TURUN YLIOPISTO
Kauppakorkeakoulu

# Kyberturvallisuus osana suomalaisten yritysten vuosiraportointia

Analyysi kyberturvallisuustietojen esittämisestä suomalaisten pörssiyhtiöiden toimintakertomuksissa ja vuosiraporteissa

Tietojärjestelmätieteen
pro gradu -tutkielma

Laatija:
Laura Haavisto

Ohjaaja:
Prof. Reima Suomi

10.7.2024
Turku

Pro gradu -tutkielma

**Oppiaine**: Tietojärjestelmätiede
**Tekijä**: Laura Haavisto
**Otsikko**: Kyberturvallisuus osana suomalaisten yritysten vuosiraportointia – Analyysi kyberturvallisuustietojen esittämisestä suomalaisten pörssiyhtiöiden toimintakertomuksissa ja vuosiraporteissa
**Ohjaaja**: Prof. Reima Suomi
**Sivumäärä**: 65 sivua + liitteet 2 sivua
**Päivämäärä**: 10.7.2024

Kyberturvallisuuden merkitys nykymaailmassa on jatkuvassa kasvussa kyberuhkien määrän lisääntyessä jatkuvasti. Esimerkiksi Yhdysvalloissa tietovuodot ovat yli 20-kertaistuneet vuosien 2005 ja 2023 välillä. Tämä kasvattaa sidosryhmien, sijoittajien ja asiakkaiden odotuksia yritysten kyberturvallisuustoimia kohtaan, ja yritysten on tärkeää viestiä ja raportoida kyberturvallisuustoimistaan julkisesti. Yksi keskeinen keino yrityksille tällaiseen viestintään on sisällyttää tietoja kyberturvallisuudesta osaksi vuosiraportointia.

Tämän tutkielman tarkoituksena oli tarkastella suomalaisten pörssiyritysten kyberturvallisuusraportointia osana vuosien 2022 ja 2023 vuosiraportteja, ja muodostaa tätä kautta poikkileikkaava kuva kyberturvallisuusraportoinnin nykytasosta Suomessa. Aihetta on tutkittu jonkin verran maailmalla, mutta Suomessa ja Euroopassa tutkimus on edelleen vähäistä.

Empiirinen tutkimus toteutettiin laadullisena tutkimuksena, ja tutkimusmenetelmäksi valikoitui sisällönanalyysi. Tutkielman aineisto koottiin Helsingin pörssiin listautuneiden yritysten uusimmista vuosiraporteista, jotka aineiston keruuhetkellä olivat joko vuoden 2022 tai 2023 raportteja. Aineisto käytiin läpi kyberturvallisuuteen liittyvien hakusanojen avulla, ja hakusanojen osumat jaoteltiin niiden kontekstin perusteella teemoihin ja edelleen alateemoihin, jotka muodostettiin tutkimuksessa sovellettua teoreettista viitekehystä mukaillen.

Tutkimuksen tulokset ovat pitkälti linjassa teorian ja aiemman tutkimuksen kanssa. Löydökset osoittavat, että kyberturvallisuusraportointi on Suomessa samalla tasolla kuin muualla maailmassa, ja suurin osa suomalaisista pörssiyrityksistä sisällyttää tietoja kyberturvallisuudesta osaksi vuosiraportointiaan, vaikkakin toimiala- ja kokoluokkakohtaisia eroja esiintyy. Raportointi on sisällöltään melko yksinkertaista ja suppeaa. Tulevaisuudessa voi olla syytä keskittyä enemmän erityisesti raportoinnin selkeyteen, ymmärrettävyyteen ja johdonmukaisuuteen.

Tutkimustulokset tarjoavat yritysjohdolle tietoa kyberturvallisuusraportoinnin tilasta ja käytännöistä nykymarkkinoilla, minkä perusteella raportointia on mahdollista edelleen kehittää. Koska aiheen tutkimus on vielä vähäistä, tarve jatkotutkimukselle on tunnistettu, ja sitä on mahdollista toteuttaa useista eri näkökulmista.

**Avainsanat:** kyberturvallisuus, tietoturva, tietosuoja, vuosikertomus, vuosiraportointi

# SISÄLLYS

# TAULUKOT

# 1 Johdanto

## 1.1 Tutkimuksen taustaa

Kyberturvallisuuden merkitys kasvaa jatkuvasti kyberuhkien lisääntyessä ja vaikuttaessa yritysten toimintaan ympäri maailman. Esimerkiksi Maailman talousfoorumi (2024) ja Forbes (2023) listaavat kyberhyökkäykset merkittävimpien yritysten kohtaamien riskien joukkoon vuonna 2024. Myös toteutuneiden uhkien määrä kasvaa, ja esimerkiksi Yhdysvalloissa tietovuotojen määrä on yli 20-kertaistunut vuosien 2005 ja 2023 välillä. Suurin hyppy on koettu juuri 2020-luvulla, jolloin määrä on kasvanut noin 1 100 tietovuodosta noin 3 200 tietovuotoon per vuosi. (Statista 2024a.) Myös tietovuotojen aiheuttamat kustannukset ovat kasvussa, ja vuonna 2023 yksittäisen tietovuodon aiheuttamat kustannukset olivat Yhdysvalloissa noin 9,48 miljoonaa dollaria (Statista 2024b). Tämä siis tarkoittaa, että pelkästään Yhdysvalloissa tietovuodoista aiheutuneet kustannukset olivat yhteensä noin 30,3 miljardia dollaria vuonna 2023. Merkittävät tietovuodot myös laskevat yritysten maineeseen liittyvää, aineetonta pääomaa keskimäärin noin 5–9 % (Makridis 2021).

Hyvä kyberturvallisuus voi siis olla yritykselle elinehto, ja yritykseen kohdistuneista kyberhyökkäyksistä aiheutuu yrityksille niin taloudellista kuin mainehaittaa. Esimerkiksi Suomessa laajasti uutisoidun Psykoterapiakeskus Vastaamon tietomurrosta vuonna 2020 koitui yritykselle paitsi merkittäviä taloudellisia vahinkoja, myös erittäin laajaa mainehaittaa. Arkaluontoisten potilastietojen vuotaminen ja esille nousseet heikot tietoturvakäytännöt heikensivät asiakkaiden ja sidosryhmien luottamusta yritykseen merkittävästi, ja Vastaamo asetettiin konkurssiin vuonna 2021. (Helsingin Sanomat 2020, Yle Uutiset 2021.)

Uhkien ja hyökkäysten yleistyessä myös asiakkaiden, sijoittajien, päättäjien ja muiden sidosryhmien odotukset niin yritysten kyberturvallisuustoimia kuin niiden läpinäkyvyyttä kohtaan kasvavat. Kyberturvallisuus ei nykypäivänä siis enää tarkoitakaan pelkästään tietojen suojelua, vaan myös jatkuvaa yrityksen riskienhallintaa sekä taloudellisen tilanteen ja markkina-aseman kehittämistä. Näin ollen yrityksille voi olla merkittävä strateginen valinta tiedottaa ja raportoida kyberturvallisuustoimistaan sidosryhmilleen.

Vuosikertomus on yrityksille yksi keskeisimmistä keinoista viestiä sidosryhmille organisaation avaintapahtumista tilikauden aikana, mutta myös rakentaa mielikuvia yrityksen

nykytilasta ja sen tulevaisuudesta (Juholin 2022). Yrityksen vuosiraportoinnin sisältö koostuu vähintään arvopaperimarkkinalain vaatimuksen mukaan tilinpäätöksestä ja toimintakertomuksesta liitetietoineen. (Arvopaperimarkkinalaki 7:5–9.) Koska vuosiraportointi on niin merkittävä osa organisaatioviestintää, lakisääteisten osien lisäksi yrityksillä on tapana lisätä sinne tietoja yrityksen toiminnasta ja tuloksesta myös vapaaehtoisesti. Tiedot yrityksen kyberturvallisuudesta ovat osa tätä niin kutsuttua vapaaehtoista raportointia, ja raportoimalla avoimesti kyberturvallisuustoimistaan yritysten on mahdollista esimerkiksi kasvattaa sijoittajien kiinnostusta yritystä kohtaan (Eijkelenboom & Nieuwsteeg 2021.)

Kyberturvallisuusraportointi onkin lisääntynyt viime vuosien aikana. Vuosien 2010 ja 2018 välillä raportointi kasvoi peräti 75 %-yksikköä (Gordon ym. 2010, Berkman ym. 2018). Nykyään kyberturvallisuusasioista raportointi on maailmalla melko yleistä, ja esimerkiksi Pohjois-Amerikassa noin 87 % yrityksistä sisällyttää tietoja kyberturvallisuudesta vuosiraportointiinsa. (Héroux & Fortin 2020).

Kyberturvallisuusraportoinnin tasosta Suomessa ei kuitenkaan ole tehty toistaiseksi tutkimusta, ja tutkimus Euroopassa on myös hyvin vähäistä. Tämän tutkielman tarkoituksena on vastata tähän tutkimusaukkoon, ja tarjota kuva kyberturvallisuusraportoinnin tilasta ja käytännöistä Suomessa. Tutkimus on myös tärkeää yritysjohdolle, sillä hahmottamalla tarkemmin kyberturvallisuusraportoinnin nykytilaa ja toisaalta myös sen puutteita, raportointia ja kyberturvallisuutta voidaan jatkossa kehittää tehokkaammin.

## 1.2 Keskeiset käsitteet

Termejä *tietoturva* ja *kyberturvallisuus* käytetään melko usein sekaisin, eikä sanojen merkitys puhekielessä välttämättä eroa juurikaan toisistaan (von Solms & van Niekerk 2013). Tämän tutkielman kannalta on kuitenkin merkityksellistä erottaa nämä käsitteet toisistaan.

**Tietoturva** (engl. *information security*) on kirjallisuudessa määritelty useasta eri näkökulmasta, ja termi itsessään on melko lavea. Yleisesti sillä kuitenkin tarkoitetaan tietojen suojaamista luvattomalta käytöltä, tai toimia, joita tietojen suojaamiseksi tehdään (Oxford English Dictionary 2023d). Tietoturvallisuudella tarkoitetaan myös sellaisia toimia, joilla voidaan varmistaa tiedon saatavuus, eheys ja luottamuksellisuus. Näitä toimia voivat

esimerkiksi olla kulunvalvonta tai asiakirjojen turvallinen säilytys, hävitys ja varmuuskopiointi. (Turvallisuuskomitea 2018.)

Myös **kyberturvallisuus** (engl. *cybersecurity*) on terminä erittäin laaja, mutta useimmiten se taas viittaa turvallisuustoimiin, jotka liittyvät tietojärjestelmiin tai internettiin, ja joiden avulla on tarkoitus ehkäistä erityisesti viruksia tai petoksia (Oxford English Dictionary 2023b). Kyberturvallisuuteen siis liittyy oletus kybertoimintaympäristöstä, eli toimintaympäristöstä, joka koostuu yhdestä tai useammasta tietojärjestelmästä. Kyberturvallisuus voi myös olla ”tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan” (Turvallisuuskomitea 2018.)

Merkittävin ero näiden termien välillä siis on, että tietoturva tarkoittaa kaikenlaista tiedon suojelua mahdollisilta heikkouksilta ja uhilta. Sen sijaan kyberturvallisuuteen liittyy aina myös oletus kyberympäristöstä. Yksinkertaistettuna tietoturva siis tarkoittaa kaikenlaista tiedon suojelua, kyberturvallisuus taas sähköisessä muodossa olevan tiedon suojelua. (von Solms & van Niekerk 2013.)

Tietoturvasta ja kyberturvallisuudesta puhuttaessa esiin nousee usein myös **tietosuoja** (engl. *information privacy, data privacy, data protection*). Tällä viitataan tietojen suojaamiseen väärinkäytöksiltä ja tuhoutumiselta erityisesti niiden tietojen osalta, joita säilytetään sähköisessä muodossa (Oxford English Dictionary 2023c). Tietosuoja-sanalla on aikaisemmin viitattu kaikenlaiseen tietoon, mutta nykyään se on rajattu käsittämään juuri henkilötietojen asianmukaista käsittelyä ja yksityisyyden säilyttämistä. Tämän vuoksi tietosuojasta käytetään myös usein termiä *henkilötietosuoja*. (Turvallisuuskomitea 2018.)

Koska tässä tutkielmassa kyberturvallisuutta käsitellään yritysten vuosiraportoinnin kautta, on myös syytä määritellä keskeisimmät termit liittyen yritysten raportointiin.

Suomessa kirjanpitolaki velvoittaa yrityksiä laatimaan vuosittain tilinpäätöksen ja toimintakertomuksen. Siinä missä tilinpäätös sisältää yrityksen taloudellisia tietoja havainnoivat dokumentit, **toimintakertomus** sisältää sen sijaan sanallisen kuvauksen organisaation toiminnan kehittymisestä ja tuloksellisuudesta, taloudellisesta tilanteesta sekä merkittävimmistä riskeistä ja epävarmuustekijöistä. (KPL 3:1, KPL 3:1a.)

Yrityksen **vuosiraportti** taas on käsitteenä laajempi, eikä sille ole laissa määritelmiä. Vuosiraportilla kuitenkin tarkoitetaan useimmiten organisaation vuosittain julkaisemaa dokumenttia tai eri dokumenttien muodostamaa kokonaisuutta, joka käsittelee muun

muassa yrityksen edellisen tilikauden toimintaa ja tapahtumia. Vuosiraportti on julkinen, ja on suunnattu yleensä erityisesti yrityksen sidosryhmille. (Oxford English Dictionary 2023a.)

## 1.3 Tutkimusongelma

Tämän tutkielman tavoitteena on tarkastella suomalaisten pörssiyritysten tapoja raportoida kyberturvallisuuskäytännöistään vuosikertomuksissa. Tarkoituksena on muodostaa poikkileikkaava kuva kyberturvallisuusraportoinnin nykytasosta ja sisällöistä Suomessa.

Tutkimuksessa pyritään vastaamaan seuraavaan tutkimuskysymykseen:

- Millä tasolla suomalaisten pörssiyritysten kyberturvallisuusraportointi osana vuosiraportointia on?

Tutkimusongelmaa lähestytään lisäksi seuraavien alakysymysten kautta:

- Minkälaisia tietoja vuosikertomukset sisältävät kyberturvallisuuteen liittyen?
- Onko raportointikäytäntöjen välillä eroja yritysten toimialan tai kokoluokan perusteella?

Tutkimuksessa tarkastellaan kyberturvallisuutta ja tietoturvallisuutta, mutta tietosuoja on rajattu tutkimuksen ulkopuolelle. Tietosuoja on perusoikeus, joka turvaa henkilötietojen käsittelyn lain määräämällä tavalla. Näin ollen tietosuoja kattaa myös paljon enemmän osa-alueita kuin esimerkiksi tietoturvallisuuden, joka on vain yksi tietosuojan toteuttamisen keino. (Tietosuojavaltuutetun toimisto, 2022.)

Tutkimuksen kohteina ovat suomalaiset pörssiyhtiöt laajasti eri toimialoilta, mutta kyberturvallisuusalan yritykset on rajattu pois tutkimuksesta. Tämä johtuu siitä, että tutkimuksessa kyberturvallisuusraportointia tarkastellaan muun muassa aihepiiriin liittyvien hakusanojen lukumäärien kautta. Kyberturvallisuusalan yritysten voidaan kuitenkin olettaa käyttävän näitä sanoja raporteissaan paljon myös muissa asiayhteyksissä, eikä niiden tarkastelu näin ollen ole tarkoituksenmukaista.

## 1.4 Tutkielman rakenne

Tämä tutkielma muodostuu johdannosta, kolmesta sisältöluvusta sekä johtopäätöksistä ja yhteenvedosta. Johdannossa esitellään tutkimuksen taustaa, tutkimusongelma sekä

tutkimuksen kannalta keskeiset käsitteet. Tutkielman ensimmäisessä sisältöluvussa tarkastellaan kyberturvallisuusraportoinnin teoreettista taustaa. Ensin käsitellään keskeisimmät yritysten vuosiraportointiin liittyvät asiat sekä lainsäädännölliset seikat kyberturvallisuuteen ja raportointiin liittyen. Tämän jälkeen esitellään tarkemmin kyberturvallisuusraportoinnin motiiveja, nykykäytäntöjä ja trendejä.

Tutkielman toinen sisältöluku keskittyy tutkimuksen metodologiaan, ja sisältää tutkimusmetodien, aineiston, tutkimuksen teoreettisen viitekehyksen sekä aineiston analyysimenetelmien esittelyn. Kolmannessa sisältöluvussa esitellään tutkimustulokset viitekehyksen perusteella muodostetun seitsemän teeman kautta.

Johtopäätökset-luvussa esitellään tutkimustulosten perusteella tehtyjä keskeisimpiä löydöksiä kyberturvallisuusraportoinnin nykytasosta. Tutkielman viimeinen luku sisältää vielä tutkimustulosten yhteenvedon, arvioinnin tutkimuksen luottavuudesta ja merkittävyydestä, sekä ehdotuksia jatkotutkimukselle.

# 2 Kyberturvallisuusraportointi kirjallisuudessa

## 2.1 Yritysten vuosiraportointi

Yritysten vuosiraportoinnin ensisijainen tehtävä on täyttää lakisääteiset vaatimukset ja julkaista sääntelyn mukaiset tiedot yrityksen toiminnasta ja taloudesta (Hynes 2009). Suomessa kirjanpitolaki velvoittaa kaikkia julkisia osakeyhtiöitä, suuryrityksiä ja muita yleisen edun kannalta merkittäviä yhteisöjä julkaisemaan tilinpäätöksen yhteydessä toimintakertomuksen. Toimintakertomukseen tulee sisällyttää keskeiset tiedot yrityksen toiminnasta ja tuloksista, taloudellisesta tilanteesta, merkittävimmistä riskeistä ja epävarmuustekijöistä sekä tarpeen vaatiessa taloudelliset tunnusluvut sekä henkilöstön ja ympäristövaikutusten tunnusluvut. Suuryritysten ja pörssilistattujen pienten ja keskisuurten yritysten on lisäksi liitettävä toimintakertomukseensa tiedot keskeisistä aineettomista voimavaroista, sekä kestävyysraportti. (KPL 3a:1.) Yritykset julkaisevatkin nämä tiedot useimmiten juuri osana vuosiraportointiaan (Leppiniemi ym. 2013).

Tilinpäätöksen, toimintakertomuksen ja muun lakisääteiden dokumentaation lisäksi yritykset voivat vuosiraportissaan vapaavalintaisesti julkaista haluamiaan muita tietoja. Vuosiraportointi onkin myös keskeinen osa yrityksen sidosryhmäviestintää, ja sillä on erityisen korostunut merkitys erityisesti sijoittajaviestinnässä ja taloudellisena tiedonantovälineenä. Vuosiraporteilla on perinteisesti pidetty olevan merkittävä osuus investointipäätöksiin, sillä ne tarjoavat kattavan kuvan yrityksen taloudellisesta suoriutumisesta kuluneen tilikauden aikana. (Leppiniemi ym. 2013, Hynes 2009.) Erinomaisen korkealaatuisilla vuosiraporteilla ei kuitenkaan ole osoitettu olevan merkitystä yrityksen markkina-arvoon, keskeisempää on viestinnän laadun sijaan sen sisältö. Yritysten osakkeita vaihdetaan keskimäärin yhtä paljon huolimatta siitä, ovatko yritysten vuosiraportit saaneet palkintoja tai muita tunnustuksia. (Chircop ym. 2022.)

Tämän lisäksi vuosiraportteja voidaan pitää tärkeänä markkinointikanavana, jolla yrityksen on mahdollista hallita julkisuuskuvaansa ja parantaa sidosryhmien luottamusta. Vuosikertomusten avulla yritysten on mahdollista esitellä arvojansa, strategiaansa ja saavutuksiaan, sekä korostaa tulevaisuuden suunnitelmiaan ja vahvuuksiansa. Ne toimivat näin keskeisenä työkaluna julkisuuskuvan rakentamisessa ja ylläpitämisessä. Hyvin laadittu vuosikertomus voi parantaa yrityksen mainetta ja vahvistaa sijoittajien luottamusta yrityksen johtoon ja taloudelliseen asemaan. (Hynes 2009.) Useat yritykset näkevät

korkealaatuisen vuosiraportoinnin tärkeänä osana yrityksen kokonaisviestintää ja pitkän tähtäimen viestintästrategiaa. Useat yritykset keskittyvätkin vuosiraporteissaan enemmän ylläpitämään yrityksen mainetta rehellisenä ja luotettavana toimijana markkinoilla pitkällä tähtäimellä sen sijaan, että juuri kuluneen tilikauden toiminta ja tulos haluttaisiin näyttää mahdollisimman positiivisessa valossa (Yuthas ym. 2002). Korkealaatuinen vuosiraportti yleensä indikoi myös korkealaatuisemmasta kokonaisviestinnästä. (Chircop ym. 2022.) Myös viestinnän sävyllä on merkitystä, ja yritysten keskimääräinen raportoinnin sävy voi vaihdella sen tavoitteiden tai tulosten mukaisesti. Organisaatioiden raportit ovat keskimäärin vaikeammin luettavia, jos ne kertovat yrityksen huonosta tuloksesta. Mitä tärkeämpää yrityksen on vältellä huonoa mainetta, sitä vaikeammin luettavia sen raportit huonojen uutisten kohdalla yleensä ovat. (Asay ym. 2018.)

