatii nykyään erilaisia verkossa olevia tietoteknisiä järjestelmiä ja niiden käyttöä. Group Controller painottaa, että kyberriskit ovat integroitu osa Yritysten liiketoimintaa, jota on vaikea ajatella erilliseksi vakuuttamisen tai Yrityksen liiketoiminnan kannalta.

ICT Technical Manager nostaa kyberriskien luonteeseen liittyen esille niihin yleisesti liittyvän haasteen. Hänen mukaansa kyberriskit mielletään liian yleisesti liiketoiminnassa

irrallisiksi tietoteknisiksi koodinpätkiksi. Tietojärjestelmistä, tietokoneista ja muista IT-maailmaan liittyvistä asioista puhuminen vaikeuttaa hänen mukaansa yhdistämästä kyberriskejä tavallisiin päivittäisiin liiketoimintoihin, koska ihmiset kokevat tekniset asiat itsestä kaukaisiksi. Vaikka ihmiset ovat päivittäin tekemisissä liiketoimintajärjestelmien kanssa, koetaan kyberriskit helposti monimutkaisiksi tietohallinnon riskeiksi, joilta suojautumisen tietohallinto on miettinyt loppuun asti valmiiksi. Group Controller on asiasta samaa mieltä ja sanoo, että juuri tästä syystä Yrityksessä pyritään korostamaan jokaisen olevan vastuussa kaikista riskeistä, kyberriskit mukaan lukien.

Erilaisista kyberriskeistä ja kyberuhista haastattelussa Yrityksen merkittävimmiksi nousevat liiketoiminnan keskeytymiseen johtavat kyberriskit. Palvelunestohyökkäykset ja muut liiketoimintakriittisiin järjestelmiin kohdistuvat kyberriskit voivat vaikutuksiltaan olla hyvin suuria. ICT Technical Manager nostaa yhdeksi keskeytyksen aiheuttamaksi kyberriskiksi kiristyshaittaohjelman leviämisen konesaliin, mikä voisi johtaa liiketoimintakriittisten järjestelmien alhaalla olemiseen, joka voisi tarkoittaa Yrityksen tehtaiden toiminnan keskeytymistä. ICT Technical Manager puhuu kyberriskien ja kriittisten liiketoimintajärjestelmien yhteydessä saatavuudesta ja saatavuusriskistä. Jos järjestelmät eivät ole saatavilla, esimerkiksi logistiikan ohjausjärjestelmä tai toiminnanohjausjärjestelmä, seurauksena voivat olla suuret taloudelliset menetykset. Myös Group Controller pitää liiketoiminnan keskeytykseen johtavia kyberriskejä kaikkein merkittävimpinä.

Tiedon luottamuksen osalta kyberriskejä pidetään keskeytykseen johtavia kyberriskejä pienempinä. Haastateltavat tiedostavat lisääntyneen regulaation myötä kasvavat tietovuotojen vaikutukset, mutta hallussa olevan arkaluontoisen tiedon määrää pidetään pienenä, varsinkin suorien kuluttaja-asiakkaiden ja kolmansien osapuolien osalta. Yrityksen liiketoiminta ei haastateltavien mukaan nojaa arkaluontoisen tiedon käsittelyyn ja hallussapitoon. Tiedon luottamuksen osalta riski liittyy enemmän oman henkilöstön tietojen käsittelyyn.

Kyberriskien aiheuttaman keskeytysriskin korostuessa kyberriskien taloudelliset vaikutukset nousevat vaikutuksiltaan suurimmiksi seurauksiksi Yrityksen liiketoimintaan. Haastateltavien mukaan taloudelliset vaikutukset johtuvat erityisesti

liiketoiminnan keskeytymisestä. Tietovuotojen taloudellisia vaikutuksia ei pidetä yhtä merkittävinä, mutta tietovuotojen vaikutukset nähdään etenkin välillisinä mainehaittoina. ICT Technical Managerin mukaan tietovuodon tapahtuessa välilliset vaikutukset voivat olla merkittäviä, vaikka liiketoiminnan kannalta tärkeää tai luottamuksellista tietoa ei vuodettaisi. Hän nostaa esimerkiksi sähköpostitilien hakkeroimisen tai yksittäisten sähköpostien vuotamisen. Mainehaitat sähköpostien vuodosta voivat olla merkittäviä, vaikka ne eivät sisältäisi tärkeää luottamuksellista tietoa. Group Controller nostaa esiin välillisenä vahinkona mainehaitan, joka voisi tapahtua liiketoiminnan keskeytymisestä johtuvien taloudellisten tappioiden lisäksi. Tuotannon ja tilausten toimittamisen keskeytyminen voisi hänen mukaansa johtaa mainehaittoihin ja epävarmuuteen siitä, miten Yritys pystyy jatkossa toimittamaan tilauksia ja pystytäänkö toimitusten jatkuvuuteen luottamaan.

Haastateltavat uskovat kyberriskien merkityksen kasvavan tulevaisuudessa jatkuvasti. ICT Technical Manager nostaa esiin automatisaation, digitalisaation ja pilvipalvelut, jotka toimivat ajureina merkityksen kasvamiselle. Lisäksi yritystoiminnan tehostamistarve vaatii digitalisaation ja automaation lisäämistä, mikä tarkoittaa lisääntyvää tietotekniikan roolia ja suorien kyberuhkien lisääntymistä. Koneiden verkottamisen ja automaation lisääminen lisää hänen mukaansa vastuita siitä, että verkotettuja laitteita ei voitaisi ajaa kerralla alas haitallisen tahon toimesta.

