Mikko Heikkinen

KYBERRISKIT JA -UHKAT SUOMALAISTEN PÖRSSI-YHTIÖIDEN HALLITUSTEN TOIMINTAKERTOMUK-SISSA 2019–2023

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

TIIVISTELMÄ

Heikkinen, Mikko
Kyberriskit ja -uhkat suomalaisten pörssiyhtiöiden hallitusten toimintakertomuksissa 2019–2023
Jyväskylä: Jyväskylän yliopisto, 2024, 74 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja: Lehto, Martti

Tutkimuksen tavoitteena oli tuottaa tietoa kyberriskien ja -uhkien esiintyvyydestä ja niiden kehityksestä suomalaisten pörssilistattujen yhtiöiden hallitusten toimintakertomuksissa sekä tunnistaa kyberriskikuvauksissa esiintyvä teemoja. Yrityksillä on keskeinen rooli suomalaisessa kokonaisturvallisuuden mallissa, jonka yksi osa-alue on kyberturvallisuus. Yrityksen hallituksella on viimesijainen vastuu yrityksen riskienhallinnan toteuttamisesta ja valvonnasta. Suomessa on tehty vähän tutkimusta yritysten hallitusten roolista kyberturvallisuuden johtamisessa ja tämä tutkimus selvitti missä määrin kyberriskit ja -uhkat koetaan merkittävinä riskeinä ja epävarmuustekijöinä pörssilistatuissa yhtiöissä.

Tutkimus oli pitkittäistutkimus, jonka perusjoukkona oli arvopaperipörssi Nasdaq Helsingin päälistalla noteeratut yhtiöt vuosina 2019–2023. Aineistona käytettiin yhtiöiden julkaisemia hallituksen toimintakertomuksen sisältäviä vuosiraportteja. Tutkimusmenetelmänä oli aineistolähtöinen sisällönanalyysi, joka toteutettiin sekä määrällisin että laadullisin tekniikoin.

Tuloksena tutkimuksessa esitettiin, että vuosina 2019–2023 kyberriskien ja -uhkien esiintymistiheys pörssilistattujen hallitusten toimintakertomuksissa kasvaa ja riskikuvaukset muuttuvat luonteeltaan yleisistä yksityis- ja yrityskohtaisemmiksi. Merkittävä osa yhtiöistä raportoi kuitenkin edelleen kyberriskeistään yleisellä tasolla, jonka lisäarvo raportoinnin sidosryhmille jää matalaksi. Tutkimuksen perusteella kyberriskiä ei koeta strategisena riskinä, vaan se nähdään operatiivisena riskinä.

Asiasanat: kyberriski, kyberuhka, hallituksen toimintakertomus, pörssiyhtiö

ABSTRACT

Heikkinen, Mikko
Cyber risks and threats in the board of directors' reports of Finnish listed companies in 2019–2023
Jyväskylä: University of Jyväskylä, 2024, 74 pp.
Cyber Security, Master's Thesis
Supervisor: Lehto, Martti

The aim of the study was to examine the prevalence and evolution of cyber risks and threats as reported in the annual reports of Finnish publicly listed companies and to identify recurring themes in the descriptions of cyber risks. Companies play a central role in the Finnish comprehensive security model, which includes cybersecurity. The responsibility for implementing and overseeing a company's risk management ultimately lies with its board of directors. However, there has been limited research in Finland on the involvement of company boards in managing cybersecurity. This study aimed to assess the extent to which cyber risks and threats are regarded as significant risks and as uncertainties by publicly listed companies.

This longitudinal study focused on companies listed on the main list of the Nasdaq Helsinki stock exchange from 2019 to 2023. The data consisted of annual reports containing the board directors' report, as published by these companies. The research method employed was data-driven content analysis, incorporating both quantitative and qualitative techniques.

The results of this study indicated that between 2019 and 2023, the frequency of mentions of cyber risks and threats in annual reports increased. Additionally, the descriptions of these risks evolved from general statements to more detailed and company-specific narratives. Despite this trend, a substantial portion of companies continued to report their cyber risks in a general manner, which provides limited value to stakeholders. The results of this study suggested that cyber risk is not perceived as a strategic risk but rather as an operational risk.

Keywords: cyber risk, cyber threat, board of directors' report, listed company

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Suomessa on käytössä kokonaisturvallisuuden yhteistoimintamalli, jossa kansallinen kokonaisturvallisuus rakentuu toimijoiden yhteistyössä. Elinkeinoelämä, jota yritykset edustavat, on yksi keskeinen toimija kokonaisturvallisuuden yhteistoimintamallissa (*Yhteiskunnan turvallisuusstrategia*, 2017). Kyberturvallisuus on osa kokonaisturvallisuutta ja yritysten roolina on suojata oma toimintansa, mutta myös osallistua osaltaan kokonaisturvallisuuden toteutukseen kansallisesti. Yhteiskunnan turvallisuusstrategiassa (2017) on määritetty yhteiskunnan toimivuuden kannalta kaikissa tilanteissa ylläpidettävät välttämättömät toiminnot. Yksi välttämättömäksi määritelty toiminto on talous, infrastruktuuri ja huoltovarmuus. Tähän toimintoon kuuluu muun muassa rahoitusjärjestelmän toiminnan turvaaminen. Rahoitusmarkkinoiden toimivuudella on nykyisessä yhteiskunnassa erittäin merkittävä rooli ja se on myös täysin riippuvainen tietoliikenneyhteyksistä ja tietojärjestelmistä. Tietoliikenneyhteyksiä tai rahoitusmarkkinapalveluita tarjoavia yrityksiä vastaan toteutettu laajamittainen kyberhyökkäys olisi koko yhteiskuntaa koskettava ja se olisi vaikutuksiltaan dramaattinen. Rahoitusmarkkinapalveluita tarjoavien yritysten keskuudessa tämä riski on tunnistettu. Englannin keskuspankki tekee puolivuosittain tutkimuksen, joka kartoittaa rahoitusmarkkinoiden systeemisiä riskejä. Vuoden 2023 toisen vuosipuoliskon tutkimuksessa suurimpana riskien lähteenä pidettiin kyberhyökkäyksiä (Bank of England, 2023). 80 % vastaajista piti kyberoperaatioita vaikutuksiltaan merkittävimpänä riskinä rahoitusmarkkinoiden toiminnalle. Kyberriskit mainittiin tässä tutkimuksessa 5 %-yksikköä useammin kuin puolta vuotta aiemmin tehdyssä tutkimuksessa. Samassa tutkimuksessa selvitettiin vastaajien mielipidettä siitä, että mitkä riskit heidän mielestään toteutuvat todennäköisimmin. Tässä kysymyksessä talouden inflaatiota (52 % vastaajista) pidettiin todennäköisimpänä toteutuvana riskinä, mutta kyberuhkat (46 % vastaajista) koettiin heti toiseksi todennäköisimpänä toteutuvana uhkana (Bank of England, 2023).