## 2.2 Lainsäädäntö kyberturvallisuudesta

NIS on EU:n direktiivi, joka asettaa minimivaatimukset kyberturvallisuudelle EU:n alueella toimiville yrityksille, ja pyrkii nostamaan kyberturvallisuuden tasoa Euroopassa. Direktiivi asettaa lainsäädännöllisiä vaatimuksia muun muassa jäsenvaltioiden kyberturvallisuuden valmiustasolle, kansainväliselle yhteistyölle sekä turvallisuuskulttuurin edistämiselle huoltovarmuuden kannalta merkittävillä sektoreilla, kuten energiateollisuudessa, vedenjakelussa, rahoitusmarkkinoilla tai terveydenhuollossa. (Euroopan komissio 2023.) Direktiivi asettaa tiettyjä vaatimuksia myös kyberturvallisuuspoikkeamista ilmoittamiselle. Yritysten tulee raportoida vakavista kyberturvallisuuspoikkeamista paikallisille viranomaisille. Poikkeamien vakavuuden mukaan viranomaiset voivat raportoida tai velvoittaa yritystä myös kertomaan julkiselle yleisölle poikkeamista. (EU 2022/2555:23.)

Toinen merkittävä EU-asetus GDPR taas asettaa perusvaatimukset sille, miten yksityishenkilöt, yritykset ja organisaatiot saavat käsitellä ja säilyttää henkilötietoja. Asetusluotiin suojaamaan erityisesti digitaalisessa muodossa olevia henkilötietoja. (Euroopan komissio 2024.) Myös GDPR asettaa vaatimukset tietoturvaloukkauksesta ilmoittamiselle. Henkilötietojen rekisterinpitäjän tulee ilmoittaa tietoturvaloukkauksesta valvontaviranomaiselle. Myös tietoturvaloukkausta koskevalle rekisteröidylle on ilmoitettava, mikäli on todennäköistä, että se aiheuttaa korkean riskin henkilön oikeuksille ja vapauksille. (EU 2016/679:33–34.)

Lisäksi Suomen laki määrittää vielä erikseen joitakin kyberturvallisuuteen liittyviä vaatimuksia terveydenhuollon, televiestinnän ja sähköverkkojen toimialoille.

Terveydenhuollon ja televiestinnän osalta nämä vaatimukset liittyvät ilmoitusvelvollisuuteen kyberturvallisuuden häiriötilanteissa. Sähköverkkojen osalta taas yleisesti todetaan, että riittävästä kyberturvallisuuden tasosta on huolehdittava. (Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä 9:66, Laki sähköisen viestinnän palveluista 33:275, Sähkömarkkinalaki 4:22.)

Lainsäädäntö siis määrittelee raamit riittäville kyberturvallisuustoimille sekä kyberturvallisuuspoikkeamista ilmoittamiselle. Kuitenkaan niin EU-tason kuin Suomenkaan lainsäädäntö ei aseta kyberturvallisuusraportoinnille vaatimuksia vuosiraportointia ajatellen. Viranomaiset eivät myöskään Euroopassa tai Suomessa ole luoneet strukturoitua ohjeistusta yritysten kyberturvallisuusraportoinnille.

## 2.3 Kyberturvallisuusraportoinnin motiivit

### 2.3.1 Raportoinnin hyödyt

Vaikka laki ei kaikkialla aseta vaatimuksia kyberturvallisuusraportoinnille, yritykset kuitenkin harjoittavat myös vapaaehtoista kyberturvallisuusraportointia, ja kertovat vuosiraportointikokonaisuuksissaan enemmän tietoja liittyen kyberturvallisuuteen, kuin olisi pakko. Vapaaehtoinen kyberturvallisuusraportointi on siis aina yrityksen strateginen valinta, ja yksikään yritys tuskin tekisi sitä, ellei sillä voitaisi ajatella olevan positiivista vaikutusta yrityksen liiketoimintaan. (Gordon ym. 2010.)

Kyberturvallisuusraportoinnin avulla yritysten on mahdollisuus viestiä muun muassa prioriteeteistaan. Vuosikertomukseen liitetyillä asioilla voidaan viestiä siitä, mikä yritykselle on tärkeää tai mihin milläkin hetkellä panostetaan. Lisäksi kyberturvallisuusraportointi kertoo siitä, että yritys noudattaa kyberturvallisuudesta säädettyjä lakeja ja regulaatioita. Kyberturvallisuudesta kertominen voi näin ollen siis lisätä sijoittajien ja sidosryhmien kiinnostusta yritystä kohtaan. (Eijkelenboom & Nieuwsteeg 2021.)

Logiikka ajatuksen taustalla on yksinkertainen: vapaaehtoinen kyberturvallisuusraportointi viestii joko suorasti tai epäsuorasti yrityksen asiakkaille ja sidosryhmille, että yritys tekee aktiivisesti töitä ylläpitääkseen hyvää tietoturvan tasoa (Gordon ym. 2010). Nämä viestit taas kasvattavat kuluttajien luottamusta yritykseen, joka esimerkiksi alentaa kynnystä tehdä ostoksia yrityksen verkkokaupassa (Pavlou ym. 2007). Kasvanut

verkkokaupan myynti taas luonnollisesti kasvattaa yrityksen liikevaihtoa ja mahdollisesti myös tulosta.

Avoimella raportoinnilla yrityksen kohtaamista riskeistä on positiivinen yhteys yrityksen hyvään tulokseen (Isiaka 2021). Kyberturvallisuusraportoinnilla on myös osoitettu olevan positiivinen vaikutus yrityksen markkina-arvoon. Julkiset yhtiöt, jotka raportoivat kyberturvallisuustoimistaan vuosiraporteilla oma-aloitteisesti ja laajemmin, kuin laki minimissään velvoittaa, ovat keskimäärin korkeammin arvotettuja markkinoilla. (Gordon ym. 2010, Berkman ym. 2018.) Vapaaehtoinen kyberturvallisuusraportointi vaikuttaa Gordonin ym. (2010) mukaan yrityksen osakkeen hintaan positiivisesti keskimäärin 6 % verran. Berkman ym. (2018) taas antoivat yrityksille kyberturvallisuusraportoinnin pisteitä välillä 0–616, ja yhden pisteen nousu vastaa keskimäärin 1,619 USD korkeampaa osakkeen hintaa.

Myös raportoinnin sävyllä on merkitystä. Vuosiraportointia voidaan luokitella positiiviseen tai negatiiviseen sen mukaan, sisältääkö yrityksen teksti vuosiraportointikokonaisuudessa enemmän positiivissävytteisiä (esim. saavuttaa, tehokas, kannattava) vai negatiivissävytteisiä (esim. tappio, velka, riski) sanoja (Loughran & McDonald 2011). Yleistasolla positiivissävytteinen vuosiraportointi indikoi korkeampaa markkina-arvoa, negatiivissävytteinen raportointi taas matalampaa. Kun tarkastellaan erikseen kyberturvallisuusraportointia, ei positiivissävytteinen raportointi vaikuta yrityksen markkina-arvoon suuntaan tai toiseen, mutta negatiivinen raportointi on myös kyberturvallisuuden suhteen negatiivisessa yhteydessä yrityksen markkina-arvoon. (Berkman ym. 2018.)

Vapaaehtoisella raportoinnilla on erityisen positiivinen vaikutus niiden toimialojen yrityksiin, joiden liiketoiminta on jossain määrin riippuvaista verkkokaupasta, kuten esimerkiksi kuluttajatuotteiden myynti. Sen sijaan pankkisektorilla vapaaehtoinen raportointi ei juuri nosta yrityksen markkina-arvoa, joka voi johtua esimerkiksi siitä, että sijoittajat ajattelevat jo muutoinkin pitkälti säännellyllä toimialalla toimivien yritysten kiinnittävän keskimääräistä enemmän huomiota kyberturvallisuuteen. (Gordon ym. 2010.)

Kyberturvallisuusraportoinnilla on yrityksen taloudellisten hyötyjen lisäksi myös joitakin yhteiskunnallisia hyötyjä. Se, että yritykset jakavat julkisesti tietoja kyberturvallisuudesta, lisää kokonaisymmärrystä kyberturvallisuuden yleisestä tasosta ja käytännöistä, sekä toisaalta yritysten kohtaamista kyberturvallisuusuhista ja -tapahtumista. Tämän vuoksi kyberturvallisuutta voi olla mahdollisuus kehittää tehokkaammin, kun eri

organisaatiot voivat hyödyntää toistensa tietoja, eikä jokaisen tarvitse oivaltaa samoja asioita itse. Tiedon lisääminen myös mahdollistaa parempien kyberturvallisuusratkaisujen kehittämisen markkinoille, esimerkiksi kyberturvallisuusvakuutukset tai tietoturvaohjelmistot voivat näin toimia entistä tehokkaammin. (Eijkelenboom & Nieuwsteeg 2021.)

Saavutettujen hyötyjen lisäksi vapaaehtoisen kyberturvallisuusraportoinnin taustalla saattaa vaikuttaa asiakkaiden, sijoittajien tai kilpailijoiden asettama paine. Esimerkiksi tietomurtojen tapauksessa paine viestinnälle on kova, sillä tietomurrot saavuttavat usein julkista huomiota, ja näin ollen yrityksillä voi olla paineita pyrkiä viestimään avoimesti myös itse tilanteesta säilyttääkseen legitiimiytensä. Myös kilpailijoiden kokemat kyberturvallisuuden häiriötilanteet vaikuttavat. Jos kaikki yritykset tietyllä toimialalla kohtaavat samanaikaisesti häiriötilanteita, lisää yhden yrityksen avoin raportointi paineita raportoinnista myös muille. (D'Arcy & Basoglu 2022.)

### 2.3.2 Raportointia rajoittavat tekijät

Kyberturvallisuusraportoinnilla ei ole pelkästään hyötyjä, vaan on muistettava, että kyberturvallisuus on yrityksille myös merkittävä riskitekijä. Riskien hallinnan näkökulmasta on olemassa myös siis syitä, miksi kyberturvallisuusraportointia voi olla jossain määrin hyödyllistä rajoittaa.

Ensinnä, kyberturvallisuushyökkäyksen tai tietovuodon kohteeksi joutuminen ei ole yritykselle koskaan varsinainen ylpeydenaihe. Tällaisista kyberturvallisuustapahtumista raportoiminen voikin aiheuttaa yritykselle merkittävää mainehaittaa ja sidosryhmien luottamuksen heikentymistä. Toiseksi, samalla kun kyberturvallisuuskäytännöistä kerrotaan julkisesti sidosryhmille, ovat tiedot saatavilla myös kyberrikollisille. Esimerkiksi yrityksen kyberturvallisuusstrategiasta kertominen voi paljastaa samanaikaisesti myös sen kyberturvallisuuden heikkoja kohtia, joita rikolliset voivat käyttää hyväkseen. (Eijkelenboom & Nieuwsteeg 2021.)

On myös osoitettu, että yritykset, jotka raportoivat kyberturvallisuudesta erityisen pitkästi, tai sisällyttävät raportointiin erityisesti tietoja yrityksen kyberriskeistä, kokevat todennäköisemmin kyberturvallisuuden häiriötilanteita tulevaisuudessa. Tämän vuoksi voi olla, että jotkin yritykset raportoivat kyberturvallisuudestaan mieluummin niukemmin, kuin laajemmin. (Li ym. 2018.)

## 2.4 Kyberturvallisuusraportoinnin käytännöt

### 2.4.1 Raportoinnin yleisyys ja laajuus

Kansainvälisesti kyberturvallisuusraportointi on niukkaa, eikä tarkkoja tietoja yritysten kokemista tietoturvauhista tai niiden tietoturvakäytännöistä ole tavanomaista kertoa julkisesti, joskin käytännöt vaihtelevat eri yritysten välillä. Esimerkiksi S&P/TSX 60 -listatut organisaatiot, eli Toronton pörssiin listatut 60 suurinta yritystä, raportoivat kyberturvallisuudestaan keskimäärin melko heikolla tasolla. Peräti 87 % näistä organisaatioista viittasi kyberturvallisuuteen vuosiraportointikokonaisuudessaan, mutta raportointi pysyi yleisluontoisena, eikä yrityskohtaisia tietoja juurikaan paljastettu. (Héroux & Fortin 2020.)

Laajennettaessa otantaa S&P/TSX Composite Index -listattuihin yrityksiin (indeksi, joka kattaa noin 70 % Toronton pörssin markkina-arvosta, tässä tapauksessa 250 suurinta yritystä), noin 84 % yrityksistä viittasi kyberturvallisuuteen vuosiraporteissaan. Tutkimuksessa annettiin raportoinnin kattavuudelle pisteitä välillä 0–40, ja keskiarvo kaikille yrityksille oli 11,58. Tämänkin tutkimuksen perusteella kyberturvallisuuden raportointi on siis melko heikolla tasolla. (Héroux & Fortin 2022.)

Myös Hollannissa päädyttiin samankaltaisiin tuloksiin: 87 % vertailluista yrityksistä mainitsi kyberturvallisuuden ainakin jollain tasolla vuosiraporteissaan. Jopa 53 % yrityksistä laajensi kuvauksia hieman tarkemmin esimerkiksi kyberturvallisuusstrategian, -tapahtumien tai -investointien osalta, mutta nämä tiedot eivät olleet kovinkaan tarkkoja. Itseasiassa vain 5 % vertailluista yrityksistä kertoi kyberturvallisuudesta kuudesta tai useammasta näkökulmasta. (Eijkelenboom & Nieuwesteeg 2021.)

Berkman ym. (2018) taas mittasivat yhdysvaltalaisten yritysten kyberturvallisuusraportoinnin tasoa antamalla niille pisteitä siten, että yritykset, jotka eivät viitanneet ollenkaan kyberturvallisuuteen vuosiraportointikokonaisuudessaan, saivat 0 pistettä, ja kattavimmin kyberturvallisuutta käsitellyt yritys sai vertailussa 616 pistettä. Keskiarvo kaikkien yritysten pisteille oli 21,93, mikä myös viittaa melko alhaiseen raportoinnin keskitasoon.

Kyberturvallisuusraportoinnissa on eroja muun muassa yrityksen toimialan perusteella. Mitä riippuvaisempi yrityksen toimiala on teknologiasta, sitä enemmän sanoja se keskimäärin käyttää kyberturvallisuudesta kertomiseen. Kyberturvallisuudesta raportoidaan erityisen paljon esimerkiksi kuluttajapalveluiden, tietojärjestelmäpalvelujen ja

pankkipalveluiden toimialoilla. (Gao ym. 2020.) Heikointa raportointi sen sijaan on aloilla, jotka eivät ole suoraan riippuvaisia teknologiasta, kuten hiiliteollisuudessa ja tekstiiliteollisuudessa (Berkman ym. 2018).

Myös yrityksen koko vaikuttaa kyberturvallisuusraportointiin, ja suurempi koko ennakoi laajempaa tietoturvallisuusraportointia. Yrityksen liikevaihdon kasvaessa 10 %, myös kyberturvallisuuteen liittyvien sanojen määrä 10-K-raportilla (lakisääteinen taloudellinen vuosiraportti Yhdysvalloissa) kasvoi keskimäärin 3 kpl. Tämä ei kuitenkaan tarkoita automaattisesti parempaa kyberturvallisuusraportointia. Pienempien yritysten kyberturvallisuuteen liittyvä raportointi on nimittäin keskimäärin helpommin luettavaa. (Gao ym. 2020.)

### 2.4.2 Raportoinnin sisällöt

Héroux & Fortin (2020) tarkastelivat kyberturvallisuusraportointia S&P/TSX 60 -yhtiöiden vuosiraportointikokonaisuuksissa. Tutkimuksessa raportointi jaettiin eri asiakokonaisuuksiin, joita olivat kyberturvallisuusriskit, kyberturvallisuuden häiriötilanteiden mahdolliset vaikutukset, vastuu kyberturvallisuusstrategiasta, kyberturvallisuusriskien lieventäminen, potentiaaliset kyberturvallisuuden häiriötilanteet, kohdatut kyberturvallisuuden häiriötilanteet sekä muut mainitut kyberturvallisuusasiat. Yritykset kertoivat eniten tietoja liittyen kyberturvallisuusriskeihin ja vähiten taas todellisiin, kohdattuihin kyberturvallisuuden häiriötilanteisiin sekä muihin mainittuihin kyberturvallisuusasioihin. Vuonna 2022 Héroux & Fortin toistivat saman tutkimuksen S&P/TSX Composite Index -yhtiöillä, ja yleisimmin ja vähiten raportoidut asiat pysyivät samoina.

Yhdysvaltalaiset julkiset osakeyhtiöt ovat velvoitettuja julkaisemaan vuosiraportin lisäksi joka vuosi myös 10-K-raportin, joka on vuosiraporttia yksityiskohtaisempi, ja tarjoaa kattavan yhteenvedon yrityksen taloudellisesta suorituskyvystä. Näiden perusteella yritykset raportoivat kaikista eniten dataan liittyvistä riskeistä, erityisesti tietovuotojen näkökulmasta, sekä riskeistä, joilla voi olla merkitystä yrityksen toimintakykyyn ja toiminnan jatkuvuuteen. Vähiten taas raportoidaan yrityksen yksilöllisistä kyberturvallisuustoimenpiteistä ja kyberhäiriötilanteista. (Gao ym. 2020.)

Pankeilla on hallussaan valtava määrä luottamuksellista dataa, jonka vuoksi pankkisektori kohtaa myös poikkeuksellisen paljon kyberhyökkäyksiä. Firoozi & Mohsni (2023) tarkastelivat pohjoisamerikkalaisten pankkien kyberturvallisuusraportointia osana

vuosiraportointikokonaisuuksia 62 eri aspektin kannalta, ja näistä 23 arviointikohdetta huomioitiin vähintään joka toisen pankin vuosiraportointikokonaisuudessa. Kaikki tarkastelluista pankeista mainitsivat kyberturvariskit osana vuosiraportointikokonaisuuttaan, ja yli 90 % kertoi kyberriskien olevan osa yrityksen merkittävimpiä riskejä, sekä kertoi liiketoiminnoista tai muista näkökohdista, jotka aiheuttavat kyberturvallisuuden kannalta merkittäviä riskejä. Tämän lisäksi yli 90 % nosti vuosiraportointikokonaisuudessaan esiin myös kyberriskien toteutumisen mahdolliset seuraukset kuten mainehaitan, asiakkaiden luottamuksen heikkenemisen, menetetyt voitot ja luottamuksellisten tietojen vuotamisen. Toisaalta 62 tarkastellun aspektin mukana oli myös 18 arviointikohdetta, jotka mainittiin alle 20 % vuosiraporteissa. Yksikään tarkastelluista pankeista ei ottanut kantaa esimerkiksi tietoturvatapahtumien kustannuksiin, joita aiheutuu muun muassa mainehaitan, tulevien tietoturvatapahtumien ehkäisyn sekä lakisääteisten selvitysten toteuttamisen kautta.

Kaiken kaikkiaan myös pankkisektorilla kyberturvaraportointi jää melko yleisluontoiselle tasolle. Pankit kertovat vuosiraportointikokonaisuuksissaan esimerkiksi paljon kyberriskeistä ja niiden mahdollisista vaikutuksista. Riskit ovat kuitenkin usein samoja koko toimialalle, eivätkä näin ollen sisällä yrityskohtaisia tietoja. Esimerkiksi yrityksen yksilöllisistä tietoturvakäytännöistä tai hallintotavoista taas ei ole yleistä kertoa osana vuosiraportointia. (Firoozi & Mohsni 2023.)

## 2.5 Kyberturvallisuusraportoinnin trendit

Kyberturvallisuus on viime vuosina noussut yhä tärkeämmäksi yhteiskunnalliseksi aiheeksi. Sitran megatrendien 2023 mukaan tulevaisuudessa ”digitalisoituva maailma on entistä haavoittuvampi”, ja digitaalisten ratkaisujen lisääntyminen joka puolella luo uusia tietoturvauhkia ympärillemme. Samaan aikaan kuitenkin myös ihmisten teknologinen ymmärrys lisääntyy, ja tämän vuoksi ihmisillä on paremmat kyvyt ymmärtää meitä ympäröiviä kyberuhkia, sekä miten niiltä on mahdollista suojautua. (Sitra 2023.)