ICT Technical Manager nostaa esille koronaviruspandemian aiheuttamat muutokset perinteiseen työntekoon. Maailma on ottanut pandemian aikana harppauksen eteenpäin ja työskentelyn tulee olla mahdollista mistä ja milloin vain. Hän uskoo etätyöskentelyn yleistyvän jatkossa entisestään. Pilvipalvelut lisääntyvät ja konesalissa olevien järjestelmien käyttö ei vaadi enää työskentelyä omalta työpisteeltä. Pilvipalveluiden lisääntyminen vaatii hänen mukaansa uutta näkökulmaa kyberriskien ja tietoturvakontrollien rakentamiseen. Group Controller nostaa esille myös tiedon ja datan entistä nopeamman leviämisen verkossa. Tiedon nopea leviäminen voi kasvattaa kyberriskejä entuudestaan. Hän käyttää esimerkkinä tiedon leviämisestä sitä, kuinka nopeasti julkisuudessa esillä olleissa tapauksissa tieto verkon suojauksen aukoista on levinnyt muille haitallisille tahoille. Haastateltavat nostavat myös disinformaation lisääntymisen kasvavaksi riskiksi yrityksille.

4.5 Kyberriskien tunnistaminen ja arviointi

ICT Technical Managerin mukaan kyberriskien tunnistaminen on Yrityksellä hyvin pitkälti tietohallinnon varassa. Yrityksen tietohallinto pyrkii tunnistamaan säännöllisin väliajoin laaja-alaisia koko IT-infrastruktuuria koskevia riskejä. Uusien järjestelmien ja tietoteknisten ratkaisujen käyttöönoton myötä riskien tunnistamiseen panostetaan ja keskitytään huolellisesti. Riskikartoitukset ovat kyberriskien osalta pitkälti tietohallinnon sisäisiä, mutta myös liiketoimintojen puolelta riskejä pyritään tunnistamaan enenevissä määrin. Hänen mukaansa olisi tärkeää, että myös liiketoimintajärjestelmiä käyttävät kykenisivät tunnistamaan käytettävien järjestelmien kriittisyyttä saatavuuden osalta ja pyrkisivät tunnistamaan saatavuuteen liittyviä riskejä. Aika ajoin merkittäviä kyberriskeihin liittyviä muutostarpeita nostetaankin liiketoimintojen puolelta esiin. Group Controllerin mukaan riskikartoituksia tehdään säännöllisin väliajoin yhteistyössä vakuutusyhtiön kanssa, mutta kyberriskien osalta erillistä kartoitusta ei vielä olla tehty. Hän pitää vakuutusyhtiön riskikartoitusta kuitenkin mahdollisuutena täydentää tietohallinnon sisäisiä riskikartoituksia.

Riskien arvioinnin apuna käytetään ICT Technical Managerin mukaan riskienarviointityökalua, jonka avulla arvioidaan riskien todennäköisyyksiä ja vaikutuksia. Riskienarviointityökalun avulla riskianalyysiin pyritään lisäämään kvantitatiivisuutta. Pääosin kyberriskien arvioiminen on kuitenkin kvalitatiivista. Hänen mukaansa riskien tarkkojen todennäköisyyksien ja vaikutusten analyysi on aina haasteellista ja perustuu osin arvauksille. Haasteelliseksi nähdään myös numeeristen analyysien vertailukelpoisuus. Todennäköisyyksien ja vaikutusten arviointi esimerkiksi asteikolla yhdestä viiteen voi yrityksen sisällä saada useita merkityksiä ilman selkeitä yhtenäisiä kriteerejä. Tämä vaikeuttaa riskien keskinäistä vertailua.

Yrityksellä on paljon merkittäviä riskejä, jotka vaativat reagointia. ICT Technical Managerin mukaan liiallinen riskien arviointi ja kartoitus syö paljon resursseja itse riskien ratkaisemiselta ja pienentämiseltä. Tietohallinnossa pystytään sisäisesti hiljaisen tiedon varassa ymmärtämään kyberriskien kokoluokkaa ja asettamaan riskejä merkittävyydeltään järjestykseen. Hän pohtii näkökulmaa riskien arviointimenetelmän valintaan ja rajanvetoa sille, milloin riskien arviointi vaatii kvantitatiivista arviointia ja

koska kvalitatiivinen on riittävää. Kuitenkin kaikkein tärkeimpänä hän pitää sitä, että riskienarviointimenetelmistä riippumatta arviointia tehdään. Menetelmä on lopulta toissijainen asia ja ongelmallisinta olisi, jos analyysiä ei tehtäisi ollenkaan.

Haastateltavien mukaan tietohallinnon rooli on suuri myös kyberriskien arvioinnissa. ICT Technical Managerin mukaan riskien yksityiskohtainen arviointi vaatii kuitenkin yhteistyötä liiketoimintojen ja tietohallinnon välillä. Erityisesti kyberriskien vaikutusten arviointi vaatii panosta liiketoiminnoilta. Liiketoimintaomisteisten järjestelmien tulisi kyetä arvioimaan, mitkä ovat järjestelmälle mahdollisia uhkia ja millaisia vaikutuksia järjestelmien kaatumisella on liiketoimintaan. Edelleen tietohallinnon konsultoinnilla riskeistä saadaan kokonaisvaltaisempi kuva huomioimalla järjestelmien yksityiskohtaisemmat tekniset puitteet. Hänen mukaansa liiketoimintojen panos kyberriskien arviointiin ei vaadi käytännössä tekniikkaa ja sen tarkempaa tietämystä liiketoiminnallisten vaikutusten osalta. Haaste liittyy haastateltavien mukaan jo aiemmin mainittuun kyberriskien luonteeseen ja ihmisten käsityksiin. Kyberriskit mielletään turhaan äärimmäisen monimutkaisiksi ja irrallisiksi asioiksi. ICT Technical Managerin mukaan haaste on hänelle tuttu konsulttimaailmasta ja pörssiyhtiöistä, liiketoiminnoille kyberriskien arviointi on tavallisesti todella haasteellista.