Kyberuhkat eivät ole vain rahoitusmarkkinoiden tai tietoliikenteen palveluita tarjoavien yritysten ongelma. Toimivien tietoliikenneyhteyksien ja tietojärjestelmien merkitys ja rooli on keskeinen lähes jokaiselle toimialalle. Kun kyber-

turvallisuus pettää, voi yritykselle aiheutua mittavia taloudellisia tappioita ja muita vahinkoja esimerkiksi maineen menetyksen muodossa. Suomessa pörssilistatuista yhtiöistä ainakin Uponor ja Tietoevry ovat joutuneet kyberhyökkäysten kohteiksi, joista aiheutui yrityksille merkittävää haittaa. Uponor raportoi vuonna 2022 tapahtuneen kyberhyökkäyksen laskeneen liikevaihtoa kymmenillä miljoonilla euroilla (Helsingin Sanomat, 2023) ja Tietoevry arvioi siihen alkuvuonna 2024 kohdistuneen kyberhyökkäyksen aiheuttaneen 2–4 miljoonan euron kustannukset (Helsingin Sanomat, 2024). Pahimmillaan seurauksena on liiketoiminnan loppuminen ja konkurssi, kuten esimerkiksi surullisen kuuluisa psykoterapiakeskus Vastaamon tapaus osoitti. Kyseisessä tapauksessa vahingon kärsijöiksi eivät joutuneet pelkästään yrityksen omistajat, vaan Vastaamoon tehty tietomurto aiheutti lisäksi mittaamatonta inhimillistä kärsimystä kymmenille tuhansille yrityksen asiakkaina olleille suomalaisille.

Yrityksen johdolla ja hallituksella on erityinen merkitys siinä, miten kyberturvallisuus koetaan yrityksessä. Perinteisesti tietoturva ja kyberturvallisuus on mielletty operatiiviseksi asiaksi ja sitä ei ole nähty yrityksissä strategisena kysymyksenä. Hepfnerin ja Powellin mukaan (2020) tähän on useita syitä. Ensinnäkin kyberturvallisuus on koettu IT-asioihin kuuluvaksi ja sen hallinta on delegoitu tietohallinnolle. Useassa yrityksessä tietohallintoa ei koeta kilpailuetua tuovana strategisena toimintona ja sen vuoksi myös kyberturvallisuuteen liittyvät asiat nähdään osana operatiivista tietohallintoa. Lisäksi kyberturvallisuuden priorisointiin vaikuttaa hallituksen ja ylemmän johdon oma osaaminen ja kokemus tietoturvasta ja kyberturvallisuudesta. Koska kyberhyökkäyksiä kohdistuu yrityksiä kohtaan kuitenkin verrattain harvoin, puuttuu ylemmältä johdolta kokemus huomioida kyberuhkat strategisessa suunnittelussa. Tapahtuneista kyberhyökkäyksistä ei myöskään aina kerrota julkisesti, joten yritysjohdon tilannekuva kyberuhkista saattaa jäädä vajaaksi. Kun toteutuneista kyberriskeistä ei jaeta tietoa, ei yritysjohdolla ole mahdollisuutta jakaa kokemuksia muiden yritysten kanssa ja siten oppia muiden kokemuksista. Tärkein Hepfnerin ja Powellin (2020) havainto on kuitenkin se, että yritysjohto ei näytä ymmärtävän kyberriskien strategista luonnetta. Kyberriskit mielletään sattumanvaraisiksi ja huonosti ennakoitaviksi tapahtumiksi, kun todellisuudessa yksikään yritys ei nykyisin ole immuuni kyberhyökkäyksille. Yritysten välillä on eroja siinä, kuinka houkuttelevana kohteena ne nähdään kyberuhkatoimijoiden keskuudessa. Vaikka yritys mieltäisi oman houkuttelevuutensa matalaksi kyberuhkatoimijoiden silmissä, se voi olla osa laajempaa asiakkaiden ja yhteistyötahojen verkostoa, johon kuuluu myös korkeamman riskin kohteita. Niin sanotut toimitusketjuhyökkäykset ovat kasvava uhka (Suojelupoliisi, 2021b). Yritysjohdon on varauduttava siihen, että yritykseen kohdistuneen kyberhyökkäyksen vaikutukset heijastuvat omassa toimitusketjussa ja verkostossa myös muihin osapuoliin. Vastaavasti johdon on valmistauduttava toimitusketjussa toiseen osapuoleen kohdistuneen kyberhyökkäyksen vaikutuksiin omaan toimintaan.