Myös kyberturvallisuusraportointi on lisääntynyt viime vuosien aikana. Esimerkiksi vuonna 2010 noin 14 % yrityksistä raportoi kyberturvallisuudesta osana vuosiraportointikokonaisuuttaan, kun taas vuonna 2018 vastaava luku oli jo noin 89 % (Gordon ym. 2010, Berkman ym. 2018). Pankkisektorilla taas vuonna 2014 noin 35 % pohjoisamerikkalaisista pankeista raportoi kyberturvallisuudesta, ja vuonna 2020 määrä oli kasvanut 50 %:iin (Firoozi & Mohsni 2023). Samankaltaisiin tuloksiin päädyttiin myös

Bangladeshissa ja Etelä-Amerikassa. Vuonna 2014 Bangladeshin pankkien vuosiraportointikokonaisuuksissa kyberturvallisuuteen liittyviä hakusanoja löydettiin keskimäärin 7,6 kpl per raportti, kun vuonna 2020 vastaava luku oli 38,6. Tämä tarkoittaa siis yli 400 % kasvua hakusanojen määrässä seitsemän vuoden aikana. (Mazumder & Hossain 2022.) Etelä-Amerikassa kasvu on ollut maltillisempaa, mutta tasaista: rahoitussektorin yritysten kyberturvallisuusraportointi on kasvanut noin 85 % vuosien 2016 ja 2020 välillä (Ramírez ym. 2022).

Samalla kun raportoinnin määrä lisääntyy, lisääntyy myös sen kompleksisuus. Vuosien 2011 ja 2018 välillä kyberturvallisuusraportit ovat muuttuneet yhä vaikealukuisemmiksi. Tämä voi johtua esimerkiksi siitä, että digitaalinen ympäristömme on kasvanut suuremmaksi ja monimutkaisemmaksi. Näin ollen yritykset kyllä lisäävät kyberturvallisuusraportoinnin määrää, mutta samalla tieto muuttuu kompleksisemmaksi ja raporttien ymmärtämiseen tarvitaan myös parempaa ymmärrystä kyberturvallisuudesta. (Gao ym. 2020.)

Erityisesti Yhdysvalloissa kyberturvallisuusraportoinnin kasvu on yhteydessä SECin ohjeistukseen kyberturvallisuusraportoinnista vuonna 2011. Vuosien 2007 ja 2011 välillä raportointi kasvoi noin 23 prosenttiyksikön verran, kun vuosien 2011 ja 2015 välillä kasvua oli noin 31 prosenttiyksikköä. (Li ym. 2018.)

Raportoinnin kasvuun voi myös vaikuttaa sukupuolten välisen tasa-arvon kasvu yritysten hallituksissa. Esimerkiksi Suomessa naisten osuus pörssiyhtiöiden hallituksissa kesällä 2023 oli keskimäärin noin 33 %, kun vielä vuonna 2007 osuus oli vain 12 % (THL 2023, Lipasti ym. 2020). Sillä, että yrityksen hallituksessa on myös naisia, on osoitettu olevan positiivinen yhteys yrityksen tulokseen (Baker ym. 2020). Naisten läsnäolo pörssiyritysten hallituksissa näyttää vaikuttavan positiivisesti myös raportoinnin määrään yrityksen kohtaamista riskeistä (Bravo 2018). Lisäksi yritykset, joiden hallituksissa on vähintään kolme naista, raportoivat kyberturvallisuudesta keskimäärin enemmän muihin yrityksiin verrattuna (Radu & Smaili 2022).

Käänteentekeviä kohtia raportoinnin kannalta voivat myös olla laajat kyberturvallisuushäiriöt, jotka ylittävät kansallisen tai kansainvälisen uutiskynnyksen. Esimerkiksi vuonna 2016 Bangladeshin keskuspankki joutui poikkeuksellisen suuren kybervarkauden kohteeksi, kun hakkerit veivät kaiken kaikkiaan pankin tileiltä 81 miljoonaa Yhdysvaltain dollaria. Vuoden 2016 jälkeen myös kyberturvallisuusraportointi kasvoi bangladeshilaisissa pankeissa räjähdysmäisesti. Raportointi kasvoi keskimäärin 32 % vuodessa vuosien

2014 ja 2020 välillä, mutta kasvu oli voimakkainta juuri vuoden 2016 raporteissa, joissa näkyy peräti 62 %:n kasvu verrattuna edelliseen vuoteen. (Mazumder & Hossain 2022.)

# 3 Metodologia

## 3.1 Tutkimusmetodit

Tutkimus toteutettiin laadullisena tutkimuksena, ja tutkimusmenetelmäksi valikoitui sisällönanalyysi. Useat tutkijat ovat todenneet sisällönanalyysin korvaamattomaksi tutkimusmenetelmäksi sellaisten dokumenttien tutkimiseen, joita ei ole alun perin käytetty tutkimustarkoituksiin, kuten lehtiartikkelit, tiedotteet tai tässä tapauksessa vuosikertomukset. Sisällönanalyysin avulla tekstiaineisto on mahdollista jakaa luokittelun avulla pienempiin, helpommin käsiteltäviin osiin. (Weber 1990, 5.) Koska sisällönanalyysi mahdollistaa dokumenttien analysoinnin systemaattisesti ja objektiivisesti, tutkittavasta ilmiöstä voidaan tätä kautta pyrkiä saamaan tiivistetty ja yleismuotoinen kuvaus. Analysoitua aineistoa voidaan myös kvantifioida, ja kuvatusta aineistosta voidaan näin ollen saada myös määrällisiä tuloksia. (Tuomi & Sarajärvi 2018.)

Koska tutkimuksen aineisto on vapaasti saatavilla yritysten verkkosivuilla, ei tässä tutkimuksessa tunnistettu eettisiä ongelmia.

## 3.2 Aineiston esittely

Tutkimuksen aineisto kerättiin yrityksiltä, jotka olivat listautuneina Helsingin pörssin päälistalle (OMX Helsinki) 31.12.2023. Aineiston lähteeksi valittiin niiden yritysten vuosiraportointikokonaisuuteen kuuluvat dokumentit, jotka 1) olivat suomenkielisiä, 2) ladattavissa PDF-muotoisena vapaasti yritykseen verkkosivuilla ja 3) luettavissa tekstintunnistusohjelmalla.

Aineisto kerättiin uusimmista vuosiraporteista, jotka olivat saatavilla 25.2.2024 mennessä. Tässä vaiheessa saatavilla oli 18 kpl vuoden 2023 raportteja, ja 94 kpl vuoden 2022 raportteja.

Aineistossa huomioitiin kaikki ne vuosiraportoinnin dokumentit, jotka yritys itse omilla verkkosivuillaan oli osoittanut kuuluvan vuosiraportointiin. Vuosiraportointi koostui aineiston yrityksillä 1–6 erillisestä dokumentista, jotka oli otsikoitu seuraavasti tai muulla vastaavalla tavalla:

- vuosiraportti, vuosikertomus tai vuosikatsaus
- toimintakertomus

- tilinpäätös
- liiketoimintakatsaus, taloudellinen katsaus tai taloudelliset tiedot
- hallinnointiraportti tai selvitys hallinto- ja ohjausjärjestelmästä
- palkitsemisraportti
- vastuullisuusraportti, kestävän kehityksen raportti tai GRI-liite
- selvitys muista kuin taloudellisista tiedoista

Aineiston joukosta rajattiin pois yritykset, joiden toimialana tai merkittävänä osana palvelutarjoomaa on tietoturva tai kyberturvallisuus, sillä näiden tarkasteleminen valituin tutkimusmenetelmin ei ole mielekästä. Näillä yrityksillä kyberturvallisuuteen liittyvät hakusanat viittaavat useammin yrityksen tuotteisiin tai palveluihin, eivätkä niinkään yrityksen omaan kyberturvallisuuteen.

Rajauksien jälkeen aineisto kerättiin 112 yhtiön vuosiraporteista. Yritykset on esitetty taulukossa 1.

Taulukko 1 Yritykset, joiden vuosiraporteista aineisto on kerätty

| | | |
|---|---|---|
| Afarak Group | Kamux Oyj | Rapala VMC Oyj |
| Aktia Bank Abp | Kemira Oyj | Raute Oyj |
| Alisa Pankki Oyj | Keskisuomalainen Oyj | Reka Industrial Oyj |
| Alma Media Oyj | Kesko Oyj | Relais Group Oyj |
| Anora Group Oyj | KH Group Oyj | Revenio Group Oyj |
| Apetit Oyj | Kojamo Oyj | Robit Oyj |
| Aspo Oyj | KONE Oyj | Saga Furs Oyj |
| Aspocomp Group Oyj | Konecranes Oyj | Sampo Oyj |
| Atria Oyj | Koskisen Oyj | Sanoma Oyj |
| Biohit Oyj | Kreate Group Oyj | Scanfil Oyj |
| Boreo Oyj | Lamor Corporation Oyj | Siili Solutions Oyj |
| CapMan Oyj | Lassila & Tikanoja Oyj | Sitowise Group Oyj |
| Cargotec Oyj | Lehto Group Oyj | Solteq Oyj |
| Caverion Oyj | Mandatum | SRV Yhtiöt Oyj |
| Citycon Oyj | Marimekko Oyj | Stockmann Oyj Abp |
| Componenta Oyj | Martela Oyj | Stora Enso Oyj |
| Consti Oyj | Metsä Board Oyj | Suominen Oyj |
| Digitalist Group Oyj | Metso Oyj | Taaleri Oyj |

| | | |
|---|---|---|
| Dovre Group Oyj | Musti Group Oyj | Talenom Oyj |
| Eezy Oyj | Neste Oyj | Tecnotree Oyj |
| Elecster Oyj | NoHo Partners Oyj | Terveystalo Oyj |
| Enento Group Oyj | Nokian Renkaat Oyj | Tokmanni Group Oyj |
| Enersense International Oyj | Nurminen Logistics Oyj | Trainers´ House Oyj |
| eQ Oyj | Olvi Oyj | Tulikivi Oyj |
| Etteplan Oyj | Oma Säästöpankki Oyj | United Bankers Oyj |
| Evli Oyj | Optomed Oyj | UPM-Kymmene Oyj |
| Exel Composites Oyj | Oriola Oyj | Uponor Oyj |
| Finnair Oyj | Orion Oyj | Vaisala Oyj |
| Fiskars Oyj Abp | Orthex Oyj | Valmet Oyj |
| Fortum Oyj | Outokumpu Oyj | Valoe Oyj |
| Glaston Oyj Abp | Ovaro Kiinteistösijoitus Oyj | Verkkokauppa.com Oyj |
| Harvia Oyj | Pihlajalinna Oyj | Viking Line Abp |
| HKScan Oyj | Ponsse Oyj | Wärtsilä Oyj Abp |
| Honkarakenne Oyj | Purmo Group Oyj | Wetteri Oyj |
| Huhtamäki Oyj | Puuilo Oyj | Wulff-Yhtiöt Oyj |
| Ilkka Oyj | QPR Software Oyj | YIT Oyj |
| Incap Oyj | Qt Group Oyj | |
| Investors House Oyj | Raisio Oyj | |

Aineistosta rajattiin pois 18 yritystä. Tarkastelematta jätetyt yritykset on esitetty taulukossa 2.

Taulukko 2 Yritykset, jotka on rajattu pois aineistosta

| | | |
|---|---|---|
| AS Tallink Grupp FDR | Kesla Oyj | SSH Communications Security |
| Bittium Oyj | Nokia Oyj | Teleste Oyj |
| Digia Oyj | Nordea Bank Abp | Telia Company |
| Elisa Oyj | Panostaja Oyj | TietoEVRY Oyj |
| Endomines Finland Oyj | PunaMusta Media Oyj | WithSecure Oyj |
| F-Secure Oyj | Remedy Entertainment Oyj | Ålandsbanken Abp |
| Gofore Oyj | Sotkamo Silver AB | |
| Innofactor Plc | SSAB | |

Kerätty aineisto on luokiteltu lisäksi toimialojen sekä yritysten koon perusteella. Nämä tiedot on esitetty taulukoissa 3 ja 4.

Taulukko 3 Aineisto toimialoittain

| Toimiala | Yritysten lukumäärä aineistossa |
|---|---|
| Teollisuustuotteet- ja palvelut | 39 |
| Kuluttajatuotteet | 15 |
| Rahoituspalvelut | 11 |
| Tukku- ja vähittäiskauppa | 9 |
| Teknologia | 8 |
| Perusteollisuus | 8 |
| Terveydenhuolto | 7 |
| Kiinteistöt | 4 |
| Kuluttajapalvelut | 4 |
| Media | 4 |
| Muut | 3 |
| *Yhteensä* | *112* |

Taulukko 4 Aineisto kokoluokittain

| Kokoluokka | Yritysten lukumäärä aineistossa |
|---|---|
| Suuri (markkina-arvo yli 1 MRD €) | 27 |
| Keskisuuri (markkina-arvo 150 M € - 1 MRD €) | 40 |
| Pieni (markkina-arvo alle 150 M €) | 45 |
| *Yhteensä* | *112* |

## 3.3 Teoreettinen viitekehys

Heroux & Fortin (2020) esittelevät viitekehyksen, jossa yritysten kyberturvallisuusraportointi on jaettu seitsemään eri osa-alueeseen: 1) kyberturvallisuusriskit, 2) kyberturvallisuuden häiriötilanteiden mahdolliset vaikutukset, 3) vastuu kyberturvallisuusstrategiasta, 4) kyberturvallisuusriskien lieventäminen, 5) potentiaaliset kyberturvallisuuden häiriötilanteet, 6) kohdatut kyberturvallisuuden häiriötilanteet sekä 7) muut mainitut kyberturvallisuusasiat.

Tämän tutkimuksen tulosten analysoinnissa ja jaottelussa on hyödynnetty mukaillen Hérouxin & Fortinin (2020) viitekehystä, ja käytetty seuraavia seitsemää teemaa: 1) Kyberriskien tunnistaminen, 2) kyberturvallisuuden häiriötilanteiden mahdolliset vaikutukset, 3) kyberturvallisuusstrategia, 4) kyberturvallisuustoimenpiteet, 5) kyberturvallisuusuhat ja mahdolliset häiriötilanteet, 6) kohdatut kyberturvallisuuden häiriötilanteet ja 7)

muut kyberturvallisuusasiat. Taulukossa 5 on esitetty tarkemmin viitekehyksen teemoja tämän tutkimuksen kannalta.

Taulukko 5 Tutkimuksen teemat Hérouxin & Fortinin (2020) viitekehystä mukaillen

| # | Teema - Héroux & Fortin (2020) | Teema tässä tutkimuksessa | Sisällöt tässä tutkimuksessa |
|---|---|---|---|
| 1 | kyberturvallisuusriskit | kyberriskien tunnistaminen | Tunnistaako yritys kyberturvallisuuden merkittäväksi strategiseksi tai operatiiviseksi riskiksi? |
| 2 | kyberturvallisuuden häiriötilanteiden mahdolliset vaikutukset | kyberturvallisuuden häiriötilanteiden mahdolliset vaikutukset | Mitä taloudellisia, maine- tai muita haittoja yritykselle voi mahdollisesti koitua kyberturvallisuuden häiriötilanteiden seurauksena? |
| 3 | vastuu kyberturvallisuusstrategiasta | kyberturvallisuusstrategia | Onko yrityksellä kyberturvallisuusstrategiaa? Miten vastuu kyberturvallisuudesta on jaettu? Mikä on yrityksen hallinnon näkökulma kyberturvallisuuteen? |
| 4 | kyberturvallisuusriskien lieventäminen | kyberturvallisuustoimenpiteet | Mitä toimenpiteitä yritys tekee kyberturvallisuusriskien lieventämiseksi, kyberturvallisuuden parantamiseksi ja kyberturvallisuustilanteen seurantaan ja hallintaan liittyen? |
| 5 | potentiaaliset kyberturvallisuuden häiriötilanteet | kyberturvallisuusuhat ja mahdolliset häiriötilanteet | Mitä yleisiä tai yritys- tai toimialakohtaisia kyberturvallisuuden uhkia tai häiriötilanteita yritys voi kohdata? |
| 6 | kohdatut kyberturvallisuuden häiriötilanteet | kohdatut kyberturvallisuuden häiriötilanteet | Mitä toteutuneita kyberturvallisuuden häiriötilanteita yritys on kohdannut? Miten näistä on kerrottu? |
| 7 | muut mainitut kyberturvallisuusasiat | muut kyberturvallisuusasiat | Muut kyberturvallisuuteen liittyvät asiat esimerkiksi lainsäädännön, kestävän kehityksen tai yhteiskunnallisen näkökulman kannalta. |

## 3.4 Aineiston analyysi

Aineiston analyysi toteutettiin etsimällä kyberturvallisuuteen liittyviä hakusanoja aineistosta. Hakusanat valittiin Turvallisuuskomitean Kyberturvallisuuden sanaston avulla. Kaikkia sanaston käsitteitä ei otettu huomioon, vaan hakusanat valittiin teemoista *tietoturva*, *kyberturvallisuus* ja *kyberuhat*, sillä osa sanaston käsitteistä voi kontekstin mukaan viitata myös muuhun kuin kyberturvallisuuteen, ja näin ollen niiden tarkastelu olisi voinut vääristää tutkimuksen tuloksia.

Hakusanoja valittaessa otettiin huomioon, että osa sanaston käsitteistä tulee käsiteltyä yhden hakusanan perusteella. Esimerkiksi hakusana *tietoturva* kattaa myös käsitteet tietoturvatapahtuma, tietoturvahäiriö ja niin edelleen. Hakusanoja muodostettaessa pyrittiin

myös ottamaan mahdollisimman kattavasti huomioon suomen kielen eri sijapäätteet ja taivutusmuodot. Esimerkiksi hakusana *haittaohjelm* kattaa muodot haittaohjelma, haittaohjelmat, haittaohjelman, haittaohjelmista ja niin edelleen.

Valitut hakusanat on esitetty taulukossa 6. Koko lista aineistosta löytyneistä hakusanoista on esitetty tarkemmin tutkimuksen liitteessä 1.

Taulukko 6 Hakusanat, joilla aineiston analyysi toteutettiin

| # | Hakusana | Sisältää mm. |
|---|---|---|
| 1 | kyber | kyberturvallisuus, kyberhyökkäys, kyberuhat |
| 2 | tietoturv | tietoturva, tietoturvallisuus, tietoturvauhat |
| 3 | palvelunest | palvelunestohyökkäys, palvelunestohyökkäykset, palvelunestohyökkäyksestä |
| 4 | haittaohjelm | haittaohjelma, haittaohjelmat, haittaohjelmien |
| 5 | kiristysohjelm | kiristysohjelma, kiristysohjelmat, kiristysohjelmista |
| 6 | hakkeri | hakkeri, hakkerit, hakkerien |
| 7 | haavoittuv | haavoittuvuus, haavoittuvuudet, haavoittuvuuksien |
| 8 | verkkovalvomo | tietoverkkovalvomo, verkkovalvomo |
| 9 | pääsynhallin | pääsynhallinta, pääsynhallinnan, pääsynhallinnasta |
| 10 | identiteetinhallin | identiteetinhallinta, identiteetinhallinnan, identiteetinhallinnasta |
| 11 | käyttöoikeuksien hallin | käyttöoikeuksien hallinta, käyttöoikeuksien hallinnan |
| 12 | monivaihei | monivaiheinen todentaminen, monivaiheinen todennus |
| 13 | verkkovalvon | verkkovalvonta, tietoverkkovalvonta, verkkovalvonnan |
| 14 | verkkotiedus | verkkotiedustelu, tietoverkkotiedustelu, verkkotiedustelut |
| 15 | verkkohyök | verkkohyökkäys, tietoverkkohyökkäys, verkkohyökkäykset |

Aineisto tallennettiin ensin tutkijan työasemalle, jonka jälkeen se käytiin koneellisesti hakusanojen avulla läpi. Aineisto käsiteltiin Pythonin avulla, ja jokaisen hakusanan kohdalta haettiin lisäksi sivunumero, jolla hakusana esiintyy, sekä sata merkkiä ennen ja jälkeen hakusanan, jotta hakusanan liittäminen oikeaan kontekstiin tai manuaalinen tarkastaminen tarpeen tullen oli helpompaa. Tiedot vietiin Exceliin, jossa tarkempi aineiston luokittelu ja analysointi tehtiin. Kaikki hakusanat tarkasteltiin manuaalisesti kontekstin avulla läpi ja näin aineiston joukosta poistettiin ne osumat, jotka eivät liittyneet kyberturvallisuuteen. Epäselvissä tilanteissa konteksti tarkastettiin alkuperäisiltä pdf-dokumenteilta. Tämän jälkeen osumat luokiteltiin viitekehyksen mukaan yläteemoihin ja edelleen tarkempiin alateemoihin tarkastelua varten.

# 4 Tutkimustulokset

## 4.1 Yleiset havainnot aineistosta

### 4.1.1 Kyberturvallisuusraportoinnin yleisyys

Tutkimuksen tuloksien perusteella taulukossa 7 esitetään, että aineiston 112 yrityksen joukosta 96 yritystä raportoi kyberturvallisuudesta ainakin jollakin tasolla. 16 yrityksen vuosiraportoinnista ei taas löytynyt osumia yhdellekään tutkimuksessa käytetylle hakusanalle.