Kyberriskien taloudellisten vaikutusten arviointi on haastateltavien mukaan helpompaa järjestelmiin kohdistuvien ja keskeytyksen aiheuttavien riskien osalta. ICT Technical Managerin mukaan liiketoimintakriittisten järjestelmien esimerkiksi toiminnanohjausjärjestelmän ja logistiikan ohjauksen osalta Yrityksessä ollaan tietoisia kyberriskien taloudellisista vaikutuksista. Liiketoiminnan seisomiselle pystytään muodostamaan suhteellisen tarkka arvio taloudellisista tappioista, mutta vähemmän kriittisten järjestelmien kaatumiselle ja muille erilaisille vaikutuksille rahallisen menetyksen suuruuden arvioiminen on vaikeaa.

4.6 Kyberriskien hallintatoimenpiteet

Kyberriskien hallinnasta kysyttäessä haastateltavat nostavat esille kolme keskeisintä keinoa riskien hallitsemiseen. ICT Technical Managerin mukaan Yrityksellä on ensinnäkin tarkat linjaukset tietohallinnossa liiketoimintakriittisten järjestelmien

hankinnoista ja teknisistä kontrolleista. Teknisiin kontrolleihin sisältyy tietoturvakontrolleja, verkkojen kahdentamista ja useampien varajärjestelmien luomista liiketoimintakriittisille järjestelmille. Varajärjestelmien osalta on tunnistettu, että niiden luominen mahdollisimman aikaisessa vaiheessa on tärkeää.

Toisena keinona nousee esille kyberriskien tietoisuuden lisääminen. ICT Technical Managerin mukaan se on hyvin yksinkertainen asia, mutta yksi merkittävimmistä kyberriskien ehkäisyssä. Työntekijöitä pyritään valistamaan kyberriskeistä ja muistuttamaan niiden olemassaolosta erilaisten koulutusten avulla. Group Controller kehuu tietohallinnon luomia koulutuksia ja korostaa niillä olevan iso merkitys. ICT Technical Managerin mukaan tietoisuuden lisäämisen rooli on suuri, koska tietohallinnolla ei ole silmiä kaikkialle. Kyberriskien olemassaolo ja merkitys tulee olla iskostettuna ihmisten mieleen. Palkitsevaa on, kun tietohallinnon ulkopuolelta otetaan yhteyttä kyberriskeihin ja järjestelmien tietoturvaan liittyvistä asioista. Esiin nostetut huolet saattavat paljastaa mahdollisia aukkoja järjestelmissä, joita ei olla osattu ottaa aiemmin huomioon.

Haastateltavat nostavat kolmantena esille kybervakuutuksen. Kybervakuutus on Yritykselle vielä suhteellisen uusi ja molemmat haastateltavat ovat osallistuneet kybervakuutusneuvotteluihin vakuutusyhtiön kanssa. Kybervakuutuksen avulla varaudutaan Yrityksessä kyberriskien taloudellisten vaikutusten varalta. Group Controller pitää yleisesti vakuutuksia merkittävinä ja yritysten osittaista riskien taloudellisten vaikutusten siirtoa vakuutuksiin tärkeänä. Yrityksellä tulee olla kuitenkin omaa aloitteellisuutta riskien tunnistamiseen ja hallitsemiseen. Vakuutus ei korvaa kaikkea ja vakuutuksiin liittyy aina myös omavastuut.

Aiemmin mainitun mukaisesti, haastateltavia kummastuttaa erillisen kybervakuutuksen ja keskeytysvakuutuksen tarpeellisuus. Luonteeltaan kybervakuutus on kuitenkin keskeytysvakuutus. Group Controller pitää kyberriskejä sellaisena, joita on mahdollista vakuuttaa hyvin rajallisesti taloudellisten vaikutusten määrään nähden. Liiketoiminnan keskeytysvakuutukseen kuuluu kattavat liikevaihtoon ja katetasoihin liittyvät korvaussummat, mutta kybervakuutuksen summa on kiinteä, vaikka taloudelliset menetykset voivat kyberriskin aiheuttamassa keskeytyksessä olla samaa luokkaa. Haastateltavien mukaan Yrityksen liiketoiminnassa on niin massiiviset päivittäiset

myynnin volyymit, etteivät he koe kybervakuutuksen takaavan aivan riittävää vakuutusta taloudellisille menetyksille.

ICT Technical Managerin mukaan kybervakuutus ei ole IT-asiaa ja se on pidettävä erillään kyberriskien muista hallintakeinoista. Kybervakuutus ei korvaa yhtäkään tietoturvakontrollia, eikä se voi olla vaihtoehto muille kyberriskien pienentämisen menetelmille. Päätöstä ei voida tehdä tietoturvakontrollien rakentamisen ja kybervakuutuksen ottamisen välillä.