Konsultointiyhtiö McKinsey & Companyn (2024) mukaan yrityksen hallituksella on useita rooleja ja tehtäviä kyberuhkilta suojautumisessa. Hallituksen

tehtävä on ennen kaikkea valvoa ja ohjata kyberturvallisuuden käytännön toteutusta sekä varmistaa, että kyberturvallisuus otetaan huomioon niin digitaalisten tuotteiden suunnittelussa kuin käytetyissä työkaluissa. Hallituksen tehtäviin kuuluu myös riskien priorisointi. Hallitusten kokoonpanoissa ei välttämättä ole kyberturvallisuuden asiantuntemusta, mutta sen vuoksi yhteistyö kyberturvaosaajien kanssa on tärkeä riskitason sovittamisessa. Vastuu kyberturvallisuuteen ylläpitoon ja kehittämiseen allokoitavasta budjetista ja resursseista kuuluu myös hallituksen toimenkuvaan. Valvonta-, priorisointi- ja resursointitehtävien toteuttamiseksi hallituksen on myös järjestettävä kyberturvallisuuden raportointiprosessi ja johtovastuut. Näin siis teoriassa ja liikkeenjohdon konsulttien raporteissa. Tieteellisen tutkimuksen perusteella on kuitenkin epäselvää, kuinka hallituksen roolit kyberturvallisuuden johtamisessa käytännössä toteutuvat (Gale ym., 2022). Vaikka kirjallisuudessa korostetaan kyberturvallisuuden strategista merkitystä, nähdään kyberturvallisuus kuitenkin teknisenä osa-alueena, jolla on vähäinen liiketoiminnallinen merkitys (Oltsik, 2020). Operatiivisen johdon ja hallituksen välinen kommunikaatiossa on myös puutteita (McKinsey & Company, 2024; World Economic Forum, 2023). Kommunikaatio ylimmän johdon kanssa pitäisi sisältää vähemmän kyberturvallisuuden jargonia ja ylimmän johdon tulisi pystyä kommunikoimaan paremmin, mitä yrityksen informaatiovarantoja ja niihin liittyviä prosesseja pitäisi priorisoida kyberturvallisuuden johtamisessa (World Economic Forum, 2023).

Vaikka ylimmän johdon ja toimivan johdon välillä on viestinnällisiä haasteita ja eroavia riskinäkemyksiä kyberturvallisuuden luonteesta, on geopoliittisten jännitteiden lisääntyminen kuitenkin vähentänyt riskinäkemysten eroja. Maailman talousfoorumin vuonna 2023 julkaistun tutkimuksen mukaan (World Economic Forum, 2023) 91 % vastaajista piti vähintäänkin jokseenkin todennäköisenä kauaskantoisen ja katastrofaalisen kyberturvallisuustapahtuman mahdollisuutta seuraavan kahden vuoden aikana ja 70 % vastaajista kertoi geopoliittisten jännitteiden lisääntymisen vaikuttaneen organisaation kyberturvallisuusstrategiaan vuotta myöhemmässä tutkimuksessa (World Economic Forum, 2024).

Euroopan unionin uusi kyberturvallisuusdirektiivi (NIS2-direktiivi) tulee voimaan lokakuussa 2024. Suomen hallitus on tehnyt esityksen uudesta kyberturvallisuuslaista[1], jolla pannaan täytäntöön kansallisesti NIS2-direktiivin vaatimukset (HE 57/2024). Lakiesityksessä lain soveltamisala laajenee NIS-direktiiviin ensimmäiseen versioon verrattuna ja laki koskettaa huomattavan suurta osaa suomalaisista yrityksistä yhteiskunnan kannalta keskeisiksi ja tärkeiksi määritellyillä toimialoilla. Lisäksi lakiesityksen perusteella yrityshallitusten rooli ja vastuu kyberturvallisuudesta laajenee. Lakiesityksen perusteella lain soveltamisalaan kuuluvien yritysten hallituksille tulee muun muassa korvausvastuu lain määräysten rikkomuksesta ja hallituksessa on oltava riittävä ja ajantasainen perehtyneisyys kyberturvallisuuden riskienhallintaan sekä velvoite

[1] Valmisteluvaiheessa laista on käytetty myös nimitystä laki kyberturvallisuuden riskienhallinnasta.

hankkia ja ylläpitää kyberturvallisuuteen liittyvää perehtyneisyyttä kouluttautumalla tai muulla tavoin säännöllisin väliajoin.

1.1 Tutkimuskysymys ja tutkimuksen tavoitteet

Tämän tutkimuksen tavoitteena on muodostaa kuva siitä, miten suomalaisissa pörssilistatuissa yhtiöissä tunnistetaan kyberriskejä ja -uhkia ylimmän johdon näkökulmasta. Tutkimuksen lopputuloksena syntyy tietoa siitä, miten merkittävinä uhkatekijöinä kyberriskejä organisaatioissa pidetään vai nousevatko ne ollenkaan niin sanotusti ”hallitusten agendalle”. Tavoitteena on luoda uutta tietoa tutkittavasta perusjoukosta sekä tutkittavan perusjoukon kehityksestä ja nykytilanteesta. Tutkimuskysymyksenä on, *mitä kyberriskejä ja -uhkia suomalaisten pörssiyhtiöiden hallitukset ovat raportoineet toimintakertomuksissaan vuosina 2019–2023 ja mitä teemoja kyberriskikuvauksissa esiintyy?*

Työn kontribuutiona syntyy tietoa siitä, missä laajuudessa kyberriskit koetaan merkittävinä epävarmuustekijöinä suomalaisissa pörssiyhtiöissä ja siitä, onko Suomen turvallisuustilanteessa tapahtunut muutos vaikuttanut yhtiöiden hallitusten raportoimiin merkittäviin epävarmuustekijöihin kyberriskien osalta. On syytä painottaa, että tutkimuksessa kyberriskien ja -uhkien näkökulma on strateginen ja keskittyy siihen, mitä yhtiöiden hallitukset ovat kyberriskeistä ja -uhkista toimintakertomuksissaan todenneet. Julkisesti saatavilla olevista raporteista ei voida muodostaa läpileikkaavaa kokonaiskuvaa kaikista yritysten tunnistamista riskeistä ja näin ollen esimerkiksi tietoturvaan ja kyberturvallisuuteen liittyviä riskejä on todennäköisesti yhtiöissä tunnistettu, vaikka niitä ei erikseen mainittaisikaan hallituksen toimintakertomukseen sisältyvässä arviossa yhtiön riskeistä ja epävarmuustekijöistä.