Taulukko 7 Raportoinnin yleisyys toimialoittain ja kokoluokittain

| **Toimiala** | **Raportoi (%)** | **Ei raportoi (%)** |
|---|---|---|
| Teollisuustuotteet- ja palvelut | 33 (85 %) | 6 (15 %) |
| Kuluttajatuotteet | 11 (73 %) | 4 (27 %) |
| Rahoituspalvelut | 11 (100 %) | 0 (0 %) |
| Tukku- ja vähittäiskauppa | 8 (89 %) | 1 (11 %) |
| Teknologia | 7 (88 %) | 1 (13 %) |
| Perusteollisuus | 7 (88 %) | 1 (13 %) |
| Terveydenhuolto | 6 (86 %) | 1 (14 %) |
| Kiinteistöt | 2 (50 %) | 2 (50 %) |
| Kuluttajapalvelut | 4 (100 %) | 0 (0 %) |
| Media | 4 (100 %) | 0 (0 %) |
| Muut | 3 (100 %) | 0 (0 %) |
| *Yhteensä* | *96 (86 %)* | *16 (14 %)* |
| **Kokoluokka** | **Raportoi (%)** | **Ei raportoi (%)** |
| Suuri | 27 (100 %) | 0 (0 %) |
| Keskisuuri | 36 (90 %) | 4 (10 %) |
| Pieni | 33 (73 %) | 12 (27 %) |
| *Yhteensä* | *96 (86 %)* | *16 (14 %)* |

Yleisintä raportointi on rahoituspalveluiden, kuluttajapalveluiden ja median toimialoilla sekä muilla toimialoilla, joilla 100 % yrityksistä raportoi kyberturvallisuudesta osana vuosiraportointiaan. Niiden yritysten lukumäärien välillä, joilta ei löytynyt vuosiraporteistaan yhtään osumaa käytetyille hakusanoille, ei ole havaittavissa merkittäviä eroja toimialan perusteella. On kuitenkin huomattava, että kiinteistötoimialan yrityksistä 50 % ei raportoi kyberturvallisuudesta ollenkaan, joskin toimialan yritysten kokonaislukumäärä aineistossa on melko pieni. Kokoluokan suhteen sen sijaan kaikki suuret yritykset olivat

raportoineet kyberturvasta. Näin ollen kaikki yritykset, joilta osumia hakusanoille ei löytynyt, olivat kokoluokaltaan keskisuuria tai pieniä.

### 4.1.2 Raportoinnin laajuus

Hakusanojen osumien määrän perusteella voidaan esittää päätelmiä myös raportoinnin laajuudesta. Taulukossa 8 esitetään tulosten perusteella havainnot osumien yrityskohtaisista lukumääristä toimialoittain ja kokoluokittain. Keskimääräinen osumien määrä yritysten raporteissa oli 12,2, eli yritykset käyttävät kyberturvallisuuteen liittyviä sanoja vuosiraporteissaan keskimäärin 12 kertaa. Yritysten välillä oli kuitenkin selkeää vaihtelua, sillä laajimmin raportoiva yritys käytti hakusanoja raportoinnissaan yhteensä 241 kertaa, kun osa yrityksistä ei raportoinut kyberturvallisuudesta ollenkaan.

Taulukko 8 Raportoinnin laajuus toimialoittain ja kokoluokittain

| **Toimiala** | **Yritysten lkm.** | **Osumien lkm.** | **Osumien ka per yritys** | **Vaihteluväli** |
|---|---|---|---|---|
| Media | 4 | 217 | 54,3 | 24–93 |
| Rahoituspalvelut | 11 | 378 | 34,4 | 1–241 |
| Terveydenhuolto | 7 | 126 | 18,0 | 0–59 |
| Tukku- ja vähittäiskauppa | 9 | 118 | 13,1 | 0–63 |
| Perusteollisuus | 8 | 63 | 7,9 | 0–23 |
| Kiinteistöt | 4 | 31 | 7,8 | 0–18 |
| Teknologia | 8 | 60 | 7,5 | 0–34 |
| Teollisuustuotteet- ja palvelut | 39 | 277 | 7,1 | 0–30 |
| Muut | 3 | 20 | 6,7 | 5–8 |
| Kuluttajatuotteet | 15 | 70 | 4,7 | 1–13 |
| Kuluttajapalvelut | 4 | 6 | 1,5 | 1–3 |
| *Yhteensä* | *112* | *1366* | *12,2* | *0–241* |
| **Kokoluokka** | **Yritysten lkm.** | **Osumien lkm.** | **Osumien ka per yritys** | **Vaihteluväli** |
| Suuri | 27 | 701 | 26,0 | 2–241 |
| Keskisuuri | 40 | 416 | 10,4 | 0–68 |
| Pieni | 45 | 249 | 5,5 | 0–34 |
| *Yhteensä* | *112* | *1366* | *12,2* | *0–241* |

Kyberturvallisuudesta raportoitiin keskimääräistä enemmän median, rahoituspalveluiden, terveydenhuollon ja tukku- ja vähittäiskaupan yrityksissä. Suppeimmin raportoitiin taas

kuluttajapalveluiden ja -tuotteiden toimialoilla sekä muilla toimialoilla. Kokoluokan perusteella kyberturvallisuudesta raportoivat eniten suuret yritykset, vähiten taas pienet.

### 4.1.3 Raportoinnin keskeiset sisällöt

Raportoinnin keskeiset sisällöt jaettiin seitsemään eri teemaan Hérouxin & Fortinin (2020) viitekehyksen perusteella. Taulukossa 9 esitetään tulosten perusteella kyberturvallisuusraportoinnin keskeiset sisällöt. Tuloksia tarkasteltaessa on otettava huomioon, että sarakkeessa *yritysten lukumäärä* osa yrityksistä on voitu ottaa huomioon useammalla eri rivillä, eikä rivin *yhteensä* kohdalla yritysten lukumäärä ole näin ollen ylempien rivien summa, vaan yritysten lukumäärä kyseisen teeman kohdalla yhteensä. Tämä huomio pätee myös taulukoihin 10–16.

Yläteemoihin luokiteltujen hakusanojen osumien lisäksi aineistossa oli mukana osumia, joissa hakusana tai sen konteksti oli epäselvä, eikä sitä näin ollen voitu yhdistää yhteenkään yläteemaan. Tähän kategoriaan kuuluivat myös otsikkotason tai luetteloiden osumat, joissa hakusanaa ei saatu liitettyä suoraan yläteemaan. Tällainen oli esimerkiksi otsikko ”Kyberturvallisuus”, jonka alla esiteltiin kaikki yrityksen kyberturvallisuuteen liittyvät asiat.

Taulukko 9 Raportoinnin keskeiset sisällöt

| **Yläteema** | **Yritysten lkm.** | **Mainintojen lkm.** | **Mainintojen ka per yritys** | **Vaihteluväli** |
|---|---|---|---|---|
| 1) Kyberriskien tunnistaminen | 43 | 91 | 2,1 | 1–7 |
| 2) Kyberturvallisuuden häiriötilanteiden mahdolliset vaikutukset | 37 | 83 | 2,2 | 1–7 |
| 3) Kyberturvallisuusstrategia | 30 | 171 | 5,7 | 1–41 |
| 4) Kyberturvallisuustoimenpiteet | 75 | 655 | 8,7 | 1–131 |
| 5) Kyberturvallisuusuhat ja mahdolliset häiriötilanteet | 36 | 78 | 2,2 | 1–8 |
| 6) Kohdatut kyberturvallisuuden häiriötilanteet | 14 | 72 | 5,1 | 1–25 |
| 7) Muut kyberturvallisuusasiat | 20 | 56 | 2,8 | 1–15 |
| Hakusana tai konteksti epäselvä | 53 | 184 | 3,5 | 1–35 |
| *Yhteensä* | *96* | *1390* | *14,5* | *1–241* |

Tulosten perusteella yritykset raportoivat eniten suoranaisista kyberturvallisuustoimenpiteistään. Tästä yläteemasta raportoi yhteensä 75 yritystä, ja keskimäärin teemaan liittyviä mainintoja esiintyi vuosiraporteissa 8,7 kertaa.

Raportoivien yritysten lukumäärän perusteella vähiten raportoitiin taas kohdatuista kyberturvallisuuden häiriötilanteista, joista raportoi yhteensä vain 14 yritystä. Huomattavaa kuitenkin on, että tähän teemaan liittyvien mainintojen keskiarvo raporteilla oli 5,1. Voidaan siis olettaa, että yritykset, jotka raportoivat aiheesta, raportoivat siitä kuitenkin melko laajasti. Teemakohtaisten mainintojen lukumäärän perusteella taas vähiten raportoidaan kyberturvallisuuden häiriötilanteiden mahdollisista vaikutuksista. Kaiken kaikkiaan tästä yläteemasta raportoi 37 yritystä, mutta mainintojen lukumäärä jää vähäiseksi, keskimäärin 1,6 per yritys. Tämän perusteella voidaan siis olettaa, että vaikka tähän yläteemaan liittyvä raportointi on kohtalaisen yleistä, ei se sisällöltään ole kovin laajaa.

Teemakohtaisia tutkimustuloksia käsitellään tarkemmin tämän tutkielman luvuissa 4.2–4.8.

## 4.2 Kyberriskien tunnistaminen

Tutkimuksen tulosten perusteella taulukossa 10 on kuvattu, että kaiken kaikkiaan vain 43 yritystä (38 %) raportoi kyberriskien tunnistamisesta. Yleisintä raportointi oli, kun sillä viitattiin liiketoimintariskeihin, vähäisintä taas muissa kyberriskeihin liittyvissä konteksteissa.

Taulukko 10 Raportointi kyberriskien tunnistamisesta

| **Alateema** | **Yritysten lkm.** | **Mainintojen lkm.** | **Mainintojen ka per yritys** | **Vaihteluväli** |
|---|---|---|---|---|
| Keskeinen liiketoimintariski | 39 | 70 | 1,8 | 1–5 |
| Liiketoiminnan kulmakivi | 12 | 16 | 1,3 | 1–3 |
| Muut | 3 | 5 | 1,7 | 1–3 |
| *Yhteensä* | *43* | *91* | *2,1* | *1–7* |

Yrityksistä 39 (35 %) kertoi kyberturvallisuuden olevan keskeinen liiketoimintariski. Vaikka maininnat jäävät useimmiten melko yleistasoiseksi, kuten Mandatumin lainauksessa alla, avaavat jotkin yritykset lyhyesti myös riskien taustoja tai mahdollisia riskienhallintatoimenpiteitä, kuten Alma Median lainauksessa.

> *”Merkittävimpiä operatiivisten riskien itsearviointiprosessissa tunnistettuja riskejä ovat muun muassa seuraavat: tietoturvaan ja -suojaan liittyvät asiat, tietojärjestelmien vanheneminen sekä mahdolliset virheet paljon manuaalisia työvaiheita sisältävissä prosesseissa.” (Mandatum Oyj, Vuosikertomus 2022)*

> *”Operatiivisista riskeistä merkittävimmät ovat kyberriskit, tietotekniikan ja -liikenteen häiriöt sekä päivittäiseen uutistuotantoon liittyvät keskeytykset. Tietoturvariskejä hallitaan mm. parantamalla ennakoivaa automaatiota palvelinhyökkäysten havaitsemiseksi ajoissa ja kouluttamalla säännöllisesti henkilöstöä tietoturvaan ja tietosuojaan liittyen.” (Alma Media Oyj, Vuosikertomus 2022)*

Teemasta raportointi oli yleisintä rahoituspalveluiden toimialalla, jossa jopa 82 % yrityksistä raportoi kyberturvallisuuden olevan merkittävä riski liiketoiminnalle. Yleistä raportointi oli myös media-alan (75 % raportoi) ja tukku- ja vähittäiskaupan alan (56 % raportoi) yrityksistä. Sen sijaan kiinteistötoimialoilla ja muilla toimialoilla yritykset eivät raportoineet riskistä ollenkaan, ja myös perusteollisuuden alalla raportointi oli varsin vähäistä, kun vain 13 % yrityksistä raportoi teemasta.

Media-alalla myös 75 % yrityksistä raportoi kyberturvallisuuden olevan yksi liiketoiminnan kulmakivistä, mutta kaikilla muilla toimialoilla tämän teeman raportointi on vähäistä, ja vaihtelee 0–25 %:n välillä. Ne yritykset, jotka raportoivat teemasta, tekivät sen lähinnä toteamuksen muodossa, kuten Alma Media tai SRV Yhtiöt.

> *”Korkea tietoturva ja tietosuoja sekä datan vastuullinen käsittely ovat liiketoimintamme kulmakiviä.” (Alma Media Oyj, Vuosiraportti 2022)*

> *”Tietojärjestelmien toimivuus ja tietoturva ovat keskeisessä asemassa yrityksen liiketoiminnassa.” (SRV Yhtiöt Oyj, Vuosiraportti 2022)*

Muut kyberturvallisuusriskeihin liittyvät maininnat jäivät vähäiseksi, ja kaiken kaikkiaan vain kolme yritystä raportoi tällaisista. Muut-kategoriaan luokiteltiin tässä tutkimuksessa maininnat kyberturvallisuudesta osana yrityksen arvoja sekä kyberturvallisuus osana yrityksen keskeisiä tavoitteita.

Tämän yläteeman kohdalla tutkimustulokset eivät osoittaneet merkittäviä eroja yrityksen kokoluokan perusteella.

## 4.3 Kyberturvallisuuden häiriötilanteiden mahdolliset vaikutukset

Kyberturvallisuuden häiriötilanteiden mahdollisilla vaikutuksilla viitataan niihin yritykseen vaikuttaviin tekijöihin, jotka eivät ole toteutuneet, mutta voisivat olla mahdollisia

seurauksia jonkin kyberhäiriötilanteen seurauksena. Taulukossa 11 on esitetty raportoinnin alateemojen yleisyyttä tutkimuksen tulosten perusteella. Kaiken kaikkiaan 37 yritystä (33 %) yrityksistä raportoi joistakin mahdollisista vaikutuksista.

Taulukko 11 Raportointi kyberturvallisuuden häiriötilanteiden mahdollisista vaikutuksista

| Alateema | Yritysten lkm. | Mainintojen lkm. | Mainintojen ka per yritys | Vaihteluväli |
|---|---|---|---|---|
| Yleinen haitta toiminnalle | 14 | 18 | 1,3 | 1–2 |
| Mainehaitta | 12 | 15 | 1,3 | 1–3 |
| Taloudellinen haitta | 11 | 14 | 1,3 | 1–3 |
| Tietovuoto | 10 | 15 | 1,5 | 1–2 |
| Toiminnan keskeytyminen | 9 | 13 | 1,4 | 1–3 |
| Negatiivinen vaikutus tuotantoon | 3 | 3 | 1,0 | 1 |
| Järjestelmävahingot | 2 | 3 | 1,5 | 1–2 |
| Toimitusketjuhäiriöt | 2 | 2 | 1,0 | 1 |
| *Yhteensä* | *37* | *83* | *2,2* | *1–7* |

Yleisintä on mainita, että kyberturvallisuuden häiriötilanteista voi toteutuessaan aiheutua yleisesti haittaa yrityksen toiminnalle. Kuitenkin vain kahdeksan yritystä jättää maininnat pelkästään tälle tasolle, ja 29 yritystä raportoi tarkemmin kyberturvallisuuden häiriötilanteiden mahdollisista vaikutuksista. Mahdollisia vaikutuksia ei kuitenkaan ole yleistä analysoida syvällisesti, vaan niitä ilmoitetaan useimmiten luettelomuodossa. Esimerkiksi Kesko kertoo mahdollisista häiriötilanteiden seurauksista seuraavasti:

> *”Kyberhyökkäyksen seurauksia voivat olla liiketoiminnan keskeytyminen, asiakkaiden luottamuksen menettäminen tai viranomaisten määräämät sakot.” (Kesko Oyj, Vuosiraportti 2022)*

Tämän yläteeman kohdalla tutkimustulokset eivät osoittaneet merkittäviä eroja yrityksen toimialan tai kokoluokan perusteella.

## 4.4 Kyberturvallisuusstrategia

Tutkimuksen tulosten perusteella taulukossa 12 on esitetty, miten yritykset raportoivat kyberturvallisuusstrategiasta ja kyberturvallisuusasioihin liittyvästä yrityksen sisäisestä vastuunjaosta vuosiraportointikokonaisuuksissaan. Tutkimusten tulosten perusteella yhteensä 30 yritystä eli hieman yli neljännes (noin 27 %) raportoi teemasta. On huomattavaa, että mikäli yritys raportoi teemasta, on raportointi myös jokseenkin keskiarvoa (4,6)

laajempaa, sillä yritysten vuosiraporteissa esiintyi teemaan liittyviä mainintoja keskimäärin 5,7 kertaa.

Taulukko 12 Raportointi kyberturvallisuusstrategiasta

| Alateema | Yritysten lkm. | Mainintojen lkm. | Mainintojen ka per yritys | Vaihteluväli |
|---|---|---|---|---|
| Yleinen maininta kyberturvallisuusstrategiasta | 5 | 12 | 2,4 | 1–8 |
| Kyberturvallisuus sisältyy yhtiön strategisiin tavoitteisiin | 6 | 6 | 1,0 | 1 |
| Kyberturvallisuusjohtamisen malli | 5 | 15 | 3,0 | 1–8 |
| Kyberturvallisuuden toimielin | 20 | 73 | 3,7 | 1–13 |
| Vastuunjako & roolit | 18 | 65 | 3,6 | 1–17 |
| *Yhteensä* | *30* | *171* | *5,7* | *1–41* |

Itse kyberturvallisuusstrategiasta raportointi ei ollut kovin yleistä, vaan raportointi liittyi enemmän yrityksen sisäiseen kyberturvallisuuden vastuunjakoon, rooleihin ja toimielimiin. Ainoastaan viisi yritystä mainitsi joko suoraan tai epäsuorasti, että yrityksellä on olemassa kyberturvallisuusstrategia. Tämän lisäksi kuusi yritystä kertoi, että kyberturvallisuus kuuluu yrityksen keskeisiin strategisiin tavoitteisiin, ja viisi yritystä taas raportoi, että heillä on käytössään erityinen kyberturvallisuuden johtamismalli. Mainontojen yhteydessä usein kerrottiin, mihin kyberturvallisuusstrategialla tai tietoturvajohtamisella pyritään. Esimerkiksi Kamux kertoo strategiansa avulla pyrkivänsä häiriöiden estämiseen, Mandatum taas tietoisuuteen tietoturvan tilasta, sen kehityksen painoalueista sekä riittävien resurssien varmistamisesta.