Riskien hallintamenetelmiin liittyen Group Controller nostaa esille jatkuvuussuunnitelmat. Jatkuvuussuunnitelmien merkitys riskienhallinnassa on suuri ja niiden laatiminen helpottaa riskien ymmärtämistä. Riskien realisoituessa suunnitelma toimii viitekehyksenä toimenpiteille. Kyberriskeille jatkuvuussuunnitelmaa ei ole vielä laadittu, mutta sen laatimisesta puhuttiin kybervakuutuksen neuvottelujen yhteydessä ja sen tarpeellisuus on huomioitu. ICT Technical Managerin mukaan kyberriskien realisoitumisen varalle on olemassa selvät sävelet toimenpiteiden varalle, mutta dokumentoitu suunnitelma riskien varalle olisi hyvä ajan ja resurssien puitteissa. Ensimmäisenä lähtökohtana varautumiselle hän pitää kuitenkin selkeää vastuiden jakoa ja sitä, että jokaisella järjestelmällä on vastuussa oleva omistaja. Vastuutetuilla henkilöillä on motivaatiota ja ymmärrystä kontaktoida oikeita henkilöitä ja ryhtyä tarvittaviin toimenpiteisiin. Ongelma syntyy siinä vaiheessa, kun kyberriskin realisoituessa vastuuhenkilöä riittävällä osaamisella ei tiedetä.

Kysyttäessä kyberriskien hallintakeinojen riittävyydestä haastateltavat ovat yhtä mieltä siitä, ettei ideaalitilannetta ole ja ikinä ei voida sanoa keinojen olevan täysin riittäviä. Kyberriskien hallinta on jatkuvaa arviointia siitä, koska ollaan suotuisassa tilanteessa ja riskit on saatettu hyväksyttävälle tasolle Yrityksen kannalta. ICT Technical Managerin mukaan riskejä voidaan aina pienentää ja on tärkeää tunnistaa kyberriskien osalta relevantit riskienhallintakeinot resurssien puitteissa. Investoinnit kyberriskien pienentämiseksi voivat olla suuria tai pieniä, mutta lopullisten keinojen valinnan analyysissä tulee huomio kiinnittää siihen lisäarvoon, mikä saavutetaan suhteessa käytettyihin resursseihin. Hän käyttää esimerkkinä tietoturvavalvomon suunnittelua. Valvomo on kallis investointi, jonka toteuttaminen riippuu siitä, tuottaako se riittävästi lisäarvoa kyberriskien pienentämiseen. Toisena esimerkkinä hän mainitsee

sähköpostitilien kaksivaiheisen tunnistautumisen. Tunnistautuminen on ollut yksinkertainen ja taloudellisesti halpa kyberriskien pienentämisen keino toteuttaa, mutta se on ollut vaikutuksiltaan hyvin tehokas. Yrityksessä pyritään riskienhallinnassa tunnistamaan edullisia ja tehokkaita hallintakeinoja kyberriskeille, mutta myös suurempia investointeja harkitaan riskien hallitsemiseksi.

Yrityksessä kyberriskien tunnistamista, arviointia ja hallintakeinojen arviointia toteutetaan säännöllisesti jatkuvana prosessina. Uusia riskejä pyritään kartoittamaan ja erityisesti kaikkein merkittävimpiä kyberriskejä ja niiden tilannetta arvioidaan uudelleen säännöllisin väliajoin. Riskienhallintakeinojen osalta pyritään tunnistamaan tehokkaita kyberriskejä pienentäviä keinoja, jotta riskit saadaan hyväksyttävälle tasolle. ICT Technical Managerin mukaan kyberriskien sisäisen raportoinnin osalta suurimman vastuun omaava tietohallinto viestii tietohallintojohtajan kautta riskeistä edelleen yrityksen johdolle. Tiettyjen välittömiä toimenpiteitä vaativien yksityiskohtaisten kyberriskien osalta, jotka eivät vaadi johtoryhmän käsittelyä, tietohallinto ja liiketoiminnot viestivät keskenään osana päivittäisiä riskienhallinnan toimintoja.

5 YHTEENVETO

5.1 Tutkimuskysymyksiin vastaaminen

Ensimmäisen tutkimuskysymyksen avulla pyrittiin selvittämään kyberriskien merkitystä kohdeyritykselle ja syitä koetulle merkitykselle. Yritys pitää kyberriskejä merkittävyydeltään yhtenä liiketoiminnan merkittävimmistä riskeistä. Kyberriskejä pidetään merkittävänä erityisesti niiden liiketoiminnan mahdolliseen keskeytymiseen johtavien vaikutusten vuoksi ja tässä yhteydessä Yritys puhuu liiketoimintakriittisten järjestelmien saatavuusriskistä. Tiedon luottamuksen osalta kyberriskejä pidetään keskeytymiseen johtavia kyberriskejä pienempinä, sillä Yrityksen liiketoiminta ei perustu arkaluontoisen tiedon käsittelyyn ja hallussapitoon. Tiedon luottamuksen osalta riski liittyy suurimmilta osin vain omaan henkilöstöön. Tutkielman teorian mukaisesti kyberriskien vaikutusten osalta taloudellisia vaikutuksia pidetään kaikkein merkittävimpinä. Taloudellisissa vaikutuksissa korostuvat kuitenkin lähinnä välittömät vaikutukset. Välilliset vaikutukset nähdään enemmän mainehaittoina, jotka voivat olla merkittäviä, vaikka niillä ei olisi suoria liiketoiminnallisia vaikutuksia Yritykseen.

Yrityksen kannalta merkittävimmiksi kyberuhiksi nousevat liiketoiminnan keskeytymiseen johtavat kyberuhat. Haastattelujen pohjalta erilaiset haittaohjelmat ja palvelunestohyökkäykset mainitaan Yrityksen kannalta relevanteiksi ja ne nostetaan merkittäviksi myös teorian perusteella. Esimerkiksi Choo (2011) ja ENISA (2020a) mukaan haittaohjelmat ovat jatkuvasti sijoittuneet merkittävimpien kyberuhkien joukkoon. Evansin (2019) mukaan palvelunestohyökkäyksien suuri taloudellinen tappio muodostuu erityisesti prosessitasolla liiketoiminnan keskeytymisenä, jota Yritys pitää merkittävänä. Tietomurtojen uhkaa Yritys ei pidä yhtä suurena. Kyberriskien haasteeksi nähdään se, että riskit koetaan liikaa liiketoiminnasta erillisiksi riskeiksi, vaikka todellisuudessa ne ovat integroitu osa yritysten liiketoimintaa yhä kasvavissa määrin teknologian kehittyessä.