1.2 Keskeiset käsitteet

1.2.1 Kyberturvallisuus

Kyberturvallisuuden käsite on hankala tieteellisestä näkökulmasta. Toisin kuin monille muille käsitteille tieteessä, sille ei ole yrityksistä huolimatta pystytty antamaan universaalia määritelmää. Kyberturvallisuuden määritelmä vaihtelee kontekstin mukaan ja yleisesti hyväksytyn määritelmän puutteen on esitetty johtuvan kyberturvallisuuden monitieteellisestä luonteesta (Craigen ym., 2014). Tämä aiheuttaa hankaluuksia niin tutkijoille kuin kyberturvallisuuden käytännön toimijoille (Neil ym., 2023). Lisäksi informaatioturvallisuus ja kyberturvallisuus sekoitetaan usein keskenään, vaikka ne eivät ole synonyymeja toisilleen (Azmi & Kautsarina, 2019; R. von Solms & van Niekerk, 2013). Tutkijoilla ei ole yhtenäistä näkemystä kyberturvallisuuden ja informaatioturvallisuuden käsitteiden välistä suhteesta. Osa tutkijoista luokittelee kyberturvallisuuden osaksi

informaatioturvallisuutta (Taherdoost, 2022; B. von Solms & von Solms, 2018) ja osalle tutkijoita kyberturvallisuus on yläkäsite, johon informaatioturvallisuus kuuluu (Galinec & Steingartner, 2017).

Kyberturvallisuuden käsitteen monimutkaisuuden vuoksi Euroopan unionin kyberturvallisuusvirasto (ENISA) on ehdottanut, että kyberturvallisuudelle ei tarvita yksiselitteistä ja kattavaa määritelmää samalla tavalla kuin yksinkertaisimmille käsitteille, kuten käyttäjien autentikointi (ENISA, 2016). ENISAn mukaan kyberturvallisuus on yläkäsite, jolle ei ole mahdollista laatia kaikkia sen näkökulmia universaalisti huomioivaa määritelmää. Sen sijaan kyberturvallisuuden määritelmä ehdotetaan muodostettavan sen kontekstin perusteella, joka sopii kullekin organisaatiolle tai standardeja kehittävälle organisaatiolle (engl. Standardisation Developing Organisation, DSO).

Kyberturvallisuuden konteksti tässä tutkimuksessa on suomalaiset pörssiyhtiöt ja niiden hallitukset. Kyberturvallisuus tulee nähdä osana hallitusten vastuuta toteuttaa ja valvoa yhtiön hallintoa. Tähän kuuluu myös vastuu riskienhallinnan prosessin toteuttamisesta ja johtamisesta. Yritysriskienhallinta on laaja kokonaisuus erilaisia riskejä, johon kuuluvat myös sekä informaatio- että kyberturvallisuus. Yrityksen hallituksen ja ylimmän johdon kontekstissa von Solms & von Solms (2018) ovat määritelleet kyberturvallisuuden seuraavasti:

> *Kyberturvallisuus on osa informaatioturvallisuutta, joka keskittyy erityisesti suojaamaan digitaalisten informaatiovarantojen luottamuksellisuutta, eheyttä ja saatavuutta miltä tahansa uhalta, joka aiheutuu ja vaarantaa informaatiovarannot internetin käytön vuoksi.* (s. 6)

Tässä määritelmässä kyberturvallisuus luetaan osaksi informaatioturvallisuutta ja erityisesti koskemaan niitä uhkia, jotka tulevat internetin käytöstä. Tutkijat itsekin toteavat, että tätä määritelmää tullaan kritisoimaan. Määritelmää voi kritisoida muun muassa siitä, että se ei ota huomioon tuotannollisen toiminnan ohjaukseen käytettäviä niin sanottuja OT-verkkoja (engl. Operational Technology), jotka eivät ole yhteydessä julkiseen internetiin. OT-verkkojen turvallisuudesta huolehtiminen sisältyy usein kuitenkin kyberturvallisuuden konseptiin. Von Solms & von Solms kuitenkin argumentoivat, että tämä määritelmä palvelee tavoitetta yksinkertaistaa kyberturvallisuuden konseptia ylimmälle johdolle ja hallituksille. Vaikka määritelmä on altis kritiikille, on tutkijoiden esittämälle argumentille perusteet. Yritysten hallitusten jäsenten taustat ja osaamiset vaihtelevat, eikä heiltä välttämättä edellytetä tietoteknistä osaamista. Tämän vuoksi tarvitaan yksinkertaistettu määritelmä kyberturvallisuudelle, jotta hallitusten huomio saadaan käännettyä uusiin kyberuhkiin ja niiden hallintaan – vaikka määritelmän puutteet on tunnistettukin.