> *”Kamuxin ja ulkopuolisten palveluntarjoajien liiketilat ja järjestelmät saattavat altistua riskeille liittyen luvattomaan käyttöön, väärinkäytöksiin, työntekijöiden virheisiin tai väärinkäytöksiin, tietokoneviruksiin, hakkereiden hyökkäyksiin tai muihin vastaaviin uhkiin. Häiriöt pyritään estämään yhtiön tietoturvastrategian mukaisin keinoin.” (Kamux Oyj, Vuosikertomus 2022)*

> *”Mandatum kehittää tietoturvaa ja kyberturvallisuutta systemaattisesti ja johdon hyväksymän tietoturvastrategian mukaisesti huomioiden jatkuvasti muuttuvan uhkaympäristön. Strategian ensisijaisena tavoitteena on varmistaa johdon tietoisuus tietoturvan tilasta, määritellä kehitystoimien painopisteet ja varmistaa niiden riittävä resursointi.” (Sampo Oyj, Riskienhallintaraportti 2022)*

Useat yritykset sen sijaan raportoivat siitä, millainen vastuunjako kyberturvallisuuden toteuttamiseen liittyy, sekä minkälaisia rooleja tai kyberturvallisuuden toimielimiä yrityksessä on. 20 yritystä kertoi vuosiraportointikokonaisuudessaan eri kyberturvallisuuden

toimielimistä tai työryhmistä, joita niillä on. Näitä toimielimiä olivat muun muassa kybervaliokunnat, kyberriskikomiteat, tietosuoja- ja tietoturvaorganisaatiot sekä tietoturvaryhmät tai -tiimit. Näihin toimielimiin liittyvä raportointi sisälsi keskimäärin 3,7 yrityskohtaista osumaa hakusanoille, ja raportoinnin yhteydessä kerrottiinkin lähes aina myös tarkemmin toimielinten tehtävistä, vaikkakin tehtäväkuvaukset eivät ole kovin spesifejä tai sisällä yritys- tai toimialakohtaisia tietoja. Esimerkiksi Ilkka ja Terveystalo kertovat toimielinten vastuista seuraavasti:

> *”Ilkka Oyj:n kehitys- ja tietohallinto-osasto toimii tietoturvan teknisenä asiantuntijaorganisaationa. Se ohjaa ja kehittää tietoturvan toteutumista konsernissa.” (Ilkka Oyj, Vuosikertomus 2022)*

> *”Lisäksi Terveystalossa toimii tietosuojan ja tietoturvan työryhmiä, jotka käsittelevät ja seuraavat tietosuojaan ja tietoturvaan liittyviä asioita sekä kehittävät tietosuoja- ja tietoturvatoimintaa.” (Terveystalo Oyj, Vuosikertomus 2023)*

Muutamat yritykset kertovat toiminnoista myös tarkemmalla tasolla, ja esimerkiksi Metso kertoo vuosiraportoinnissaan seuraavaa yrityksen kyberturvallisuustoiminnon vastuista:

> *”Kyberturvallisuustoiminnon päätavoitteena on suojata ja tukea yhtiön liiketoiminnan jatkuvuutta sekä yhtiön liikekumppaneita. Kyberturvallisuustoiminto tarjoaa reaaliaikaisen tilannekuvan asiaankuuluville sidosryhmille, ja toimintoa parannetaan sekä kehitetään jatkuvasti. – – Kyberturvallisuustoiminto johtaa ja toteuttaa strategian mukaisia sisäisiä tietoturva-auditointeja ja on mukana Metso Outotecin erilaisissa hyväksymisprosesseissa. Kaikista tietoturvapoikkeamista, tarkastushavainnoista ja korjaavia toimenpiteitä koskevista suosituksista raportoidaan säännöllisesti Metso Outotecin IT-johtoryhmälle, riskienhallintatoiminnolle sekä tarkastus- ja riskivaliokunnalle.” (Metso Oyj, Selvitys hallinto- ja ohjausjärjestelmästä 2022)*

Lähes yhtä yleistä oli myös raportoida muista yrityksen kyberturvallisuuteen liittyvistä rooleista tai vastuunjaosta. Tästä alateemasta raportoi yhteensä 18 yritystä, ja alateemasta myös kerrottiin lähes yhtä laajasti: noin teemaan liittyvää 3,6 mainintaa per yritys. Pääosin nämä maininnat pitävät sisällään tietoja siitä, kenelle on eskaloitu viime käden vastuu kyberturvallisuudesta tai esimerkiksi tietoturvallisuuden johtamisesta. Osa yrityksistä selvitti tarkemmin myös tietoturvallisuuden vastuiden ja toimintojen hierarkiaa. Lisäksi jotkut yritykset tarkensivat vastuullisten henkilöiden tehtäväkuvauksia samoin, kuin kyberturvallisuuden toimielinten vastuista raportoidessa. Esimerkiksi United Bankersin kohdalla tämä tarkoitti seuraavaa:

> *”Hallitus arvioi vuosittain tietosuojan ja -turvallisuuden tasoa ja riittävyyttä sekä hyväksyy näitä ohjaavat politiikat. United Bankers -konserniin on nimetty tietoturvapäällikkö ja tietosuojavastaava, jotka vastaavat osaltaan tietoturvallisuuden ja tietosuojan kehittämisestä, ohjaamisesta, seurannasta ja sitä koskevan ohjeistuksen ylläpitämisestä sekä johdon raportoinnista.” (United Bankers Oyj, Vuosi 2022)*

Myös kyberturvallisuusstrategian kohdalla raportointi oli yleisintä media-alalla, jossa 100 % yrityksistä raportoi teemasta, ja toiseksi yleisintä rahoituspalveluiden toimialalla, jossa noin 55 % yrityksistä raportoi teemasta. Sen sijaan kuluttajapalveluiden toimiala oli ainoa, jossa yksikään yritys ei raportoinut ollenkaan kyberturvallisuusstrategiasta tai siihen liittyvistä rooleista ja vastuista. Kokoluokan perusteella raportointi taas oli yleisintä suurilla yrityksillä, joista noin 44 % raportoi teemasta, kun taas keskisuurilla ja pienillä yrityksillä raportoivien yritysten osuus jäi noin 21 % paikkeille.

## 4.5 Kyberturvallisuustoimenpiteet

Taulukossa 13 esitetään tutkimusten tulosten perusteella, että kyberturvallisuuteen liittyvistä toimenpiteistä raportointi on vuosiraportoinnissa kaikkein yleisintä. Teemasta raportoi kaiken kaikkiaan 75 yritystä, eli noin 67 % yrityksistä. Tämän lisäksi niiden hakusanojen osumien kokonaismäärä, jotka liitettiin tähän kontekstiin, on noin 47 % kaikista osumista. Näin ollen voidaan siis todeta, että kyberturvallisuustoimenpiteistä raportointi on tämän tutkimuksen teemoista kaikkein yleisintä.

Taulukko 13 Raportointi kyberturvallisuustoimenpiteistä

| Alateema | Yritysten lkm. | Mainintojen lkm. | Mainintojen ka per yritys | Vaihteluväli |
|---|---|---|---|---|
| **Tarkentamattomat toimenpiteet** | | | | |
| Kyberturvallisuussitoumukset | 18 | 23 | 1,3 | 1–3 |
| Kyberturvallisuuden ylläpito | 8 | 13 | 1,6 | 1–4 |
| Kyberturvallisuuden jatkuva kehittäminen | 31 | 63 | 2,0 | 1–11 |
| **Hallinta, ohjeistus ja prosessit** | | | | |
| Yhtiötason ohjeistus tai politiikka | 35 | 132 | 3,8 | 1–31 |
| Kyberturvallisuuden hallintajärjestelmä | 9 | 18 | 2 | 1–6 |
| Prosessit ja käytännöt | 14 | 21 | 1,5 | 1–4 |
| **Seuranta** | | | | |
| Kyberturvallisuuden tason seuranta ja arviointi | 20 | 42 | 2,1 | 1–8 |

| | | | | |
|---|---|---|---|---|
| Riskien kartoittaminen, arviointi ja seuranta | 22 | 33 | 1,5 | 1–5 |
| Poikkeamien kartoittaminen | 5 | 7 | 1,4 | 1–3 |
| **Tekniset ratkaisut** | | | | |
| Kyberturvallisuustestaus | 2 | 9 | 4,5 | 2–7 |
| Muu tekninen toimenpide tai ratkaisu | 17 | 25 | 1,5 | 1–3 |
| **Operatiivinen toiminta** | | | | |
| Henkilöstön kouluttaminen | 38 | 125 | 3,3 | 1–23 |
| Kyberturvallisuushanke, -projekti tai -ohjelma | 9 | 22 | 2,4 | 1–6 |
| **Sertifioinnit** | | | | |
| Sertifiointi | 10 | 18 | 1,8 | 1–3 |
| Sertifiointien mukaisuus | 7 | 17 | 2,4 | 1–5 |
| **Auditointi** | | | | |
| Sisäinen auditointi | 18 | 29 | 1,6 | 1–4 |
| Ulkoinen auditointi | 6 | 6 | 1 | 1 |
| **Raportointi & viestintä** | | | | |
| Sisäinen raportointi | 8 | 15 | 1,9 | 1–7 |
| Ulkoinen raportointi & viestintä | 6 | 9 | 1,5 | 1–3 |
| **Muut toimenpiteet** | | | | |
| Taloudelliset investoinnit | 3 | 4 | 1,3 | 1–2 |
| Konsulttipalveluiden käyttö | 4 | 4 | 1 | 1 |
| Vaatimukset alihankkijoille tai toimitusketjulle | 8 | 15 | 1,9 | 1–3 |
| Vakuutukset | 5 | 5 | 1 | 1 |
| *Yhteensä* | *75* | *655* | *8,7* | *1–131* |

Tästä teemasta raportointi oli yleisintä media-alalla sekä muilla toimialoilla, joilla 100 % yrityksistä raportoivat teemasta. Myös tukku- ja vähittäiskaupan, teknologian ja perusteollisuuden toimialoilla raportointi oli yleisempää, ja vähintään 75 % näiden alojen yrityksistä raportoi tästä teemasta. On syytä huomata, että vaikka muilla toimialoilla 100 % yrityksistä raportoi tästä teemasta, raportoinnin laajuus jää näillä yrityksillä kovin pieneksi, ja teemaan linkitettäviä mainintoja on vain yksi jokaista yritystä kohden.

Yritysten kokoluokan perusteella suuret yritykset raportoivat kyberturvallisuuden toimenpiteistään eniten, pienet taas vähiten. Pienet ja keskisuuret yritykset kuitenkin keskittyvät kokonaisraportoinnissaan tähän teemaan keskimäärin enemmän kuin suuret

yritykset, ja pienten ja keskisuurten yritysten vuosiraportoinnista tähän teemaan sopivien mainintojen osuus on noin 8 % korkeampi kuin suurilla yrityksillä.

**Tarkentamattomat toimenpiteet** viittaavat sellaisiin mainintoihin, joita yritykset eivät tarkentaneet konkreettisilla yksityiskohdilla vuosiraporttien teksteissään. Yhteensä 18 yritystä kertoi raporteissaan toimenpiteidensä kautta sitoutuvansa kyberturvallisuuteen, ja nämä maininnat sisälsivät yleisiä lausuntoja kuten Keskisuomalaisen lainauksessa alla:

> *”Tietoturvasta huolehtiminen on Keskisuomalainen-konsernille merkittävä vastuullisuuden teema, jota seuraamme ja kehitämme jatkuvasti.” (Keskisuomalainen Oyj, Vuosikertomus 2022)*

Kahdeksan yritystä taas viittasi vuosiraporteissaan ylläpitävänsä tietoturvan nykytasoa, muttei tarkentanut tätä yksittäisillä konkreettisilla toimenpiteillä. Näin teki esimerkiksi Mandatum:

> *”Mandatum on varmistanut sekä hallinnollisin että teknisin toimenpitein, että konsernin tieto- ja kyberturvallisuus on kunnossa.” (Mandatum Oyj, Yritysvastuuraportti 2022)*

Lisäksi 31 yritystä kertoi panostavansa kyberturvallisuuden jatkuvaan kehittämiseen, muttei tämän maininnan yhteydessä kertonut konkreettisia toimenpiteitä, kuten Elecster:

> *”Viime vuoden aikana panostimme erityisen paljon tietoturvaan ja siihen on tarkoitus kiinnittää entistäkin enemmän huomiota tulevaisuudessa.” (Elecster Oyj, Vuosikertomus 2022)*

On kuitenkin syytä huomata, että vain kahdella yrityksellä kaikki maininnat kyberturvallisuustoimenpiteistä jäivät tälle tasolle, ja kaikki loput yritykset ovat tarkentaneet toimiaan konkreettisemmin myös jonkin muun alateeman tasolla.

**Hallinnalla, ohjeistuksella ja prosesseilla** tarkoitetaan tässä yhteydessä, että yrityksellä on yhtenäiset kyberturvallisuuden ohjeistukset ja käytänteet, joita sovelletaan läpi yrityksen sen eri tasoilla tai liiketoiminnoissa. 35 yritystä kertoo vuosiraporteissaan, että niillä on yhtiötason kyberturvallisuusohjeistus tai -politiikka. Käytännössä tämä voi tarkoittaa esimerkiksi sitä, että yrityksellä on selkeät yhteiset ohjenuorat, joihin sen kyberturvallisuuskäytännöt perustuvat. Yhtiötason ohjeistukseen tai politiikkaan liittyviä mainintoja esiintyi noin 3,8 kertaa per yritys, joten tästä teemasta raportoidaan keskimäärin laajemmin verrattuna kaikkiin kyberturvallisuustoimenpiteisiin, ja useimmat yritykset liittävätkin raportointiinsa myös keskeiset tavoitteet kyberturvallisuuspolitiikalle, kuten esimerkiksi Apetitin tai HKScanin lainauksissa alla:

> *”Apetit-konsernilla on säännöllisesti päivitettävät tietoturva- ja tietosuojapolitiikat hyvien tietojenkäsittelytapojen ja yksityisyydensuojan varmistamiseksi.” (Apetit Oyj, Vuosikertomus 2022)*

> *”Yhtiön tietoturvapolitiikassa asetetaan tavoitteet ja periaatteet ja määritellään tietoturvaan liittyvät vastuut.” (HKScan Oyj, Toimintakertomus ja tilinpäätös 2022)*

Yhteensä yhdeksän yritystä lisäksi kertoo, että niillä on käytössään kyberturvallisuuden hallintajärjestelmä. Nämä maininnat kuitenkin jäävät varsin yleistasoisiksi, joskin muutama yritys tarkentaa järjestelmän noudattavan ISO/IEC 27000 tai 27001 standardia.

14 yritystä taas avaa tietoturvallisuuteen liittyviä prosesseja tai käytäntöjä vuosiraportoinnissaan. Käytännössä nämä voivat tarkoittaa esimerkiksi yhtiötason ohjeistuksia siitä, miten kyberturvallisuuden häiriötilanteessa toimitaan. Vaikka prosesseista tai käytännöistä mainitaan keskimäärin vain 1,5 kertaa per yritys, useimmat yritykset kuitenkin avaavat myös näitä raporteissaan hieman tarkemmin, mutta keskittyvät tavoitteiden sijaan kertomaan prosesseista ja käytännöistä saatavia hyötyjä. Esimerkkinä Caverionin lainaus alla:

> *”Olemme laatineet tehokkaan ja kestävän tietoturvaprosessin, joka säästää aikaa, energiaa ja huomion tarvetta ja vähentää tietoturvariskejä.” (Caverion Oyj, Kestävän kehityksen raportti 2022)*

**Seuranta** viittaa niihin toimenpiteisiin, joita yritys tekee seuratakseen niin yleistä kyberturvallisuustilannetta kuin oman yhtiön kyberturvallisuuden nykytasoa. Yhteensä 20 yritystä kertoi seuraavansa ja arvioivansa oman yrityksen kyberturvallisuuden tasoa jatkuvasti. Nämä maininnat jäivät kuitenkin melko suppeiksi, ja yritykset lähinnä totesivat yhdellä lauseella, että kyberturvallisuutta seurataan jatkuvasti. Muutama yrityksistä kertoo työkaluikseen tähän esimerkiksi säännölliset kyberturvallisuus- tai haavoittuvuuskartoitukset.

Riskien kartoittamisesta, arvioinnista ja seurannasta raportoi taas 22 yritystä. Tällä tarkoitetaan yrityksen kohtaamien kyberturvallisuusriskien ja -uhkien jatkuvaa kartoittamista. Nämäkin maininnat jäävät osin suppeiksi, mutta useampi yritys kertoo samassa yhteydessä myös toimintatavoistaan hallita näitä riskejä, kuten Alma Media tai QPR Software:

> *”Alma Median liiketoimintaympäristö on jatkuvassa muutoksessa, ja tästä johtuen yhtiössä tarkastellaan säännöllisesti tietoturvallisuuteen vaikuttavia riskejä ja valmiuksia reagoida muuttuvan ympäristön riskeihin. Tietoturvaa*

> *ja tietosuojaa vahvistetaan kulloinkin tarpeen mukaan riskien pienentämiseksi.” (Alma Media Oyj, Vuosikertomus 2022)*

> *”QPR Software tarkkailee ja pyrkii minimoimaan säännöllisesti tietoturvariskejä operatiivisella tasolla sekä raportoimalla yhtiön hallitukselle. – – Tietoturvariskien vähentämiseksi olemme ottaneet käyttöön tieto- ja toimittajahallintamalleja, suorittaneet kumppaneille vuosittaisia tarkastuksia, sekä järjestäneet asianmukaisia sisäisiä koulutuksia tietoturvallisuustietoisuuden parantamiseksi.” (QPR Software Oyj, Vuosikertomus 2022)*

Lisäksi viisi yritystä kertoo, että niillä on vakiintuneet toimintatavat tietoturvapoikkeamien kartoittamiseen. Näitä toimintatapoja ei kuitenkaan avata, vaan vuosiraporteissa lähinnä todetaan niiden olemassaolo.

**Tekniset ratkaisut** tarkoittavat sellaisia teknisiä toimenpiteitä, joilla varmistetaan tietojärjestelmien ja yrityksen digitaalisen ympäristön turvallisuus ja toimivuus. Kaksi yritystä kertoo säännöllisten kyberturvallisuustestausten olevan tärkeä keino kyberturvallisuuden ylläpidossa ja kehittämisessä. Nämä yritykset myös kertovat avoimemmin, mitä tämä testaus käytännössä tarkoittaa. Esimerkiksi Sampo kertoo vuosiraportoinnissaan ensin Ifin ja tämän jälkeen Hastingsin testauskäytännöistä seuraavaa:

> *”Uusien ratkaisujen käyttöönottoon ja kriittisten sovellusten tai järjestelmien muutoksiin liittyvään muutoksenhallintaan sisältyy riippumattoman sisäisen asiantuntijaryhmän suorittama, riskiperusteista lähestymistapaa noudattava tietoturvatestaus. Erikoistuneet kolmannen osapuolen tietoturvatestaajat tekevät myös säännöllisesti sovellusten ja IT-infrastruktuurin tietoturvatestejä.” (Sampo Oyj, Vastuullisuusraportti 2022)*

> *”Riippumattomat toimijat validoivat ja testaavat toimintatavat säännöllisesti. Testauksen suorittavat yhtiön CBEST-sertifioidut kumppanit, ja se sisältää haavoittuvuusarviointeja ja tunkeutumistestejä sekä sisäisesti toteutettuja tietojenkalastelukampanjoita ja harjoituksia, joilla tarkastetaan poikkeamien hallintamenettelyjen sietokyky ja kestävyys.” (Sampo Oyj, Vastuullisuusraportti 2022)*

Lisäksi 17 yritystä raportoi käytössään olevan vaihtelevia muita teknisiä toimenpiteitä, joilla kyberturvallisuudesta huolehditaan. Näihin lukeutuvat esimerkiksi palomuurien ja virustorjuntaohjelmien käyttö, automaation ja koneoppimisen hyödyntäminen, tietoturvatapahtumien automaattinen monitorointi, identiteetin- ja pääsynhallinnan eri käytännöt, järjestelmien keskittäminen ja modernisointi sekä erityinen tietoturvallisuusarkkitehtuuri. Näistä teknisistä toimenpiteistä kerrotaan usein luettelomuodossa, kuten esimerkiksi Keskon lainauksessa alla, eikä toimenpiteitä juurikaan avata tarkemmin.

> *”Keskolla on vahva, useita suojauskerroksia käsittävä tietoturva-arkkitehtuuri. Järjestelmät ja tietoliikenneyhteydet on tärkeysluokiteltu. Järjestelmillä on palautumissuunnitelmat, joita testataan ja harjoitellaan säännöllisesti. Käytetty kyberturvateknologia hyödyntää automaatiota ja koneoppimista, mikä mahdollistaa uhkien erittäin nopean havaitsemisen ja vastatoimien käynnistämisen.” (Kesko Oyj, Vuosiraportti 2022)*

**Operatiivisen toiminnan** toimenpiteet pitävät tässä tutkimuksessa sisällään henkilöstön kouluttamiseen sekä erilaiset kyberturvallisuuden hankkeet ja projektit. Henkilöstön kouluttaminen oli yleisin alateema kaikista kyberturvallisuuden toimenpiteistä, ja yhteensä 38 yritystä, eli noin 34 % yrityksistä kertoo vuosiraporteissaan tarjoavansa henkilöstölleen koulutusta kyberturvallisuusasioihin liittyen. Teemaan liittyviä mainintoja löytyi myös keskimäärin 3,3 kpl per yritys, mutta tästä huolimatta raportointi jää hyvin pinnalliselle tasolle. Suurin osa yrityksistä yksinkertaisesti toteaa kouluttavansa henkilöstöä tietoturva-asioista, kuten esimerkiksi Eezyn lainauksessa alla. Jotkut yritykset esimerkiksi esittelevät lukuja siitä, miten suuri osa henkilöstöstä on suorittanut koulutuksen, tai millä alustalla koulutukset toteutetaan. Kuitenkin vain murto-osa yrityksistä tarkentaa, mitä teemoja koulutukset sisältävät tai mitä asioita niissä käsitellään, kuten esimerkiksi Sampo tekee.

> *”Tietosuojakoulutus on osa perehdytysohjelmaamme ja koulutamme säännöllisin väliajoin toimihenkilöitämme tietosuojakäytänteisiin.” (Eezy Oyj, Toimintakertomus ja tilinpäätös 2022)*

> *”If järjestää kaikille uusille työntekijöille ja alihankkijoille tietoturva- ja kyberturvallisuuskoulutusta, jota täydennetään vuosittain verkkokoulutuksella, lähiopetuksella ja intranet-artikkeleilla. Koulutuksen aiheita ovat esimerkiksi tietoturvavaatimukset, -roolit ja -vastuut, ajankohtaiset tietoturvariskit ja tietoturvapoikkeamista ilmoittaminen. ” (Sampo Oyj, Vastuullisuusraportti 2022)*

Lisäksi yhdeksän yritystä kertoo, että niillä on kuluneen tilikauden aikana joko käynnissä, suunnitteilla tai päättynyt jokin kyberturvallisuuden hanke, projekti tai muu ohjelma. Lähes kaikki avasivat hankkeidensa tavoitteita, jotka poikkeuksetta olivat kaikilla kyberturvallisuuden nykytilan parantaminen tai vahvistaminen. Tarkempia hankkeiden sisältöjä ei kuitenkaan avattu.