Yritys näkee kyberriskien merkityksen kasvavan tulevaisuudessa jatkuvasti. Automatisaatio, digitalisaatio ja pilvipalvelut toimivat ajureina liiketoiminnan kehittyessä ja laitteiston verkottuessa entisestään. Myös pandemian vaikutuksia työskentelytapojen muutoksiin pidetään kyberriskien merkitystä kasvattavana tekijänä. Teoriaosuudessa on tunnistettu samat merkitystä kasvattavat ajurit kyberriskeille, esimerkiksi ENISA (2020a) nimeää trendeiksi teknologian kehityksen ja Covid-19-pandemian aiheuttamat muutokset. Kyberriskit koetaan Yrityksessä siis merkittäviksi erityisesti niiden liiketoiminnallisten vaikutusten sekä kehittyvän luonteen takia.

Toisen tutkimuskysymyksen tarkoituksena oli keskittyä kyberriskien hallintaprosessin vaiheista tunnistamiseen, arviointiin sekä hallinnan toimenpiteisiin. Kyberriskien tunnistaminen on Yrityksessä jatkuva toimenpide. Riskikartoituksiin käytetään huolellisesti aikaa etenkin uusien järjestelmien ja tietoteknisten ratkaisujen käyttöönoton ja kehittämisen yhteydessä. Kyberriskien tunnistaminen ja riskikartoitukset ovat Yrityksessä pitkälti tietohallinnon vastuulla, mutta liiketoimintojen panosta pyritään kasvattamaan jatkuvasti. Teoriaosuudessa tunnistettuja riskikartoituksia tehdään säännöllisesti vakuutusyhtiön kanssa, mutta kyberriskien osalta erillistä kartoitusta ei ole vielä toteutettu.

Kyberriskien arvioinnissa todennäköisyyksien ja vaikutusten arvioinnissa Yrityksellä on käytössä riskienarviointityökalu. Kyberriskien arvioinnissa käytetään kuitenkin pääsääntöisesti kvalitatiivisia arviointimenetelmiä. Kyberriskejä arvioidaan teorian mukaisesti todennäköisyyksien ja vaikutusten osalta, esimerkiksi Vaughanin (1997) mukaan. Myös riskitulon kaltaista arviointia käytetään. Liiallisella kyberriskien arvioinnilla ei Yrityksessä haluta viedä liikaa resursseja itse hallintatoimenpiteiltä. Erityisesti tietohallinnon sisäisesti pystytään hiljaisen tiedon varassa arvioimaan kyberriskien kokoluokkaa ja vakavuutta. Tietohallinnolla on suuri vastuu myös kyberriskien arvioinnissa, mutta erityisesti kyberriskien taloudellisen merkityksen arvioimiseksi tarvitaan myös liiketoimintojen panosta. Arvioinnissa taloudellisten vaikutusten määrittäminen pystytään tekemään suhteellisen tarkasti liiketoimintojen keskeytymisen osalta, varsinkin kriittisten liiketoimintajärjestelmien, mutta vähemmän kriittisten järjestelmien ja välillisten taloudellisten vaikutusten osalta arviointi on hankalampaa.

Kyberriskien riskienhallintakeinoina Yritys käyttää kyberriskien pienentämistä ja siirtämistä. Pienentäminen on tehokas riskienhallintakeino, kun riskiä ei pystytä poistamaan tai siirtämään kokonaan. Kyberriskien luonteen omaisesti niiden poistaminen on mahdotonta liiketoiminnan ollessa teknologiasta riippuvaista. Kolme keskeistä Yrityksen keinoa kyberriskien hallitsemiseksi ovat tekniset kontrollit, kyberriskien tietoisuuden lisääminen sekä kybervakuutus. Teknisiin kontrolleihin sisältyy tietoturvakontrolleja, verkkojen kahdentamista sekä varajärjestelmien luomista liiketoimintakriittisille järjestelmille. Kontrollien lisäksi Yrityksellä on tarkat linjaukset liiketoimintakriittisten järjestelmien hankinnoista. Teknisten kontrollien avulla pystytään vaikuttamaan järjestelmävirheistä muodostuviin kyberriskeihin, kuten Cebula ym. (2010) jakaa kyberriskit lähteiden mukaan.

Tietoisuuden lisäämisen avulla Yrityksen työntekijöitä pyritään valistamaan kyberriskeistä ja niiden olemassaolosta. Tietoisuutta lisätään koko henkilöstöä koskevien koulutusten avulla. Koulutusten avulla pystytään hallitsemaan ihmisten toimenpiteiden aiheuttamia kyberriskejä. Teoriaan verrattuna ihmisten tahattomien ja toteuttamatta jätettyjen tekojen aiheuttamien kyberriskien todennäköisyyttä saadaan pienennettyä. Yritys pitää hallintakeinoa merkittävänä sen yksinkertaisuudesta huolimatta.