Yllä esiteltyä von Solms & von Solms (2018) määritelmää edelleen yksinkertaistaen, mutta samalla myös laajentaen tässä tutkimuksessa kyberturvallisuus määritellään yritysturvallisuuden osa-alueeksi, joka keskittyy suojaamaan yrityksen tietojärjestelmiä, tietoverkkoja, laitteita ja niiden käyttäjiä digitaalisessa toimintaympäristössä esiintyviltä uhkilta. Digitaalisella toimintaympäristöllä tarkoitetaan useista toisiinsa kytketyistä järjestelmistä muodostuvaa kokonaisuutta, jossa tietoa ja informaatiota käsitellään digitaalisessa muodossa. Tässä

määritelmässä ei oteta kantaa kyberturvallisuuden ja informaatioturvallisuuden väliseen suhteeseen ja hierarkiaan. Se ei myöskään korosta internetistä tulevia uhkia, vaan rajaa toimintaympäristön kaikkiin digitaalisessa muodossa oleviin ympäristöihin.

1.2.2 Riski

Nobel-palkitun fyysikon Niels Bohrin sanomaksi väitetyn sitaatin mukaan ennustaminen on vaikeaa, varsinkin tulevaisuuden ennustaminen. Tulevaisuuteen liittyy aina epävarmuutta, joka johtuu tietämättömyydestä ja epätietoisuudesta tulevista tapahtumista. Käsitteellä riski tarkoitetaan ennakolta tunnistettua tulevaisuudessa mahdollisesti toteutuvaa tapahtumaa. Useissa määritelmissä riski kuvataan epäedulliseksi ja vaikutuksiltaan negatiiviseksi tapahtumaksi. Kielitoimiston sanakirjassa (*Kielitoimiston sanakirja*, 2022) riski kuvataan menetyksen, tappion tai muun epäedullisen tapahtuman mahdollisuudeksi. Kokonaisturvallisuuden sanastossa (*Kokonaisturvallisuuden sanasto*, 2017) puolestaan riski määritellään kielteisen seikan tai tapahtuman todennäköisyyden ja vaikutuksen yhdistelmäksi.

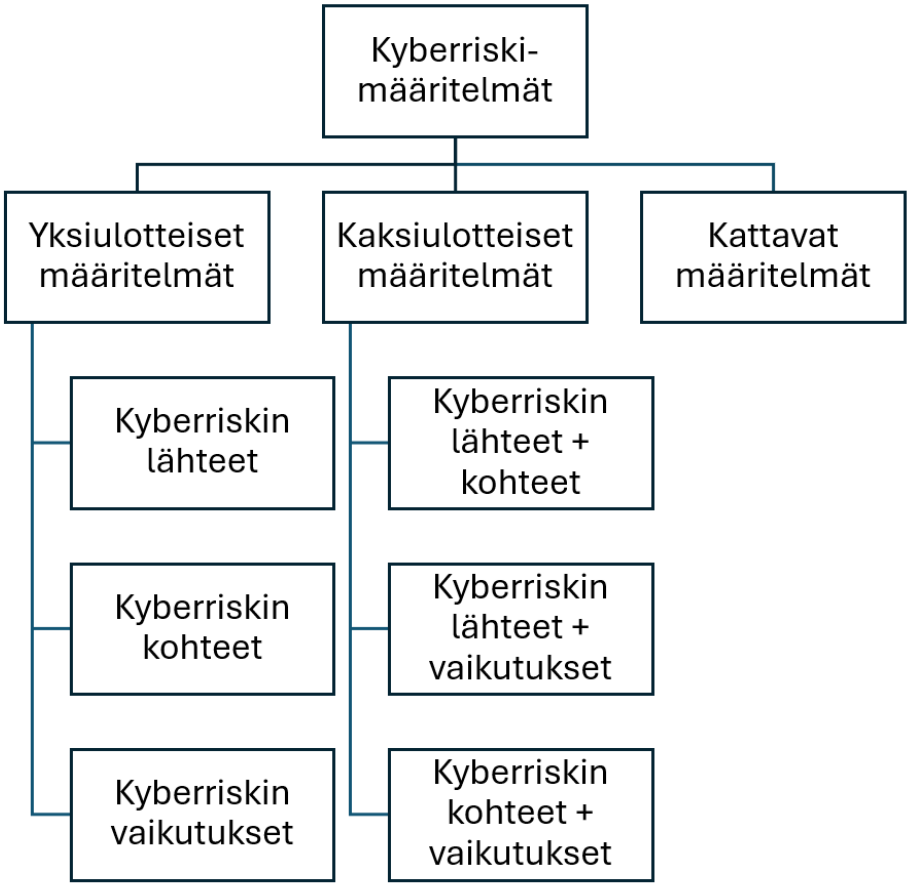
Riskin käsitettä käytetään kaikilla elämänaloilla ja se on käsitteenä läsnä ihmisten arkipäiväisissä keskusteluissa. Kaikki riskeihin liittyvät aspektit olisi mahdotonta käydä läpi tässä tutkimuksessa ja sen vuoksi riskin käsitettä ja olemusta käsitellään yritysten näkökulmasta. Yrityksen toimintaan liittyvät riskit voidaan jakaa riskilähteen mukaan liikeriskeiksi, henkilöriskeiksi, omaisuusriskeiksi, tuoteriskeiksi, tietoriskeiksi, sopimus- ja vastuuriskeiksi, ympäristöriskeiksi ja rikosriskeiksi (Jylhä & Viitala, 2013). Toinen yleisesti käytetty tapa on jaotella riskit strategisiin, operatiivisiin, taloudellisiin ja vahinkoriskeihin. Tämä luokittelu on usein myös käytössä tämän tutkimuksen lähdeaineistona olevissa yritysten vuosiraporteissa. Strategisia riskejä ovat koko yrityksen toimintaan vaikuttavia merkittäviä riskejä, jotka liittyvät yrityksen toimintaympäristöstä tuleviin epävarmuustekijöihin. Operatiivisilla riskeillä tarkoitetaan yrityksen päivittäiseen toimintaan liittyviä toiminnallisia riskejä, jotka voivat olla seurausta riittämättömästi toimivista sisäisistä prosesseista, huonosta johtamisesta, henkilöstön toiminnasta ja ulkoisista tapahtumista. Taloudellisiin riskeihin kuuluvat yrityksen rahaprosessiin ja sopimuksiin liittyvät riskit. Vahinkoriskeihin puolestaan kuuluvat muun muassa työsuojeluun ja -terveyteen liittyvät riskit, ympäristöriskit, kuljetusriskit ja luonnontapahtumariskit (Jylhä & Viitala, 2013). Jylhän ja Viitalan (2013) mukaan vahinkoriskeihin kuuluu myös tietohallintoturvallisuusriski. Tietohallintoon ja tietoturvaan liittyvät riskit nähdään kuitenkin nykyään useammin operatiivisena tai jopa strategisena riskinä kuin vahinkoriskinä.