**Sertifioinneilla** viitataan tässä yhteydessä yritysten hankkimiin kyberturvallisuussertifikaatteihin tai niiden mukaiseen toimintaan. Yhteensä kymmenen yritystä kertoo, että niillä on jokin kyberturvallisuuden sertifikaatti tai standardisointi. Sertifioinnista mainittiin joko siinä yhteydessä, että yritys oli saanut sen kuluvan tilikauden aikana (esimerkiksi

Sitowise Group), tai siten, että sen avulla vakuutettiin tietoturvallisuuden olevan hyvällä tasolla (esimerkiksi Caverion). On myös pantava merkille, että ainoastaan ISO-sertifikaatit tarkennettiin nimeltä, ja muita sertifikaatteja tai standardointeja ei erikseen eritelty, kuten esimerkiksi Wärtsilän vuosikertomuksesta ilmenee.

> *”Sitowiselle myönnettiin vuonna 2022 myös ISO 27001 tietoturvasertifikaatti tietoturvallisuuden hallintajärjestelmästä.” (Sitowise Group Oyj, Toimintakertomus ja konsernitilinpäätös 2022)*

> *”Meillä on ISO/IEC 27001 -tietoturvasertifikaatti osoituksena siitä, että johdamme tietoturvaa järjestelmällisellä tavalla.” (Caverion Oyj, Kestävän kehityksen raportti 2022)*

> *”On hyvä huomata, että Wärtsilällä on lukuisia kyberturvallisuussertifiointeja ja että yhtiö pyrkii jatkuvasti yhtenäistämään prosessiensa, tuotteidensa ja ratkaisujensa kyberturvallisuutta kansainvälisten standardien kanssa sekä saamaan lisää sertifiointeja.” (Wärtsilä Oyj Abp, Vuosikertomus 2023)*

Lisäksi seitsemän yritystä ei suoranaisesti kerro, että niillä olisi jokin kyberturvallisuussertifikaatti tai -standardointi, mutta ne pyrkivät aktiivisesti kertomaan toimivansa näiden viitekehysten mukaisesti ja perustavansa esimerkiksi kyberturvallisuuden hallintamallinsa tai tietoturvapolitiikkansa ISO 27001 -standardiin.

**Auditoinnilla** viitataan tässä tutkimuksessa joko sisäiseen kyberturvallisuuden omatarkkailuun tai ulkoisen toimijan tekemään tarkastukseen kyberturvallisuuden tasosta. Sisäisiä auditointeja kertoi suorittavansa yhteensä 19 yritystä. Yksikään yritys ei kuitenkaan tarkemmin kerro, mitä nämä sisäiset tarkastukset tai muut omavalvontatoimenpiteet pitivät sisällään, tai millaisia niiden tulokset olivat. Lisäksi kuusi yritystä kertoo vuosiraporteissaan, että niille on tehty jokin kyberturvallisuusauditointi ulkopuolisen arvioijan tai asiantuntijan toimesta. Myös nämä maininnat jäävät pintapuolisiksi, eikä auditointien tarkempia kohteita tai tuloksia ole avattu vuosiraportoinnissa.

**Raportoinnilla ja viestinnällä** viitataan niihin toimenpiteisiin ja käytäntöihin, joilla yritykset raportoivat ja tiedottavat kyberturvallisuuden tilasta tai kyberturvallisuustapahtumista niin yrityksen sisällä, kuin myös viranomaisille ja ulkopuolisille sidosryhmille. Yhteensä kahdeksan yritystä kertoo vuosiraportoinnissaan sisäisistä raportoinnin ja viestinnän toimenpiteistä. Suurin osa näistä yrityksistä kertoo, että yrityksellä on vakiintuneet toimintatavat siihen, miten henkilöstö raportoi esimerkiksi havaitsemistaan kyberturvallisuustapahtumista eteenpäin, tai miten kyberturvallisuudesta raportoidaan yrityksen

hallitukselle. Esimerkiksi Pihlajalinna ja Keskisuomalainen kertovat raportoinnista ja viestinnästä vuosiraporteissaan seuraavaa:

> *”Kaikissa Pihlajalinnan toimipisteissä on käytössä raportointijärjestelmä, jolla henkilökunta ilmoittaa havaituista tietosuoja- ja tietoturvapoikkeamista.” (Pihlajalinna Oyj, Vuosiraportti 2022)*

> *”Tietoturvatilanteesta ja siihen liittyvistä kehitystoimista raportoidaan Keskisuomalainen Oyj:n johtoryhmälle kerran kvartaalissa.” (Keskisuomalainen Oyj, Vuosikertomus 2022)*

Kuusi yritystä kertoo vuosiraportoinnissaan myös, että niillä on vakiintuneet käytännöt ulkoiseen raportointiin ja viestintään joko viranomaisille, asiakkaille tai muille sidosryhmille. Nämä ovat kuitenkin hyvin yleisluontoisia mainintoja, eikä käytäntöjä tai prosesseja juurikaan avata. Esimerkiksi Kesko kertoo ulkoisesta raportoinnista seuraavasti:

> *”Kesko dokumentoi kaikki tietoturvaloukkaukset ja tekee tietoturvaloukkauksista ilmoitukset tietosuojaviranomaiselle, mikäli tapahtumasta aiheutuu rekisterinpitäjän käsityksen mukaan riski rekisteröidyille. Kesko ilmoittaa tietoturvaloukkauksesta viipymättä myös henkilölle, jonka henkilötietojen suoja on vaarantunut, tietosuoja-asetuksen edellyttämissä korkean väärinkäytös- tai vahinkoriskin tilanteissa.” (Kesko Oyj, Vuosiraportti 2022)*

**Muut toimenpiteet** pitävät sisällään ne toimenpiteet, joita ei järkevästi voitu luokitella muihin kategorioihin. Tässä tapauksessa ne tarkoittavat taloudellisia investointeja, konsulttipalveluiden käyttöä, kyberturvallisuusvaatimuksia alihankkijoille tai toimitusketjulle tai kyberturvallisuusvakuutuksia.

Kolme yritystä kertoo vuosiraportoinneissaan erikseen tehneensä taloudellisia investointeja kyberturvallisuuteen. Investointien tarkempia kohteita ei kuitenkaan avattu raporteissa. Neljä yritystä taas kertoo käyttävänsä ulkopuolisia konsultteja tai asiantuntijoita kyberturvallisuuden kehittämiseen. Myöskään tämän teeman yhteydessä ei avattu tarkemmin, mihin tarkoitukseen kyberturvallisuuden konsulttipalveluita on ostettu.

Yhteensä kahdeksan yritystä kertoo asettavansa alihankkijoilleen tai toimitusketjulleen vaatimuksia kyberturvallisuuteen liittyen. Käytännössä tämä tarkoittaa, että yritykset odottavat alihankkijoidensa tai toimitusketjun eri osapuolien kyberturvallisuuden olevan riittävän korkealla tasolla, tai että niiden on noudatettava samoja kyberturvallisuuskäytäntöjä kuin yrityksellä on itsellään käytössä. Esimerkiksi Glaston kuvailee vuosikertomuksessaan tätä yksinkertaisesti seuraavan lainauksen mukaisesti:

*”Myös Glastonin kumppaneiden ja alihankkijoiden edellytetään noudattavan yhtiön tietoturvaan liittyviä ohjeita.” (Glaston Oyj Abp, Vuosikatsaus 2022)*

Lisäksi viisi yritystä kertoo vuosiraportoinnissaan ottaneensa erillisen vakuutuksen kyberturvallisuustapahtumia varten, tai että yrityksen vakuutusturvassa on otettu myös kyberturvallisuus huomioon. Nämä maininnat ovat lähinnä toteamuksia, eikä niitä avata tarkemmin.

## 4.6 Kyberturvallisuusuhat ja mahdolliset häiriötilanteet

Taulukossa 14 on esitetty tutkimuksen tulosten perusteella, että kaiken kaikkiaan 36 aineiston yritystä, eli noin 32 % yrityksistä kertoo vuosiraporteissaan kyberturvallisuusuhista sekä mahdollisista kyberturvallisuuden häiriötilanteista.

Taulukko 14 Raportointi kyberturvallisuusuhista ja mahdollisista häiriötilanteista

| Alateema | Yritysten lkm. | Mainintojen lkm. | Mainintojen ka per yritys | Vaihteluväli |
|---|---|---|---|---|
| Kyberhyökkäyksien uhka - yleinen maininta | 24 | 35 | 1,5 | 1–3 |
| Kyberhyökkäyksien uhka - geopolitiikka | 6 | 8 | 1,3 | 1–3 |
| Kyberhyökkäyksien uhka - Venäjän hyökkäys Ukrainaan 2022 | 10 | 20 | 2,0 | 1–4 |
| Hyökkäyksien potentiaaliset kohteet | 7 | 9 | 1,3 | 1–2 |
| Hyökkäyksien mahdolliset syyt | 6 | 6 | 1,0 | 1 |
| *Yhteensä* | *36* | *78* | *2,2* | *1–8* |

Tavanomaisinta on yksinkertaisesti todeta, että kyberhyökkäyksien tai muiden kyberturvallisuuden häiriötilanteiden uhka on olemassa, tai että se on kasvussa. Näin tekee yhteensä 24 yritystä. Tämän lisäksi kuusi yritystä tarkentaa lausuntoaan liittämällä uhat nykyiseen geopoliittiseen tilanteeseen, ja kymmenen yritystä taas liittää kyberuhkien nykytilan tai kasvaneen tilanteen Venäjän hyökkäykseen Ukrainaan vuonna 2022.

*”Kaikessa Evlin toiminnassa keskiössä ovat tietojärjestelmät, joihin liittyy tietosuoja- ja tietoturvariskejä.” (Evli Oyj, Vuosikertomus 2023)*

*”Kyberturvallisuudesta on tullut nykyisessä geopoliittisessa tilanteessa tärkeämpää kuin koskaan aikaisemmin. Verkottuneessa maailmassa mahdolliset hyökkäykset ja seurannaisvaikutukset voivat vaikuttaa myös UPM:n liiketoimintaan.” (UPM Kymmene Oyj, Vuosikertomus 2022)*

*”Venäjän hyökkäyssota Ukrainaan on kasvattanut myös kyberhyökkäysten todennäköisyyttä.” (Pihlajalinna Oyj, Vuosiraportti 2022)*

Yleistason mainintojen lisäksi osa yrityksistä raportoi myös tarkemmin uhkien potentiaalisista kohteista tai mahdollisista syistä. Raportointi on hieman yksityiskohtaisemmalla tasolla, vaikkeivat tiedot kuitenkaan ole yrityskohtaisia, vaan pätevät yleensä kaikkeen yritystoimintaan tai ovat tyypillisiä tietylle toimialalle. Potentiaalisina kohteina yritykset mainitsevat muun muassa kriittiset liiketoiminnan IT-järjestelmät, infrastruktuurin, verkkopalvelut ja yhteistyökumppaneiden tarjoamat IT-järjestelmät ja tietoliikenneyhteydet. Mahdollisiksi syiksi taas raportoidaan muun muassa arkaluontoisen tiedon suuri määrä, ongelmat käyttöoikeuksien hallinnassa, puutteellinen elinkaaren hallinta, sekä työntekijöiden virheet tai väärinkäytökset.

Kaikkein yleisintä kyberturvallisuusuhista raportointi oli mediatoimialalla, jossa 100 % yrityksistä raportoi teemasta. Kiinteistötoimialalla yksikään yritys ei taas raportoinut kyberturvallisuusuhista tai mahdollisista kyberturvallisuuden häiriötilanteista ollenkaan. Muiden toimialojen raportoinnin yleisyys pysyi tämän teeman kohdalla melko alhaisena ja vaihteli 13–50 %:n välillä keskiarvon ollessa 33 %. Kokoluokan perusteella tämän teeman raportoinneissa ei ollut eroja, vaan raportoinnin yleisyys pysyi suurin piirtein samalla tasolla yrityksen kokoluokasta huolimatta.

## 4.7 Kohdatut kyberturvallisuuden häiriötilanteet

Kohdatuilla kyberturvallisuuden häiriötilanteilla viitataan kyberhäiriöihin, kyberhyökkäyksiin ja tietoturvaloukkauksiin, joiden kohteeksi yritys on kuluneen tilikauden aikana joutunut. Taulukossa 15 esitetty tutkimustulosten perusteella näistä häiriötilanteista raportointia osana yritysten vuosiraportoinnin kokonaisuutta. Yhteensä vain 14 yritystä ottaa vuosiraportissaan kantaa kohdattuihin häiriötilanteisiin tai niiden puutteeseen, mikä tarkoittaa noin 13 %:a yrityksistä.

Taulukko 15 Raportointi kohdatuista kyberturvallisuuden häiriötilanteista

| Alateema | Yritysten lkm. | Mainintojen lkm. | Mainintojen ka per yritys | Vaihteluväli |
|---|---|---|---|---|
| Joutunut häiriötilanteen kohteeksi | 3 | 9 | 3 | 1–5 |
| Ei merkittäviä häiriötilanteita | 5 | 12 | 2,4 | 1–3 |
| Ei häiriötilanteita | 3 | 3 | 1,0 | 1 |
| Häiriötilanteiden lukumäärä kerrottu | 8 | 21 | 2,6 | 1–8 |

| | | | | |
|---|---|---|---|---|
| Muut maininnat | 5 | 27 | 5,4 | 1–20 |
| *Yhteensä* | *14* | *72* | *5,1* | *1–25* |

Yleisintä oli raportoida häiriötilanteiden lukumäärästä, josta raportoi kahdeksan yritystä. Harvinaisinta taas oli kertoa joutuneensa hyökkäyksen kohteeksi, josta suoraan kertoi vain kolme yritystä. Kaiken kaikkiaan kahdeksan yritystä taas raportoi kaikkien kokemiensa kyberturvallisuuden häiriötilanteiden tarkan määrän, osa yhtenä kokonaisuutena, osa taas yksityiskohtaisemmin. Lisäksi kolme yritystä korostaa erikseen vuosiraporteissaan, etteivät ne ole kokeneet kuluneen tilikauden aikana ollenkaan kyberturvallisuuden häiriötilanteita. Tämän lisäksi viisi yritystä kertoo, etteivät ne ole kokeneet merkittäviä häiriötilanteita. Muut maininnat pitävät sisällään muun muassa yrityksen sisäisiä tai ulkoisia raportointikäytäntöjä, joita kyberturvallisuuden häiriötilanteiden kohdalla on käytetty, sekä häiriötilanteen seurauksista ja palautumisesta raportointia.

Tästä yläteemasta raportointi oli keskimäärin kovin pinnallisella tasolla, eikä koettuja häiriötilanteita tai niiden puutetta ole avattu yksityiskohtaisesti. Poikkeuksiakin kuitenkin oli: merkittävimmin kokonaisuudessaan koetuista häiriötilanteista raportoi Uponor, jonka vuosiraportoinnissa esiintyy häiriötilanteisiin liittyviä hakusanoja yhteensä 25 kertaa. Yritys kertoo vuosikatsauksessaan lyhyen yhteenvedon kautta, mitä vaikutuksia siihen kohdistuneella kyberhyökkäyksellä on ollut, ja miten se palautui hyökkäyksestä.

> *”Vuoden viimeisellä neljänneksellä liikevaihtomme laski 16 prosenttia vertailukaudesta Uponoriin 5. marraskuuta kohdistuneen kyberhyökkäyksen johdosta. Hyökkäyksen jälkeen yhtiö teki välittömät toimet tilanteen selvittämiseksi ja korjaamiseksi. Yksi näistä toimista oli kaikkien järjestelmien ja tuotannon sulkeminen varotoimenpiteenä. Viikon kestäneen tuotantokatkoksen jälkeen tuotantotasot alkoivat palautua ja olivat normaalilla tasolla joulukuun alusta alkaen.” (Uponor Oyj, Vuosikatsaus 2022)*

Tämän yläteeman kohdalla tutkimustulokset eivät osoittaneet merkittäviä eroja yrityksen toimialan tai kokoluokan perusteella.

## 4.8 Muut kyberturvallisuusasiat

Edellä esiteltyjen teemojen lisäksi aineiston yritysten raportoinnista löytyi myös muita kokonaisuuksia, joista raportoitiin. Tutkimuksen tulosten perusteella taulukossa 16 esitetään raportointi muiden kyberturvallisuusasioiden osalta, jotka on jaettu viiteen alateemaan: lainsäädäntö, kestävä kehitys ja vastuullisuus, tietoturvalliset tuotteet ja palvelut,

yhteiskunnan hyväksi toimiminen sekä muut maininnat. Yhteensä 20 yritystä eli noin 18 % raportoi muista kyberturvallisuusasioista.

Taulukko 16 Raportointi muista kyberturvallisuusasioista

| Alateema | Yritysten lkm. | Mainintojen lkm. | Mainintojen ka per yritys | Vaihteluväli |
|---|---|---|---|---|
| Lainsäädäntö | 11 | 17 | 1,5 | 1–4 |
| Kestävä kehitys ja vastuullisuus | 9 | 14 | 1,6 | 1–4 |
| Tietoturvalliset tuotteet ja palvelut | 5 | 11 | 2,2 | 1–4 |
| Yhteiskunnan hyväksi toimiminen | 3 | 11 | 3,7 | 1–9 |
| Muut maininnat | 2 | 3 | 1,5 | 1–2 |
| *Yhteensä* | *20* | *56* | *2,8* | *1–15* |

Lainsäädännön alateemasta raportointi tarkoitti pääasiallisesti, että yritys kertoi noudattavansa kulloinkin voimassa olevia lakeja ja säädöksiä tietosuoja- ja tietoturva-asioissa. Yksi yritys myös kertoi aktiivisesti seuraavansa sääntelyn muutoksia tietosuojaa ja tietoturvaa koskien.

Yhdeksän yritystä kytkee vastuullisuuden ja kestävän kehityksen tietoturvateemoihin vuosiraporteissaan. Nämä yritykset käsittelevät esimerkiksi kyberturvallisuuteen liittyviä ympäristövaikutuksia, ihmisoikeus- ja tasa-arvokysymyksiä ja toisaalta myös kyberturvallisuutta osana kestävää ja taloudellisesti vastuullista liiketoimintaa. Esimerkiksi Sampo kertoo vuosiraportissaan konsernin tytäryhtiön Hastingsin työstä sukupuolten välisen tasa-arvon edistämiseksi kyberturvallisuusalalla muun muassa seuraavasti:

> *”Hastings tuki vuonna 2022 kyberturvallisuuden parissa työskentelevien naisten maailmanlaajuista The Source -yhteisöä. – – Yhteisön visiona on tehdä naisista kyberturvallisuuden alalla sääntö eikä poikkeus. Hastings pyrkii yhdessä The Sourcen kanssa tekemään kyberturvallisuuden työtehtävistä naisille kiinnostavampia ja helpommin lähestyttäviä sekä Hastingsissa että koko toimialalla.” (Sampo Oyj, Vastuullisuusraportti 2022)*

Lisäksi viisi yritystä mainitsi osana vuosiraportointikokonaisuuttaan yrityksen tuotteiden tai palvelujen olevan kyberturvallisia. Esimerkiksi Alma Media kertoo tietoturvallisten palvelujen vaikuttavan suoraan yrityksen asiakastyytyväisyyteen, sekä tarkentaa, miten heillä tästä on huolehdittu:

> *”Merkittävä asiakastyytyväisyyteen vaikuttava psykologinen tekijä on luottamus palvelun toimivuuteen ja tietoturvallinen asiointi. Medioidemme ja palveluidemme yhteinen käyttäjätunnus Alma-tunnus mahdollistaa sujuvan*

> *ja turvallisen siirtymisen palvelusta toiseen Alman digitaalisessa verkostossa." (Alma Media Oyj, Vuosikertomus 2022)*

Alateema yhteiskunnan hyväksi toimiminen pitää sisällään yritysten maininnat siitä, millä tavoin ne ovat kyberturvallisuuden kautta luoneet lisäarvoa yhteiskunnalle, esimerkiksi tekemällä yhteistyötä viranomaisten kanssa. Tästä teemasta kerrotaan melko laajasti, ja tähän kontekstiin liittyviä hakusanoja esiintyykin keskimäärin 3,7 kpl jokaista teemasta raportoivaa yritystä kohden.

Tämän yläteeman kohdalla tutkimustulokset eivät osoittaneet merkittäviä eroja yrityksen toimialan tai kokoluokan perusteella.