Kolmannen merkittävän keinon eli kybervakuutuksen avulla Yritys suojautuu kyberriskien taloudellisilta vaikutuksilta. Hallintakeinona on kyberriskien aiheuttaman taloudellisen riskin siirtäminen. Kybervakuutuksen avulla taloudellista riskiä ei kuitenkaan saada täysin siirrettyä, sillä taloudelliset menetykset voivat vakuutuskorvauksen jälkeenkin jäädä hyvin merkittäviksi. Tutkielman teoriassa myös Ilmonen ym. (2016) tunnistavat siirtämisen hallintakeinoon liittyvät puutteet, jotka vaativat tueksi myös muita hallintamenetelmiä. Päivittäisten tuotannon volyymien takia keskeytymisen aiheuttama taloudellinen tappio voi koitua hyvin suureksi. Taloudellisten vaikutusten minimoimiseksi kohdeyritys tarvitsee kyberriskejä pienentäviä keinoja siirtämisen tueksi.

Yrityksen kyberriskien hallinta on jatkuvaa arviointia hallintakeinojen riittävyydestä ja siitä, ovatko riskit hyväksyttävällä tasolla. Kyberriskienkään osalta ideaalitilannetta ei ole olemassa ja ikinä ei voida sanoa olevansa kokonaan turvassa. Tärkeimpänä pidetään kyberriskien osalta relevanttien hallintakeinojen löytämistä käytettävissä olevien

resurssien puitteissa. Huomiota kiinnitetään siihen lisäarvoon, mikä saavutetaan suhteessa käytettyihin resursseihin.

Kokonaisuudessaan kohdeyrityksen kyberriskien hallintaprosessi on jatkuva prosessi, jonka avulla pyritään ehkäisemään kyberriskeistä johtuvia epäsuotuisia tapahtumia ja erityisesti suojaamaan liiketoiminnan jatkuvuutta. Hallintaprosessi noudattaa riskienhallintaprosessille tyypillisiä vaiheita, jotka ovat jaoteltavissa tunnistamiseen, arviointiin sekä hallintatoimenpiteisiin. Tavoitteiden asettaminen prosessille lähtee hallituksen riskienhallintapolitiikan tasolta, johon lisätään tarpeellisia lisätavoitteita käytännön tasolla. Kyberriskien hallinta koko prosessi huomioon ottaen on pitkälti Yrityksen tietohallinnon vastuulla, mutta liiketoimintojen roolia pyritään kasvattamaan enenevässä määrin. Viime kädessä vastuu kyberriskeistä koko riskienhallinnan asianmukaisen järjestämisen ohella on Yrityksen johdolla.

Tutkimuksen tulokset vahvistavat kyberriskien tunnistettua kasvavaa merkitystä niin yritysten kuin yhteiskunnan tasolla. Myös kyberriskien vaikutukset ovat merkittäviä. Varsinkin suurten teollisen tuotannon päivittäisten volyymien omaavien yritysten kohdalla liiketoiminnan keskeytymisen aiheuttavien kyberriskien osalta. Tulokset tuovat esille myös liiketoimintojen kasvavan roolin kyberriskien merkityksen kasvaessa. Kyberriskien ollessa yhä tiiviimpi osa päivittäistä yritysten liiketoimintaa, tulee vastuu kyberriskien hallinnasta kuulua koko henkilöstölle. Kohdeyrityksen tunnistama kyberriskien tietoisuuden ja hallintaan osallistumisen vaje tietohallinnon ulkopuolelta voidaan samaistaa yhteiskunnan tasolle. Tietoisuuden lisääminen organisaatioiden sisällä on avaintekijöitä kasvavien kyberriskien hallinnassa.

Tutkimuksen tulosten mukaisten kyberriskien tunnistamisen ja arvioinnin keinot sekä kyberriskien hallintatoimenpiteet ovat linjassa aiempien tutkimusten kanssa. Lisäksi kyberriskien hallintaprosessi noudattaa tutkimuksessa tyypillisiä riskienhallintaprosessin mukaisia vaiheita. Tutkimuksen tulokset voidaan siis nähdä vahvistavan tyypillisen riskienhallintaprosessin ja sen vaiheiden käytettävyyttä myös yritysten kyberriskien hallinnassa, tietyt riskien luonteen mukaiset ominaispiirteet huomioon ottaen. Tutkimuksen tulosten merkitystä voidaan pitää aiempia tutkimuksia vahvistavana sekä organisaation kyberriskien tietoisuuden lisäämistä korostavana. Lisäksi tutkimus

kartoittaa kuvan suomalaisen pörssiin listatun yrityksen kyberriskien hallintaprosessista ja hallinnan tasosta.

5.2 Tutkimuksen arviointi ja jatkotutkimusehdotukset

Tutkimuksen tavoitteisiin päästiin ja tutkimuskysymyksiin saatiin kattavat vastaukset, joten tutkimusta voidaan pitää onnistuneena. Tutkimuksen luotettavuutta voidaan arvioida reliabiliteetin ja validiteetin avulla. Tutkimuksen reliaabelius tarkoittaa mittaustulosten toistettavuutta ja validius tarkoittaa mittarin tai tutkimusmenetelmän kykyä mitata juuri sitä, mitä on tarkoituskin mitata. (Hirsjärvi ym. 2007, 226.) Tutkimuksen empiirisen osuuden laatuun on pyritty vaikuttamaan mahdollisimman tarkalla selostuksella tutkimuksen toteuttamisesta. Aineiston hankintaan liittyvät yksityiskohdat haastattelusta on selitetty tutkielmassa tarkasti ja aineiston litterointi on suoritettu nopeasti haastattelun jälkeen. Tutkimuksessa on haastateltu vain kahta kohdeyrityksen henkilöä, mutta tämä on otettu huomioon haastateltavien huolellisella valinnalla heidän toimenkuvansa ja osaamisensa perusteella.