1.2.3 Kyberriski

Kyberriskissä on muihin yritystoiminnan perinteisiin riskeihin verrattuna omat erityispiirteensä. Kyberriskin käsitteessä yhdistyy kaksi näkökulmaa (Böhme

ym., 2019). Yhtäältä kyberriski on luonteeltaan tekninen riski ja toisaalta se on luonteeltaan taloudellinen riski. Kyberriskin tekninen luonne on seurausta teknisen toteutuksen kompleksisuudesta, (uudelleen)ohjelmoitavista tietoverkkoon kytkettävistä laitteista[2] sekä globaalin internetin muodostamasta dynaamisesta uhka-pinta-alasta. Kyberriskin taloudellisen näkökulman fundamentit puolestaan muodostuvat epätäydellisestä informaatiosta, tekijöiden ja tapahtumien ulkoisvaikutuksista sekä keskinäisriippuvuuksista.

Kyberriskille ei ole olemassa vakiintunutta määritelmää. Määritelmä on elänyt ja kehittynyt vuosien varrella informaatioteknologian ja muuttuneen uhkaympäristön mukaan. Strupczewski (2021) kävi läpi tutkimuksessaan 20 erilaista vuosina 2000-2018 kirjallisuudessa esiintyvää kyberriskin määritelmää. Hän tunnisti kolme kyberriskin määritelmissä esiintyvää komponenttia: kyberriskin lähde, kyberriskin kohde ja kyberriskin vaikutus. Kuviossa 1 on esitetty kyberriskin määritelmien topologia sen mukaan, sisältyykö määritelmään yksi, kaksi tai useampi komponentti. Yhtä määritelmää lukuun ottamatta kaikissa Strupczewskin tutkimukseen sisältyneissä kyberriskin määritelmissä oli mukana yksi tai kaksi edellä mainittua komponenttia.



KUVIO 1 Kyberriskin määritelmien topologia (Strupczewski, 2021, s. 4)

[2] Englanninkielinen alkuperäislähde: (re)programmable behavior of networked components.

Yhdysvaltalainen National Institute of Standards and Technology (NIST) ja kansainvälinen standardoimisliitto International Organization for Standardization (ISO) ovat toimijoita, joiden julkaisemia standardeja ja viitekehyksiä käytetään laajasti kyberturvallisuuden johtamisessa ja hallinnassa. Vaikka nämä standardit ja viitekehykset ovat laajoja kokonaisuuksia, ovat molempien organisaatioiden luomat määritelmät kyberriskille varsin lyhyitä ja tiiviitä. NIST määrittelee kyberriskin riippuvuudeksi kyberresursseista (Ross ym., 2019). NISTin riskimääritelmässä ajurina on riskin lähde, joka muodostuu siitä, että organisaatio on riippuvainen kybertilassa olevista järjestelmistä ja laitteista. ISOn määritelmä riskille tietoturvallisuuden kontekstissa on hyvin yleinen ja lyhyt. Riski määritellään epävarmuuden vaikutukseksi organisaation pyrkimyksissä tavoitteisiinsa (ISO, ei pvm.). Tässä määritelmässä keskiössä on riskin kohde eli organisaation tavoitteet. Yksidimensionaalisen kyberriskin määritelmästä, jossa riskin vaikutus on keskiössä, voidaan käyttää esimerkkinä Nieuwesteeg ym. (2018, s. 3) määritelmää. He määrittelevät kyberriskiksi sellaisen riskin, josta aiheutuu potentiaalisesti fyysistä haittaa ihmisille tai omaisuudelle ja taloudellisia tappioita digitaalisen tietojärjestelmän tai tietojen turmeltumisesta. Toisaalta samassa julkaisussa he myöhemmin (2018, s. 4) kuvaavat kyberriskin osatekijöiksi uhkan, haavoittuvuuden ja vaikutuksen. Nämä tekijät eivät kuitenkaan käy ilmi heidän varsinaisesta kyberriskin määritelmästään. Yksidimensionaalista kyberriskin määritelmää edustaa myös Liikenne- ja viestintävirasto Traficomin (2023) julkaisemassa suosituksessa raideliikenteen kyberturvallisuuden edistämiseksi raideliikenteessä oleva määritelmä. Sen mukaan kyberriski ilmaisee haavoittuvuutta hyödyntävän uhkan, mahdollisten tapahtumien, seurausten ja niiden todennäköisyyksien yhdistelmän. Tässä määritelmässä riskin lähde muodostuu haavoittuvuutta hyödyntävästä uhkasta, mutta se ei ota kantaa riskin kohteeseen tai vaikutukseen.