# 5 Johtopäätökset

## 5.1 Raportoinnin yleisyys, laajuus ja keskeiset sisällöt

Kun yritysten kohtaamat kyberuhat ja -hyökkäykset yleistyvät, myös sidosryhmien odotukset yritysten kyberturvallisuustoimia ja niiden läpinäkyvyyttä kohtaan kasvavat. Kyberturvallisuus ei nykyään enää tarkoitakaan pelkkää tietojen suojaamista vaan se kattaa myös yrityksen riskienhallinnan, taloudellisen tilanteen sekä markkina-aseman kehittämisen. Näin ollen myös kyberturvallisuustoimenpiteistä raportoimisen merkitys korostuu. Yrityksille voi olla strategisesti tärkeää viestiä ja raportoida kyberturvallisuustoimistaan, mikä lisää sidosryhmien luottamusta ja vahvistaa yrityksen asemaa markkinoilla.

Tämän tutkimuksen tarkoituksena oli tarkastella kyberturvallisuusraportoinnin nykytilaa Suomessa ja luoda poikkileikkaava kuva kyberturvallisuusasioiden raportoinnista osana yritysten vuosiraportointia. Tutkimus tehtiin sisällönanalyysinä, ja aineisto koostui 112 suomalaisen pörssiyrityksen vuosiraporteista. Raportit käytiin läpi hakusanojen kautta, jonka jälkeen jokainen osuma liitettiin manuaalisesti johonkin seitsemästä eri yläteemasta ja edelleen 54:stä eri alateemasta hakusanaa ympäröivän kontekstin avulla. Teemat muodostettiin mukaillen Hérouxin & Fortinin (2020) viitekehystä.

Tutkimuksen tulosten perusteella noin 86 % aineiston yrityksistä raportoi jollain tasolla kyberturvallisuudesta, ja vain noin 14 % ei raportoi aiheesta ollenkaan. Näin ollen voidaan todeta, että reilu enemmistö suomalaisista pörssiyhtiöistä viittaa kyberturvallisuuteen vuosiraporteissaan, ja kyberturvallisuudesta raportointi edes jollakin tasolla on siis melko yleistä. Tämä on linjassa aiemman tutkimuksen kanssa, jonka mukaan kyberturvallisuudesta raportoivien yritysten osuus vaihtelee noin 84–87 %:n välillä. Viitekehyksenä sovelletun Hérouxin & Fortinin (2020) tutkimuksessa raportoivien yritysten osuus oli 87 % aineiston yrityksistä.

Raportoinnin laajuutta taas tutkittiin hakusanojen osumien määrällä per yritys, ja tutkimustulosten perusteella yrityksillä oli vuosiraporteissaan keskimäärin noin 12,2 kyberturvallisuuteen liittyvää mainintaa. Kun otetaan huomioon, että erinäisiä alateemoja, joiden perusteella hakusanoja luokiteltiin, oli tutkimuksessa 54, kattaisi tämä 12,2 mainintaa esimerkiksi vain noin 23 % eri teemoista. Näin ollen voidaan todeta, että raportointi on kuitenkin melko suppealla ja yksinkertaisella tasolla, eikä voi sisältää kovin

yksityiskohtaisia tietoja yritysten kyberturvallisuuskäytännöistä. Myös tämä on linjassa aiemman tutkimuksen kanssa.

Se, että raportointi on melko suppeaa, voi selittyä esimerkiksi yritysten strategisten valintojen kautta. Yritykset eivät välttämättä halua kertoa tarkkoja kyberturvallisuustoimenpiteitään tai -käytäntöjään, sillä liian yksityiskohtainen raportointi saattaa pahimmassa tapauksessa paljastaa kyberrikollisille tiettyjä yrityksen heikkouksia tai haavoittuvuuksia, ja altistaa niitä näin ollen kyberhyökkäysten kohteiksi. Vahvaa kyberturvallisuutta voidaan myös pitää yrityksen kilpailuetuna, johon liittyviä tarkkoja tietoja ei näin ollen haluta jakaa julkisesti. Valittujen teemojen osalta kyberturvallisuusraportointia voidaan laajentaa tai tarkentaa. Tavoitteena voi olla esimerkiksi sidosryhmien luottamuksen saavuttaminen avoimuuden kautta, sillä liian suppea raportointi voi viestiä puutteellisesta läpinäkyvyydestä tai huonosta kyberturvallisuuden tasosta.

Tämän tutkimuksen tulosten perusteella kaikkein yleisintä raportointi oli varsinaisista kyberturvallisuustoimenpiteistä, josta raportoi yhteensä noin 66 % aineiston yrityksistä, toiseksi yleisintä kyberturvallisuusriskeistä, josta raportoi noin 38 % aineiston yrityksistä, ja harvinaisinta taas kohdatuista kyberturvallisuuden häiriötilanteista, josta raportoi yhteensä vain noin 13 % aineiston yrityksistä. Tulokset ovat linjassa Hérouxin & Fortinin (2020) kanssa: samat teemat pitävät viitekehyksen tutkimuksessa ensimmäistä ja toista sijaa, joskin eniten raportoidaan kyberturvallisuusriskeistä ja toiseksi eniten kyberturvallisuustoimenpiteistä. Viitekehyksen perusteella myös harvinaisimmin raportoitu teema on sama: kohdatut kyberturvallisuuden häiriötilanteet.

Tiettyjen teemojen yleisyys tai harvinaisuus raportoinnissa voi johtua useista eri syistä. Kyberturvallisuustoimenpiteistä raportoinnin yleisyys voi selittyä esimerkiksi sillä, että toimenpiteet ovat usein konkreettisia, ja näin ollen lukijalle helpompia käsittää. Yrityksillä voi myös olla halu osoittaa, että ne ovat proaktiivisia ja sitoutuneita suojaamaan tietojaan ja järjestelmiään. Raportointi konkreettisista toimenpiteistä voi näin ollen parantaa yrityksen mainetta ja lisätä sidosryhmien luottamusta. Lisäksi tietojen saatavuus ja raportoinnin helppous voivat olla myös merkittäviä tekijöitä. Kyberturvallisuustoimenpiteet voivat useissa yrityksissä olla hyvin dokumentoituja ja seurattuja, mikä tekee myös niiden raportoimisesta helpompaa. Myös kyberturvallisuusriskeistä raportointi voi selittyä samoilla syillä: raportoimalla mahdollisista riskeistä yritys voi osoittaa olevansa tietoinen potentiaalisista uhista ja tekevänsä aktiivisesti töitä niiden hallitsemiseksi, mikä voi olla

tärkeää sidosryhmien luottamuksen saavuttamiseksi. Modernien riskienhallintajärjestelmien ansiosta yrityksillä on myös paremmat mahdollisuudet hallita kyberturvallisuusriskejään, dokumentoida niitä ja siten raportoida niistä. Sen sijaan kohdatuista häiriötilanteista raportoinnin vähäisyys voi selittyä esimerkiksi maineen tai luottamuksen menettämisen pelolla. Häiriötilanteista raportointi voi herättää huolta sidosryhmissä, ja siksi yritykset voivat olla haluttomia jakamaan näitä tietoja avoimesti. Lisäksi joissain tapauksissa tietojen avoin jakaminen saattaa asettaa yrityksen entistä alttiimmaksi riskeille, tai esimerkiksi häiritä käynnissä olevaa häiriötapauksen tutkintaa.

Löydökset kyberturvallisuusraportoinnista osoittavat, että raportointi Suomessa on melko yleisluontoista ja keskittyy pitkälti toimenpiteisiin ja riskeihin. Tarkempien tietojen julkistamista halutaan välttää strategisista syistä. Nämä havainnot raportoinnin yleisyydestä, laajuudesta ja keskeisistä sisällöistä ovat siis pitkälti linjassa tutkimuksen viitekehyksen sekä muun aiemman teorian kanssa. Näin ollen suomalaisten yritysten kyberturvallisuusraportointi on hyvin samantasoista, kuin se on maailmanlaajuisestikin. Tämä voi myös osoittaa, että suomalaiset pörssiyritykset ovat tietoisia kyberturvallisuuden tärkeydestä, haluavat raportoida siitä aktiivisesti sekä seuraavat kansainvälisiä käytäntöjä kyberturvallisuusraportoinnin suhteen.

## 5.2 Raportoinnin johdonmukaisuus ja selkeys

Teeman *kyberturvallisuusriskit* kohdalla on havaittavissa, että useilla eri toimialoilla yli puolet yrityksistä raportoivat kyberturvallisuuden olevan merkittävä riski liiketoiminnalle. Kuitenkin kaikkien toimialojen kohdalla raportoivien yritysten osuus media-alaa lukuun ottamatta jää alle neljänneksen, kun tarkastellaan, miten moni yritys raportoi kyberturvallisuuden olevan liiketoiminnan keskeinen kulmakivi. Useat yritykset, jotka tunnistavat kyberturvallisuuden merkittäväksi liiketoimintariskiksi, eivät siis kuitenkaan tunnista sen olevan merkittävä lähtökohta liiketoiminnalle. Vaikka nämä kaksi asiaa eivät olekaan ristiriidassa keskenään, ei tämä välttämättä ole kaikille lukijoille itsestään selvää, sillä he voivat myös odottaa, että merkittävä riski heijastuisi keskeisenä liiketoiminnan kulmakivenä. Harva yritys kuitenkaan selvitti tätä asiaa tarkemmin raportoinnissaan.

Lisäksi teeman *kohdatut kyberturvallisuuden häiriötilanteet* kohdalla viisi yritystä korostaa erikseen, etteivät ne ole kokeneet kuluneen tilikauden aikana ollenkaan merkittäviä kyberturvallisuuden häiriötilanteita. Tämä voi viestiä esimerkiksi siitä, että yritys haluaa korostaa tietoturvansa olevan kunnossa, tai korostaa avoimuutta ja läpinäkyvyyttä

kertomalla, ettei häiriötilanteiden määrä ole täysi nolla. On kuitenkin syytä pohtia, millä tavalla vuosiraporttien yleisö tulkitsee sanan merkittävä. Yksi lukija voi esimerkiksi ajatella tämän tarkoittavan, että käytännössä kyberturvallisuuden häiriötilanteita ei ole ollenkaan, toinen lukija taas, että yritys pyrkii peittelemään jotain, jos tilanteista ei kerrota tämän avoimemmin.

Asayn ym. (2018) mukaan epäselkeä tai vaikealukuinen vuosiraportointi voi viestiä esimerkiksi yrityksen huonosta tuloksesta tai muista huonoista uutisista, ja tätä kautta vaikuttaa sidosryhmien luottamukseen tai yrityksen maineeseen. Näin ollen nämä havainnot korostavat tarvetta kyberturvallisuusraportoinnin johdonmukaisuudelle ja selkeydelle.

## 5.3 Havainnot toimialan ja kokoluokan perusteella

Kyberturvallisuudesta raportoitiin yleisesti eniten median, rahoituspalveluiden, ja tukku- ja vähittäiskaupan yrityksissä, ja nämä toimialat näkyvät aktiivisimpien raportoijien joukossa myös useamman eri yläteeman kohdalla. Vähäisintä raportointi taas oli yleisesti kiinteistötoimialan yrityksillä, ja tämän lisäksi teemakohtaisesti vaihdellen muun muassa perusteollisuudessa, kuluttajatuotteiden ja -palvelujen aloilla sekä muilla toimialoilla. Tulokset ovat jotakuinkin linjassa aiemman tutkimuksen kanssa, johon pohjaten raportointi on juuri yleisintä niillä toimialoilla, jotka ovat voimakkaasti teknologiariippuvaisia, ja vähäisintä taas niin sanotuilla perinteisillä toimialoilla, jotka eivät ole yhtä vahvasti riippuvaisia teknologiasta (Gao ym. 2020, Berkman ym. 2018).

Media-alan yritysten kyberturvallisuusraportoinnin aktiivisuus voi selittyä esimerkiksi sillä, että toimialan yritykset luottavat paljon digitaalisiin ratkaisuihin päivittäisessä toiminnassaan. Niiden ydintoiminnot tapahtuvat pääosin verkossa tai muilla digitaalisilla alustoilla, joka kasvattaa niiden kyberturvallisuusriskejä sekä riskiä joutua kyberhyökkäysten kohteeksi. Myös rahoituspalveluiden toimiala on pitkälti riippuvainen teknologiasta, ja sen ydintoiminnot luottavat mahdollisesti vielä media-alaa enemmän digitaalisiin ratkaisuihin ja tietojärjestelmiin. Toimialalla käsitellään paljon arkaluontoista ja arvokasta asiakkaisiin liittyvää dataa ja maksutapahtumia päivittäin, mikä tekee niistä houkuttelevia kohteita kyberrikollisille. Henkilö- ja pankkitietojen käsittelyyn liittyy toisaalta myös paljon lakivaatimuksia ja sääntelyä. Myös tukku- ja vähittäiskaupan alalla luotetaan yhä enemmän tietojärjestelmiin ja digitaalisiin ratkaisuihin, ja yhtä lailla tämän toimialan yritykset käsittelevät päivittäin asiakkaisiin liittyvää dataa sekä maksutapahtumia ja -tietoja. Kaikki kolme toimialaa ovat myös hyvin asiakassuuntautuneita ja näin ollen

asiakkaiden luottamuksen säilyttäminen on elintärkeää. Tietovuoto esimerkiksi pankin tai verkkokaupan asiakastietojärjestelmissä voi herättää suurta epäluottamusta kuluttajissa, ja koko media-ala taas perustuu Suomessa pitkälti ajatukseen siitä, että lehdistöön voi lähtökohtaisesti luottaa. Näistä syistä kyberturvallisuus on merkittävä osa liiketoimintaa kaikilla näillä kolmella toimialalla, ja voi olla, että siitä raportointia on näin ollen haluttu korostaa.

Vähäinen kyberturvallisuusraportointi voi taas selittyä juuri päinvastaisilla syillä. Esimerkiksi kiinteistöalalla tai perusteollisuudessa yritysten lähtökohdat liiketoiminnalle ovat hieman erilaiset. Näillä aloilla digitalisaatio ja teknologinen muutos ei ole ollut yhtä suurta, eivätkä toimialat toistaiseksi rakennu yhtä vahvasti digitaalisten palvelujen varaan. Näiden toimialojen yritykset eivät myöskään käsittele yhtä laajasti esimerkiksi henkilötietoja tai muuta arkaluontoista dataa, joka olisi suoraan houkutteleva kohde kyberrikollisille.

Kuluttajapalveluiden toimialalla, johon on tässä tutkimuksessa laskettu mukaan myös matkustuspalveluita tarjoavat yritykset, kuten lento- ja laivayhtiöt tai hotellit, vähäinen raportointi nousi esille erityisesti kyberturvallisuusstrategian kohdalla. On merkillepantavaa, ettei yhdenkään tämän toimialan yrityksen vuosiraportoinnissa löytynyt kyberturvallisuusstrategiaan liittyviä mainintoja, vaikka näiden yritysten voidaan kuitenkin olettaa käsittelevän myös paljon arkaluontoista dataa, kuten henkilötietoja, passien tai muiden matkustusasiakirjojen tietoja tai luottokorttidataa. Raportoinnin puutteellisuus tähän teemaan liittyen voisi johtua esimerkiksi siitä, ettei sidosryhmillä tästä huolimatta ole yhtä korkeita odotuksia näiden yritysten tietoturvallisuutta kohtaan, kuin esimerkiksi pankkeja. Siinä missä moni kuluttaja käsittää pankin liiketoiminnan pitkälti pysähtyvän palvelunestohyökkäyksen tapahtuessa, voi kuluttajien näkökulma taas olla, että lentokoneet pysyvät ilmassa ja hotellivieraat voivat jatkaa majoittumista huoneissaan, vaikka yrityksen tietojärjestelmät kohtaisivatkin häiriöitä.

Kokoluokan perusteella kyberturvallisuudesta raportoivat eniten suuret yritykset, vähiten taas pienet. Tämä on linjassa myös aiemman teorian kanssa. Suuremmilla yrityksillä on yleensä laajempi sijoittajapohja, jonka vuoksi ne voivat haluta kertoa kyberturvallisuustoimistaan laajemmin. Yrityksen koon kasvaessa luonnollisesti myös riskit kasvavat, joka voi osaltaan selittää laajempaa raportointia kyberturvallisuudesta. Yksi selitys tälle

ilmiölle voi myös olla, että suuremmilla yrityksillä on yksinkertaisesti enemmän resursseja käytettävissä kyberturvallisuuteen sekä toisaalta myös siitä raportointiin.

Yhteenvetona voidaan todeta, että kyberturvallisuusraportoinnin aktiivisuus vaihtelee huomattavasti eri toimialojen välillä Suomessa, ja raportointi on sitä aktiivisempaa, mitä teknologiariippuvaisempi toimiala on kyseessä. Tämä on myös linjassa aiemman tutkimuksen kanssa. Kokoluokan perusteella raportointi on taas verrannollista yrityksen kokoon, ja suuremmat yritykset raportoivat kyberturvallisuudesta pieniä aktiivisemmin. Yrityksen kokoon perustuvat eroavaisuudet ovat todennäköisimmin selitettävissä käytössä olevien resurssien määrällä. Nämä havainnot korostavat tarvetta ymmärtää toimialakohtaisia ja kokoluokasta johtuvia eroja kyberturvallisuusraportoinnissa.

# 6 Yhteenveto

## 6.1 Yhteenveto tutkimustuloksista

Tämän tutkielman tarkoituksena oli tarkastella kyberturvallisuusraportoinnin nykytasoa Suomessa. Tutkimuksen aineisto koostui 112 suomalaisen pörssiyrityksen vuosiraporteista. Tutkimus tehtiin sisällönanalyysinä, ja aineisto käytiin läpi hakusanojen avulla, jonka jälkeen osumat liitettiin seitsemään eri teemaan ja edelleen alateemoihin kontekstinsa perusteella. Tutkimuksessa pyrittiin muodostamaan poikkileikkaava kuva kyberturvallisuusraportoinnin nykytasosta ja sisällöistä Suomessa päätutkimuskysymyksen ja lisäksi kahden alatutkimuskysymyksen kautta.

Päätutkimuskysymykseen *”Millä tasolla suomalaisten pörssiyritysten kyberturvallisuusraportointi osana vuosiraportointia on?”* vastattiin tarkastelemalla kyberturvallisuuteen liittyvien hakusanojen esiintyvyyttä koko aineistossa ja yrityskohtaisesti. Tutkimuksen tulosten perusteella voidaan todeta, että kyberturvallisuusraportointi on Suomessa samalla tasolla kuin muualla maailmassa, ja soveltaa pitkälti globaaleja käytäntöjä. Raportointi on yleistä, sillä noin 86 % yrityksistä raportoi kyberturvallisuudesta jollakin tasolla. Raportointi ei kuitenkaan ole kovin yksityiskohtaista, ja tarkkoja tietoja yrityksen kyberturvallisuudesta tai siihen liittyvistä toimista ei ole tyypillistä kertoa avoimesti. Tulevaisuudessa yritysten voi olla syytä keskittyä erityisesti raportoinnin selkeyteen, ymmärrettävyyteen ja johdonmukaisuuteen.

Ensimmäiseen alatutkimuskysymykseen *”Minkälaisia tietoja vuosikertomukset sisältävät kyberturvallisuuteen liittyen?”* vastattiin liittämällä kyberturvallisuuteen liittyvät hakusanat seitsemään eri teemaan ja edelleen alateemoihin hakusanojen kontekstin perusteella. Kyberturvallisuusraportointi Suomessa keskittyy pitkälti yritysten kyberturvallisuustoimenpiteisiin ja niiden kohtaamiin kyberturvallisuusriskeihin. Kaikkein yleisimmin raportoidaan kyberturvallisuustoimenpiteistä, joista raportoi 66 % yrityksistä, sekä kyberturvallisuusriskeistä, joista raportoi 38 % yrityksistä. Sisällyttämällä näitä teemoja vuosiraportointiinsa, yritykset voivat haluta osoittaa olevansa tietoisia potentiaalisista uhista ja tekevänsä aktiivisesti töitä suojatakseen tietojaan ja järjestelmiään. Vähiten raportoidaan taas koetuista kyberturvallisuuden häiriötilanteista, sillä näistä raportointi voi herättää huolta sidosryhmissä ja näin ollen heikentää luottamusta. Myös nämä raportoinnin sisällöt ovat linjassa globaalien käytäntöjen kanssa.

Toiseen alatutkimuskysymykseen *”Onko raportointikäytäntöjen välillä eroja yritysten toimialan tai kokoluokan perusteella?”* vastattiin tarkastelemalla tutkimustuloksia myös yritysten toimialaa ja kokoluokkaa vasten. Raportoinnin aktiivisuus vaihtelee yrityksen toimialan ja kokoluokan perusteella. Raportointi on sitä aktiivisempaa, mitä teknologiariippuvaisempi toimiala on kyseessä, ja on yleisintä media-alan, rahoituspalveluiden, ja tukku- ja vähittäiskaupan yrityksissä, ja vähäisintä taas oli kiinteistötoimialalla. Suuremmat yritykset myös raportoivat pieniä aktiivisemmin, mikä voi selittyä esimerkiksi käytettävissä olevien resurssien määrällä.