Tutkimuksen validiteettia parantaa lisäksi aineiston osalta myös se, että haastattelukysymykset on toimitettu haastateltaville etukäteen ja haastattelu on toteutettu teemahaastatteluna, joka on ehkäissyt mahdollisia kysymystenasettelun väärinymmärryksiä ja mahdollistanut täydentävät kysymykset. Aineiston määrän riittävyyteen varauduttiin laatimalla laajahkot haastattelukysymykset, joiden avulla riittävä aineiston määrä oli mahdollista saada yhdellä haastattelulla. Myös toinen haastattelukierros olisi ollut mahdollista toteuttaa, jos aineistoa analysoitaessa tämä olisi katsottu tarpeelliseksi.

Tutkimuksen teoreettisen osuuden laatuun pyrittiin vaikuttamaan valitsemalla laadukasta aiheeseen sopivaa aineistoa. Tutkimuksen tulkintateoriaan liittyvää aineistoa oli hyvin monipuolisesti tarjolla niin englannin- kuin suomenkielisenä, jota pyrittiin tuomaan mahdollisimman kattavasti ja monipuolisesti esille. Tutkimuksen taustateoria koostuu englanninkielisistä lähteistä, johon on akateemisen kirjallisuuden tueksi käytetty myös muutamia kaupallisia sekä kansallisten ja kansainvälisten virastojen lähteitä.

Tutkimuksen yleistettävyyttä heikentää se, että tutkimuksessa on tarkastelun kohteena ollut yksi yritys. Tutkimuksen case-yritystä voidaan kuitenkin pitää toimialastaan riippumatta hyvin keskisuuria suomalaisia pörssiyrityksiä kuvaavana tutkimuskohteena. Vaikka yritys toimii elintarvikealalla, tutkimuksessa ei olla tutkittu alkutuotannon riskejä. Tästä syystä yritystä voidaan pitää hyvin suomalaisia teollisen tuotannon pörssiyhtiöitä yleistävänä. Yritys käyttää pörssiyritykselle tyypillisesti riskienhallinnassaan yleisellä tasolla soveltuvin osin riskienhallinnan standardeja ja huomioi corporate governancen vaikutukset. Tutkimuksen kohdeyrityksellä ei kuitenkaan ole erillistä riskienhallinnan viitekehystä kyberriskien hallintaprosessille. Tämä ja kyberriskien kasvava sekä hallintaa muokkaava rooli yritysten riskienhallinnassa huomioiden heikentävät kuitenkin suoraa yleistettävyyttä vastaaviin yrityksiin. Huomioitavaa on myös se, että tutkimuksen kohdeyrityksen liiketoiminta ei perustu juuri lainkaan asiakkaiden tai kolmansien osapuolien kriittisten tietojen hallussa pitämiseen. Tästä syystä dataan ja tietosuojaan liittyvät kyberriskit ovat voineet jäädä pienemmälle huomiolle.

Tutkimuksen kohdeyrityksen nimi ja haastateltavien nimet on salattu, mikä voidaan nähdä ongelmallisena tutkimuksen asetelman kannalta. Kohdeyrityksen ohjeistuksen puitteissa tutkimukseen on kuitenkin pyritty tuomaan asetelman ja validiteetin kannalta keskeiset kohdeyrityksen tiedot sekä kuvaukset. Lopulta tutkimuksen kannalta merkittävistä tiedoista ei ole jouduttu luopumaan ja tutkimuksen salauksen asteeksi on jäänyt vain nimien sensurointi. Tutkimuksen empiirisen aineiston tiedot on haastateltavien toimesta kerrottu yleisellä tasolla, jotka eivät kohdeyrityksen tunnistettavaksi tullessa ole kriittisiä.

Jatkotutkimusehdotuksina kyberriskejä voidaan tutkia vielä lukuisista eri näkökulmista. Kyberriskit kehittyvät jatkuvasti, joten niiden jatkuva tutkiminen on perusteltua. Kyberriskien hallintaprosessin kannalta tutkimusta voisi olla mielekästä tutkia jonkun tietyn toimialan näkökulmasta tarkastelemalla useampien yritysten hallintaprosessia. Lisäksi viime aikoina suurta huomiota saaneiden tietomurtojen näkökulmasta tehty kyberriskien tutkimus voisi olla mielenkiintoista. Tutkittavan case-yrityksen asiantuntijat nostivat mahdollisina jatkotutkimusehdotuksina esille kybervakuutukseen liittyvän tutkimuksen ja kyberriskien jatkuvuussuunnitelmat, joiden tarpeellisuus on huomioitu myös case-yrityksessä. Tutkimusmenetelminä kvantitatiivinen tai monimenetelmäinen tutkimus voisivat tuottaa mielenkiintoista tutkimusta numeerisen tiedon käsittelyn ja

analysoinnin avulla. Esimerkiksi kyberriskien hallintakeinoja voisi tutkia kustannusten ja hyötyjen osalta, kyberriskien hallintaprosessin tutkimisessa tutkittavien yritysten määrää voisi laajentaa kyselylomakkeen avulla tai kybervakuuttamisen kehittyvää tuotetta voisi olla mielekästä tutkia numeerisesti.

LÄHDELUETTELO

Kirjallisuus:

Cebula, J. & Young, L. 2010. A Taxonomy of Operational Cyber Security Risks. Carnegie Mellon University.

Choo, K. 2011. The cyber threat landscape: Challenges and future research directions. *Computers & Security* 30(8), 719-731.

Evans, A. 2019. Managing Cyber Risk. 1. painos. Milton: Routledge.