The Institute of Risk Managementin (IRM) määritelmässä (The Institute of Risk Management, 2014) korostuvat riskin lähde ja riskin vaikutus. IRM:n määritelmän mukaan organisaation kyberriskejä ovat kaikki sen tietojärjestelmien virhetilanteista syntyvät riskit, joiden seurauksena voi olla taloudellisia menetyksiä, keskeytyksiä ja mainehaittaa organisaatiolle. Mukhopadhyay ym. (2013) määritelmän mukaan kyberriski on riski, joka liittyy ilkeämieliseen digitaaliseen tapahtumaan, joka aiheuttaa häiriöitä ja taloudellisia menetyksiä. G20-järjestöön kuuluva toimielimen Financial Stability Boardin (FSB) tehtävänä on tutkia ja antaa suosituksia kansainvälisen finanssijärjestelmän säätelemiseksi. FSB:n julkaisemassa kybersanastossa kyberriski määritellään lyhyesti kyberhäiriön (engl. incident) todennäköisyyden ja vaikutuksen yhdistelmäksi (Financial Stability Board, 2023).

Edellä on kuvattu useita eri lähteissä mainittuja määritelmiä kyberriskille. Kuvaus ei ole kattava ja kyberriskin määritelmiä on edellisten lisäksi paljon lisää. Määritelmissä on samoja piirteitä, mutta niissä näkyy myös se konteksti, johon ne on laadittu. Kun kyseessä on toimija, jonka näkökulma kyberturvallisuuteen on tekninen, on luonnollista, että kyberriskin määritelmässä on mukana tekninen aspekti. Samoin jos kyberriski on määritelty organisaatiossa, jonka

kosketuspinta kyberturvallisuuteen jää korkealla abstraktion tasolle, on kyberriskin määritelmä vastaavasti yleinen ja abstrakti. Useat tässä luvussa esitellyistä määritelmistä ovat vakuutustieteen alalta, jolloin on luontevaa, että niissä on mukana myös taloudellisia menetyksiä korostava painotus.

Kyberriskillä tarkoitetaan tässä tutkimuksessa yrityksen digitaalisesta toimintaympäristöstä aiheutuvia riskejä ja epävarmuustekijöitä. Kyberriskien keskeinen lähde on yrityksen ulkopuolisten toimijoiden aiheuttama haitta yrityksen toiminnan jatkuvuudelle, maineelle ja taloudelle. Kyberriskit kattavat myös tietoturvaan liittyvät uhkat digitaalisessa toimintaympäristössä. Tietojärjestelmien tai vastaavien vikaantumista tai uusien tietojärjestelmien käyttöönottoa ei pidetä kyberriskinä.

1.3 Tutkimuksen rakenne

Tutkielma koostuu kuudesta pääluvusta. Johdantoluvussa kuvataan tutkimuksen tavoite ja tutkimuskysymys sekä määritellään tutkimukseen liittyvät peruskäsitteet. Johdantoluvun jälkeen toisessa luvussa on kirjallisuuskatsaus, jossa käsitellään tähän tutkimukseen liittyvä aiempi relevantti tutkimus, tutkimusaineistoon liittyvää normipohjaa ja vapaaehtoisen riskien raportoinnin teorioita. Kirjallisuuskatsauksessa kuvataan, mitä tutkittavasta ilmiöistä jo tiedetään. Tutkimusaineistona on listattujen yhtiöiden julkaisemat vuosiraportit, joiden sisältöä ja muotoa ohjaavat lainsäädäntö ja muut ohjeet. Näiden käsittely riittävässä laajuudessa on edellytys aineistosta tehtävillä tulkinnoille ja johtopäätöksille. Kolmannessa luvussa esitetään tutkimuksen aineiston keräämis-, käsittely- ja analysointimenetelmät sekä arvioidaan tutkimuksen luotettavuutta. Neljännessä luvussa käydään läpi tutkimustulokset ja viidennessä luvussa esitetään tutkimustuloksista johdetut johtopäätökset. Tutkimusraportin päättävässä kuudennessa luvussa pohditaan tutkimustulosten merkityksellisyyttä, tutkimukseen liittyviä rajoitteita ja mahdollisia jatkotutkimuskohteita.

2 KIRJALLISUUSKATSAUS

Kirjallisuuskatsauksen päämääränä on asemoida tutkimus suhteessa laajempaan kirjallisuuteen ja aiemmin tehtyyn tutkimukseen (Ketokivi, 2015). Lisäksi empiirinen tarkastelu edellyttää, että argumenttien sisältämät käsitteet sekä määritellään että operationalisoidaan (Ketokivi, 2015). Edellisessä luvussa kuvattiin ja määriteltiin tutkimuksen kannalta keskeiset teoreettiset käsitteet ja luotiin kuva tutkittavasta ilmiöstä ja tutkimuskohteesta. Tässä luvussa käsiteltävä aiempi tutkimus ja kirjallisuus muodostavat pohjan, joka perustelee ja motivoi tämän tutkimuksen tarpeellisuutta. Määritellyt käsitteet ja aiemman tutkimuksen riittävän laaja läpikäynti ovat myös tärkeitä tutkimuksen tuloksen analysoinnissa, oikeiden päätelmien muodostamisessa ja kontribuutiota lisäävien tulosten tunnistamisessa.

Keskeinen kirjallisuus tässä tutkimuksessa muodostuu suomalaisia pörssilistattujen yhtiöiden raportointivelvollisuutta säätelevästä lainsäädännöstä ja muusta ohjeistuksesta, keskeisimpiä käsitteitä määrittelevästä kirjallisuudesta ja tutkimuksen aihepiiriin liittyvästä aiemmasta tutkimuksesta. Käsitteiden määrittelyn ja kirjallisuuskatsauksen pohjana olleet julkaisut on haettu Google Scholar, Scopus tai Jyväskylän yliopiston JYKDOK-palveluista. Lisäksi aineistona on käytetty tutkimuksen menetelmäoppaita, viranomaisjulkaisuja ja ammattikirjallisuutta. Lähteenä käytettyjen tieteellisten tutkimusten laatua on arvioitu Julkaisufoorumin[3] luokitusjärjestelmän perusteella ja vähintään tason 1 saavuttaneet julkaisukanavat on asetettu etusijalle.