Tutkimuksen löydökset osoittavat, että suomalaisten pörssiyritysten kybervallisuusraportointi on hyvin linjassa kansainvälisten käytäntöjen kanssa, ja suomalaisten yritysten voidaan olettaa tasapainottelevan samojen kyberturvallisuuskysymysten kanssa, kuin globaalitkin yritykset. Erot raportoinnissa toimialojen ja kokoluokkien välillä heijastelevat teknologiariippuvuuden ja käytössä olevien resurssien vaikutusta.

## 6.2 Tutkimuksen luotettavuuden arviointi

Tutkimuksen luotettavuutta on mahdollista arvioida esimerkiksi tulosten siirrettävyyden, uskottavuuden ja luotettavuuden perusteella. Laadullisesta tutkimuksesta osa perustuu kuitenkin aina myös tutkijan subjektiivisiin käsityksiin, ja näin ollen on tärkeää arvioida myös tutkijan puolueettomuutta (Tuomi & Sarajärvi 2018).

Tutkimustulosten siirrettävyydellä tarkoitetaan sitä, kuinka hyvin tulokset ovat siirrettävissä toiseen, vastaavaan kontekstiin (Tuomi & Sarajärvi 2018). Tämän tutkimuksen tulokset olivat pitkälti linjassa aiheen muun aiemman kansainvälisen tutkimuksen kanssa. Näin ollen voidaan olettaa, että näitä tutkimustuloksia voidaan soveltaa myös muualla maailmassa. Koska tutkimustuloksia tarkasteltiin myös eri toimialojen ja yritysten kokoluokkien perusteella, voi tulosten soveltaminen joissakin määrin eri kokoisiin tai eri toimialojen yrityksiin olla mahdollista. On kuitenkin huomattava, että tutkimuksessa tarkasteltiin ainoastaan pörssiyritysten raportointia vuosina 2022 tai 2023, ja näin ollen tutkimuksen tulokset muodostavat kuvan kyberturvallisuusraportoinnista ainoastaan tiettynä ajanhetkenä. Lisäksi aineistosta on rajattu pois valitun aineiston analyysimenetelmän vuoksi 18 yritystä, ja näin ollen aineisto koostuu 86 %:sta Helsingin pörssin yrityksistä (ks. luku 3.2).

Tutkimuksen uskottavuutta ja luotettavuutta voidaan arvioida pohtimalla, ovatko tutkimukseen kerätty aineisto ja tutkimustulokset totuudenmukaisia, ja voidaanko näihin tutkimustuloksiin lähtökohtaisesti luottaa (Tuomi & Sarajärvi 2018). Tutkimuksen aineisto kerättiin suoraan aineiston yritysten omilta verkkosivuilta, ja tutkimustuloksia on havainnollistettu sitaateilla, jotka ovat suoria lainauksia vuosiraporteista. Tutkimuksen aineistossa huomiotiin kaikki ne dokumentit, jotka yritykset itse kertoivat kuuluvan vuosiraportoinnin kokonaisuuteen. On siis pantava merkille, että yritysten käsitykset vuosiraportoinnista vaihtelevat, ja näin ollen raportit eivät ole määrämuotoisia eivätkä kaikilta osin lakisääteisiä, ja vaihtelua niiden tasossa voi esiintyä myös tämän vuoksi. Tutkielman aineisto käytiin läpi ensin koneellisesti, jotta mahdollisimman monilta manuaalisilta virheiltä voitaisiin välttyä. Hakusanojen osumat on kuitenkin liitetty eri teemoihin manuaalisesti, tutkijan käsityksen perusteella niiden kontekstista.

Tutkijan puolueettomuuden puolesta puhuu se, ettei tutkimusta tehty toimeksiantona millekään yritykselle. Näin ollen kaikkien yritysten vuosiraportteihin on ollut mahdollista suhtautua mahdollisimman puolueettomasti ja tulosten analysoinnissa on pyritty objektiivisuuteen. Vaikka hakusanojen osumat on liitetty teemoihin tutkijan parhaan käsityksen perusteella, on kaikkiin osumiin kuitenkin sovellettu samoja luokitteluperusteita, ja samankaltaiset osumat on luokiteltu aina samoihin teemoihin. Epäselvän kontekstin tapauksessa osumaa ei luokiteltu yhteenkään teemaan (ks. luku 4.1.3).

## 6.3 Tutkimuksen merkitys ja jatkotutkimus

Vaikka kyberturvallisuus on kasvava teema, ja vaikuttaa yhä enemmän ja enemmän yritysten toimintaan, ei sen sisällyttämisestä yritysten vuosiraportointiin ole tehty vielä systemaattisesti tutkimusta, ja erityisesti Euroopassa ja Suomessa aiheen tutkimus on ollut hyvin vähäistä. Tämä tutkielma vastaa tähän tutkimusaukkoon ja tarjoaa kuvan pörssiyhtiöiden kyberturvallisuusraportoinnin tilasta ja käytännöistä Suomessa. Tutkimus tarjoaa myös suuntaviivoja tulevaisuuden raportointikäytäntöjen kehittämiseksi.

Tutkimuksen tulokset tarjoavat myös yritysjohdolle arvokasta tietoa niin markkinan nykyisestä kyberturvallisuuden tasosta kuin siitä, miten ja mitä kyberturvallisuudesta kerrotaan osana vuosiraportointia. Tutkimuksen tulosten perusteella yritysten on mahdollista vertailla niin omia kyberturvallisuustoimenpiteitään kuin omaa kyberturvallisuusraportointiaan verrokkiryhmiensä tasoon. Tämän pohjalta organisaatiot voivat tunnistaa

tarpeellisia kehityskohteita ja toteuttaa tarvittavia toimenpiteitä kyberturvallisuusstrategioidensa ja -raportointinsa parantamiseksi.

Koska aiheen tutkimus on Euroopassa ja Suomessa edelleen hyvin vähäistä, olisi jatkotutkimus mielekästä toistettavuuden kannalta. Jatkossa tutkimusta voitaisiin laajentaa tehtäväksi esimerkiksi pitkittäistutkimuksena, jolloin voitaisiin nähdä, onko kyberturvallisuusraportointi kehittynyt Suomessa samoin kuin maailmalla. Lisäksi tämän perusteella voitaisiin myös tutkia, mitkä asiat ovat mahdollisesti Suomessa vaikuttaneet raportoinnin kehittymiseen ajan saatossa. Olisi esimerkiksi mielenkiintoista nähdä, onko Psykoterapiakeskus Vastaamon vuonna 2020 paljastuneella tietomurrolla ollut raportointiin vastaavanlaista vaikutusta, kuin Bangladeshin keskuspankin tietoturvavahingoilla vuonna 2016. Tulevaisuudessa tutkimusta voitaisiin tehdä myös liittyen kyberturvallisuusraportoinnin motiiveihin Suomessa.

## Lähteet

Arvopaperimarkkinalaki. <https://www.finlex.fi/fi/laki/ajantasa/2012/20120746#O3L7P6>, haettu 9.5.2024.

Asay, H. S. – Libby, R. – Rennekamp, R. (2018) Firm performance, reporting goals, and language choices in narrative disclosures. *Journal of Accounting and Economics,* Vol. 65, 380-398.

Baker, H. K – Pandey, N. – Kumar, S. – Haldar, A. (2020) A bibliometric analysis of board diversity: Current status, development, and future research directions. *Journal of Business Research*, Vol. 108, 232-246.

Berkman, H. – Jona, J. – Lee, G. – Soderstrom, N. (2018) Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy*, Vol. 37 (6), 508-526.

Bravo, F. (2018) Does board diversity matter in the disclosure process? An analysis of the association between diversity and the disclosure of information on risks. *International journal of disclosure and governance,* Vol. 15 (2), 104-114.

Chircop, J. – Gagnon, J. – Young, S. (2022) Capital market response to high quality annual reporting: evidence from UK annual report awards. *Accounting and Business Research,* Vol. 54 (2), 125-167.

D'Arcy, J. – Basoglu, A. (2022) The Influences of Public and Institutional Pressure on Firms' Cybersecurity Disclosures. Journal of the Association for Information Systems, Vol. 23 (3), 779-805.

Eijkelenboom, E. V. A. – Nieuwesteeg, B. F. H. (2021) An analysis of cybersecurity in Dutch annual reports of listed companies. *Computer Law & Security Review*, Vol. 40, 1-15.

Euroopan komissio (2023) Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive). <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>, haettu 4.2.2024.

Euroopan komissio (2024) Tietosuoja EU:ssa. <https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_fi>, haettu 22.2.2024.

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, <https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:02016R0679-20160504>, haettu 22.2.2024.

Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, <https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX:32022L2555&qid=1707068380347>, haettu 4.2.2024.

Firoozi, M. – Mohsni, S. (2023) Cybersecurity disclosure in the banking industry: a comparative study. *International Journal of Disclosure and Governance*, Vol. 20 (4), 451-477.

Forbes 3.12.2023 The 9 Biggest Risks And Threats That Companies Will Face In 2024. <https://www.forbes.com/sites/edwardsegal/2023/12/03/the-8-biggest-risks-and-threats-that-companies-will-face-in-2024/>, haettu 9.5.2024.

Gao, L. – Calderon, T. G. – Tang, F. (2020) Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems*, Vol. 38, 1-22.

Gordon, L. A. – Loeb, M. P. – Sohail, T. (2010) Market Value of Voluntary Disclosures Concerning Information Security. *MIS Quarterly*, Vol. 34 (3), 567-594.

Helsingin Sanomat 21.10.2020 Potilaiden tietoja vietiin psykoterapiakeskuksen tietomurrossa, yritys kertoo joutuneensa kiristyksen uhriksi. <https://www.hs.fi/kotimaa/art-2000006676407.html>, haettu 9.5.2024.

Héroux, S. – Fortin, A. (2020) Cybersecurity Disclosure by the Companies on the S&P/TSX 60 Index. *Accounting Perspectives*, Vol. 19 (2), 73-100.

Héroux, S. – Fortin, A. (2022) Board of directors' attributes and aspects of cybersecurity disclosure. *Journal of Management and Governance*, <https://doi.org/10.1007/s10997-022-09660-7>, haettu 19.2.2024.

Hynes, G. E. (2009) Annual Reports: A Tool for Businesses, Investors, and Educators. *Journal of Organizational Behavior Education*, Vol 2, 81-96.

Isiaka, A. S. (2021) Risk Factor Disclosures: A Review and Directions for Future Research. *Accounting Perspectives*, Vol. 20 (4), 583–615.

Juholin, E. (2022) *Communicare! : ota viestinnän ilmiöt ja strategiat haltuun.* 8. uud. p. Infor / Management Institute of Finland MIF Oy, Helsinki.

Kirjanpitolaki. <https://www.finlex.fi/fi/laki/ajantasa/1997/19971336 >, haettu 4.7.2024.

Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä. <https://www.finlex.fi/fi/laki/ajantasa/2023/20230703>, haettu 22.2.2024.

Laki sähköisen viestinnän palveluista. <https://www.finlex.fi/fi/laki/ajantasa/2014/20140917>, haettu 22.2.2024.

Leppiniemi, J. – Leppiniemi, R. – Kaisanlehti, T. (2013) *Hyvä tilinpäätöskäytäntö.* Alma Talent Oy, Helsinki.

Li, H. – No, W. G, - Wang, T. (2018) SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, Vol. 30, 40-55.

Lipasti, L. – Pietiläinen, M. – Katainen, A. (2020) *Naiset ja miehet yritysten ylimmässä johdossa: Tilastoselvitys.* Sosiaali- ja terveysministeriön raportteja ja muistioita 2020:12. Sosiaali- ja terveysministeriö, Helsinki.

Loughran, T. – McDonald, B. (2011) When Is a Liability Not a Liability? Textual Analysis, Dictionaries, and 10-Ks. *The Journal of Finance*, Vol. 66 (1), 35-65.

Maailman talousfoorumi 10.1.2024 Global Risks Report 2024. <https://www.weforum.org/publications/global-risks-report-2024/>, haettu 9.5.2024.

Makridis, C. A. (2021) Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018. *Journal of Cybersecurity*, Vol. 7 (1), 1-8.

Mazumder, M. M. M. – Hossain, D. M. (2022) Voluntary cybersecurity disclosure in the banking industry of Bangladesh: does board composition matter? *Journal of Accounting in Emerging Economies*, Vol. 13 (2), 217-239.

Oxford English Dictionary (2023) Annual report. <https://doi.org/10.1093/OED/9746888716>, haettu 11.2.2024.

Oxford English Dictionary (2023) Cybersecurity. <https://doi.org/10.1093/OED/6503222281>, haettu 11.2.2024.

Oxford English Dictionary (2023) Data protection. <https://doi.org/10.1093/OED/1033708625>, haettu 11.2.2024.

Oxford English Dictionary (2023) Information security. <https://doi.org/10.1093/OED/7095903709>, haettu 11.2.2024.

Pavlou, P. A. – Liang, H. – Xue, Y. (2007) Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal–Agent Perspective. *MIS Quarterly*, Vol. 31 (1), 105-136.

Radu, C. – Smaili, N. (2022) Board Gender Diversity and Corporate Response to Cyber Risk: Evidence from Cybersecurity Related Disclosure.

Ramírez, M. – Rodríguez Ariza, L. – Gómez Miranda, M. E. – Vartika (2022) The Disclosures of Information on Cybersecurity in Listed Companies in Latin America—Proposal for a Cybersecurity Disclosure Index. *Sustainability*, Vol. 14 (3), 1390.

Sitra (2023) Megatrendit 2023 Ymmärrystä yllätysten aikaan. <https://www.sitra.fi/julkaisut/megatrendit-2023/>, haettu 4.2.2024. *Journal of Business Ethics*, Vol. 177, 351–374.

Statista (2024) Annual number of data compromises and individuals impacted in the United States from 2005 to 2023. <https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/>, haettu 9.5.2024.

Statista (2024) Average cost of a data breach in the United States from 2006 to 2023. <https://www.statista.com/statistics/273575/us-average-cost-incurred-by-a-data-breach/>, haettu 9.5.2024.

Sähkömarkkinalaki. <https://www.finlex.fi/fi/laki/ajantasa/2013/20130588>, haettu 22.2.2024.

THL (2023) Sukupuolten tasa-arvo yritysjohdossa. <https://thl.fi/aiheet/sukupuolten-tasa-arvo/tasa-arvon-tila/valta-ja-paatoksenteko/sukupuolten-tasa-arvo-yritysjohdossa>, haettu 4.7.2024.

Tietosuojavaltuutetun toimisto. Tietosuoja. <https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf>, haettu 21.4.2024.

Traficom 21.4.2023 Kyberturvallisuuden uhkataso pysynyt kohonneena - kohdistettujen hyökkäysten määrä noussut. <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuden-uhkataso-pysynyt-kohonneena-kohdistettujen-hyokkaysten-maara>, haettu 9.6.2024.

Tuomi, J. – Sarajärvi, A. (2018) *Laadullinen tutkimus ja sisällönanalyysi*. Uudistettu Laitos. Tammi, Helsinki.

Turvallisuuskomitea (2018) Kyberturvallisuuden sanasto. <https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf>, haettu 11.2.2024.

von Solms, R. – van Niekerk, J. (2013) From information security to cyber security. *Computers & Security*, Vol. 38, 97-102.

Weber, R. P. (1990) *Basic Content Analysis – Second Edition*. Quantitative Applications in the Social Sciences, nro 49. Sage University Papers, Sage, Newsbury Park.

Yle Uutiset 11.2.2021 Tietomurron kohteeksi joutunut psykoterapiakeskus Vastaamo on haettu konkurssiin – selvitysmies jatkajasta: "Kiinnostuneita tahoja oli monta". < https://yle.fi/a/3-11784072>, haettu 9.5.2024.

Yuthas, K. – Rogers, R. – Dillard, J. F. (2002) Communicative Action and Corporate Annual Reports. *Journal of Business Ethics,* Vol. 41, 141–157.

# Liite 1 Kaikki hakusanojen osumat perusmuodossa

| **H** | | |
|---|---|---|
| haavoittuva | haavoittuvuusarviointi | haittaohjelmahyökkäys |
| haavoittuvuuksienhallinta | haavoittuvuuskartoitus | hakkeri |
| haavoittuvuus | haittaohjelma | |

| **K** | | |
|---|---|---|
| kiristysohjelma | kyberturvallisuusjohtaminen | kyberturvallisuustoiminto |
| kyberhäiriötilanne | kyberturvallisuuskartoitus | kyberturvallisuustuote |
| kyberharjoitus | kyberturvallisuuskäytäntö | kyberturvallisuustyö |
| kyberhyökkäys | kyberturvallisuuskeskus | kyberturvallisuusuhka |
| kyberkoordinaatio | kyberturvallisuuskoulutus | kyberturvallisuusvaatimus |
| kyberkoordinaatioryhmä | kyberturvallisuuskuukausi | kyberturvallisuusvakuutusohjelma |
| kyberkoordinointi | kyberturvallisuuskysymys | kyberturvallisuusvalmius |
| kyberrikollinen | kyberturvallisuuslautakunta | kyberturvallisuusvastuut |
| kyberrikollisuus | kyberturvallisuusloukkaus | kyberturvapoikkeama |
| kyberrikos | kyberturvallisuusohjelma | kyberturvariski |
| kyberriski | kyberturvallisuusongelma | kyberturvateknologia |
| kybersietokyky | kyberturvallisuuspäällikkö | kyberturvatietoisuus |
| kybersodankäynti | kyberturvallisuuspoikkeama | kyberturvattu |
| kybertietoisuus | kyberturvallisuusrikkomus | kyberturvauhka |
| kybertietoisuuskoulutus | kyberturvallisuusriski | kyberuhka |
| kybertoimi | kyberturvallisuusstrategia | kyberuhkatiedustelu |
| kyberturva | kyberturvallisuustapahtuma | kybervahinko |
| kyberturvallisuus | kyberturvallisuustietoisuus | kybervakuutus |
| kyberturvallisuushäiriö | kyberturvallisuustiimi | kybervaliokunta |
| kyberturvallisuusharjoitus | kyberturvallisuustoimi | käyttöoikeuksien hallinta |
| kyberturvallisuusjärjestelmä | kyberturvallisuustoiminta | |

| **P** | | |
|---|---|---|
| palvelunestohyökkäys | pääsynhallinta | pääsynhallintapolitiikka |

| T | | |
|---|---|---|
| tietoturva | tietoturvallisuuspolitiikka | tietoturvasääntely |
| tietoturva-aihe | tietoturvallisuusriski | tietoturvasertifikaatti |
| tietoturva-arkkitehtuuri | tietoturvallisuustietoisuus | tietoturvasertifioitu |
| tietoturva-asia | tietoturvallisuustoimenpide | tietoturvastandardi |
| tietoturva-asiantuntija | tietoturvallisuustoimi | tietoturvastrategia |
| tietoturva-asiantuntijatiimi | tietoturvallisuustoiminto | tietoturvastressitestaus |
| tietoturva-auditointi | tietoturvallisuustyö | tietoturvatapahtuma |
| tietoturvahäiriö | tietoturvaloukkaus | tietoturvatarkastus |
| tietoturvahyökkäys | tietoturvaloukkausilmoitus | tietoturvataso |
| tietoturvailmoitusprosessi | tietoturvaloukkausprosessi | tietoturvatavoite |
| tietoturvajärjestelmä | tietoturvaloukkaustyöryhmä | tietoturvatestaaja |
| tietoturvajärjestely | tietoturvaluokitus | tietoturvatestaus |
| tietoturvajohtaja | tietoturvamateriaali | tietoturvatesti |
| tietoturvajohtaminen | tietoturvamonitorointi | tietoturvatieto |
| tietoturvakampanja | tietoturvanhallintajärjestelmä | tietoturvatietämys |
| tietoturvakatsaus | tietoturvaohje | tietoturvatietoisuus |
| tietoturvakäytäntö | tietoturvaohjelma | tietoturvatiimi |
| tietoturvakeskus | tietoturvaongelma | tietoturvatilanne |
| tietoturvakontrolli | tietoturvaorganisaatio | tietoturvatoimenpide |
| tietoturvakoulutus | tietoturvaosaaminen | tietoturvatoimi |
| tietoturvakoulutusohjelma | tietoturvapäällikkö | tietoturvatoiminta |
| tietoturvakriittinen | tietoturvapäivitys | tietoturvatyö |
| tietoturvakulttuuri | tietoturvaperiaatteet | tietoturvauhka |
| tietoturvakysymys | tietoturvapoikkeama | tietoturvavaatimus |
| tietoturvakyvykkyys | tietoturvapolitiikka | tietoturvavalmius |
| tietoturvalaki | tietoturvaprosessi | tietoturvavalvomo |
| tietoturvallinen | tietoturvapuute | tietoturvavastaava |
| tietoturvallisuus | tietoturvaratkaisu | tietoturvaverkkokurssi |
| tietoturvallisuusasia | tietoturvarikkomus | tietoturvaviitekehys |
| tietoturvallisuuskatsaus | tietoturvariski | tietoturvayksikkö |
| tietoturvallisuuspoikkeama | tietoturvaryhmä | |