Fraser, J. & Simkins, B. 2010. Enterprise risk management. 1. painos. New Jersey: Wiley.

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

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2007. Tutki ja kirjoita. 13. painos. Helsinki: Tammi.

Hopkin, P. 2018. Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management. 5. painos. Lontoo: Kogan Page.

Ilmonen, I., Kallio, J., Koskinen, J. & Rajamäki, M. 2016. Johda riskejä. Helsinki: Finva.

Juvonen, M., Koskensyrjä, M., Kuhanen, L., Ojala, V., Pentti, A., Porvari, P. & Talala, T. 2014. Yrityksen riskienhallinta. Helsinki: Finva.

Knüpfer, S. & Puttonen, V. 2018. Moderni Rahoitus. 10. Painos. Helsinki: Alma Talent.

Koskinen, I., Alasuutari, P. & Peltonen, T. 2005. Laadulliset menetelmät kauppatieteissä. Tampere: Vastapaino.

Koskinen, L., Ahteensivu, A., Havakka, P. & Kulmala J. 2018. Riskienhallinnan ajankohtaisia teemoja. Tampere: Tampere University Press.

Lam, J. 2014. Enterprise risk management: from incentives to controls. 2. Painos. New Jersey: John Wiley & Sons.

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A. & Sadhuktan, S. 2013. Cyber-risk decision models: To insure IT or not? *Decision Support Systems* 56(1), 11–26.

Refsdal, A., Solhaug, B. & Stølen, K. 2015. Cyber-Risk Management. Cham: Springer International Publishing AG.

Ruan, K. 2019. Digital asset Valuation and Cyber Risk Measurement. 1. painos. Lontoo: Academic Press.

Sweeting, P. 2011. Financial enterprise risk management. Cambridge: CUP.

Tuomi, J. & Sarajärvi, A. 2018. Laadullinen tutkimus ja sisällönanalyysi. Uudistettu painos. Helsinki: Tammi.

Vaughan, E. 1997. Risk Management. New York: Wiley.

Internet-lähteet:

Allianz. 2020. Allianz Risk Barometer. (viitattu 15.01.2021) Saatavilla: Allianz-Risk-Barometer-2020.pdf

ENISA. 2020a. ENISA Threat Landscape 2020 – The year in review. (viitattu 13.01.2021) Saatavilla: ENISA Threat Landscape - The year in review — ENISA (europa.eu)

ENISA. 2020b. ENISA Threat Landscape 2020 – Malware. (viitattu 13.01.2021) Saatavilla: ENISA Threat Landscape 2020 - Malware — ENISA (europa.eu)

Institute of Risk Management. 2014. Cyber Risk: Resources for Practitioners. (viitattu 11.01.2021) Saatavilla: irm-cyber-risk-resources-for-practitioners.pdf (theirm.org)

ISO. 2018. ISO 31000:2018. (viitattu 01.12.2020) Saatavilla: ISO 31000:2018(en), Risk management — Guidelines

Turvallisuuskomitea. 2018. Kyberturvallisuuden sanasto. (viitattu 12.01.2021) Saatavilla: Kyberturvallisuuden-sanasto.pdf (turvallisuuskomitea.fi)

Turvallisuuskomitea. 2019. Suomen Kyberturvallisuus Strategia 2019. (viitattu 15.01.2021) Saatavilla: Kyberturvallisuusstrategia_A4_SUOMI_WEB_300919.pdf (turvallisuuskomitea.fi)

Henkilölähteet:

Asiantuntija A. Yritys Oyj. Group Controller. Haastattelu 03.12.2020.

Asiantuntija B. Yritys Oyj. ICT Technical Manager. Haastattelu 03.12.2020.

LIITTEET

Liite 1: Haastattelurunko

Haastattelu 03.12.2020.

1. Mitkä ovat kohdeyrityksen riskienhallinnan tavoitteet ja kuka tavoitteet asettaa?
2. Miten riskienhallinnan vastuualueet jakautuvat? Miten vastuut jalkautetaan konsernitasolta liiketoiminta-alueille?
3. Käyttääkö kohdeyritys riskienhallinnassaan apuna viitekehyksiä/standardeja?
4. Millä tavoin kohdeyritys pyrkii tunnistamaan kyberriskejä?
5. Millaisia kyberriskejä kohdeyritys näkee liiketoiminnassaan?
6. Millaisia arviointikeinoja kyberriskeille on / miten kohdeyritys arvioi kyberriskien todennäköisyyttä ja vakavuutta? (Riskien kvalitatiivinen tai kvantitatiivinen arviointi? Työkaluja vaikutusten arviointiin?)
7. Millaisia vaikutuksia kyberriskeillä arvioidaan olevan kohdeyrityksen liiketoimintaan?
8. Kuinka vakavana riskinä kohdeyritys pitää kyberriskejä liiketoiminnan kannalta?
9. Kuinka merkittäviä kyberriskit ovat muihin riskeihin nähden?
10. Millaisin keinoin kohdeyritys pyrkii hallitsemaan kyberriskejä?
11. Millaisia vahvuuksia ja heikkouksia nykyisiin kyberriskien hallintakeinoihin liittyy? Ovatko nykyiset hallintakeinot riittäviä?
12. Miten vastuu kyberriskeistä on jakautunut kohdeyrityksessä?
13. Miten kyberriskien hallintaprosessia seurataan ja arvioidaan?
14. Mikä on kohdeyrityksen näkemys kyberriskien merkityksestä tulevaisuudessa?

Muuta tutkimuksen kannalta oleellista, joka ei haastattelun aikana tullut ilmi kyberriskeistä tai yrityksen riskienhallinnasta?