2.1 Listattujen yhtiöiden raportointivelvollisuudet

Tässä luvussa kuvataan ne keskeiset periaatteet ja velvoitteet, joita pörssilistatulla yhtiöllä on koskien taloudellisen ja muun informaation julkistamista. Tutkimuksen empiirisenä aineistona on pörssiyhtiöiden vuosiraportit, joten tarkas-

[3] https://julkaisufoorumi.fi/fi

telu rajataan koskemaan sitä lainsäädäntöä, säädöksiä ja ohjeita, jotka ovat olennaisia tutkimusongelman kannalta. Suomessa toimivia yhtiöitä velvoittavat tässä luvussa esiteltyjen lakien ja normien lisäksi muu Suomen ja EU:n lainsäädäntö. Esimerkiksi kaikki pörssiyhtiöt ovat osakeyhtiöitä, joita koskee osakeyhtiölaki. Vaikka osakeyhtiölaki sisältää määräyksiä yhtiön julkistaman toimintakertomuksen sisällöstä, ei osakeyhtiölaissa ole määrätty yhtiötä koskevien riskien raportoinnista. Tämän vuoksi osakeyhtiölain käsittely tässä luvussa ei ole tarpeen tutkimuksen näkökulmasta.

Toimijoita, joiden liikkeelle laskemilla arvopapereilla käydään kauppaa säännellyllä markkinalla, koskee laaja tiedonantovelvollisuus (Finanssivalvonta, 2021). Tiedonantovelvollisuuden tarkoituksena on turvata eri sidosryhmien yhdenvertainen, tasapuolinen ja samanaikainen mahdollisuus tiedon saantiin. Liikkeellelaskijoiden sidosryhmiä ovat muun muassa sijoittajat, rahoittajat ja viranomaiset. Tiedonantovelvollisuus on sekä säännöllistä että jatkuvaa. Arvopaperin liikkeellelaskijaa koskevat velvollisuudet perustuvat arvopaperimarkkinalakiin, markkinoiden väärinkäyttöasetukseen ja kauppapaikan sääntöihin. Säännöllisellä tiedonantovelvollisuudella tarkoitetaan muun muassa tietoja, jotka koskevat liikkeellelaskijan taloudellista asemaa ja tulosta. Arvopaperimarkkinalain mukaan liikkeellelaskijan on julkistettava tilinpäätös ja toimintakertomus sekä puolivuosikatsaus. Laki ei edellytä vuosineljänneksittäin annettavaa raportointia liikkeellelaskijalta, mutta osavuosikatsausten antaminen on vakiintunut tapa. Jatkuvan tiedonantovelvollisuuden piiriin kuuluu liikkeellelaskijan jatkuvasti ja ajantasaisesti markkinoille julkaisemia tietoja. Siihen kuuluu ennen kaikkea sisäpiiritiedon julkistaminen sekä muiden sääntelyjen edellyttämien tietojen julkaiseminen. Tämän tutkimuksen kohteena ovat liikkeellelaskijat, joiden osakkeilla käydään kauppaa säännellyllä markkinapaikalla Suomessa. Näistä toimijoista käytetään nimitystä listayhtiö, pörssiyhtiö tai pörssilistattu yhtiö. Suomessa säännellyn markkinan ylläpitäjänä toimii Nasdaq Helsinki Oy (Helsingin pörssi).

Pörssilistattuja yhtiöiden taloudellinen raportointi tehdään kansainvälisen tilinpäätösstandardin (International Financial Reporting Standards, IFRS) mukaisesti, jonka velvoittavuus tulee Euroopan komission antamasta asetuksesta (Finanssivalvonta, 2018). Lisäksi yhtiöt joutuvat noudattamaan Suomen lainsäädäntöä, muita viranomaisten ohjeita ja niin sanottua hyvää hallintotapaa. Tämän tutkimuksen kannalta keskeinen laki on Suomen kirjanpitolaki, jonka mukaan kirjanpitovelvollinen, joka on julkinen osakeyhtiö, on velvollinen laatimaan toimintakertomuksen (Kirjanpitolaki 1336/1997, 3 luku 1 §). Kirjanpitolain 3. luvun 1 a §:n mukaan toimintakertomuksessa on kuvattava kirjanpitovelvollisen 1) toiminnan kehittymistä 2) taloudellista tilannetta; sekä 3) *merkittävimpiä riskejä ja epävarmuustekijöitä*. Toimintakertomukseen sisällytetään taloudellisia ja muita kuin taloudellisia tunnuslukuja henkilöstöstä ja ympäristövaikutuksista silloin, kun se on tarpeen kuvauksen ymmärtämiseksi. Edellisen lisäksi toimintakertomuksessa on muun muassa esitettävä tiedot olennaisista tapahtumista tilikauden päättymisen jälkeen ja arvio kirjanpitovelvollisen todennäköisesti tulevasta kehityksestä. Vaikka kirjanpitolaki koskee suurelta osin

taloudellisen informaation esittämistä ja raportointia, tarjoaa lain vaatimus toimintakertomuksesta mahdollisuuden saada myös muuta informaatiota kirjanpitovelvollisista. Tämän tutkimuksen tutkimuskysymyksen kannalta merkityksellisen aineiston muodostavat listayhtiöiden toimintakertomuksissa olevat kuvaukset merkittävimmistä riskeistä ja epävarmuustekijöistä.

Toimintakertomuksen laadintaa ohjaa myös työ- ja elinkeinoministeriön alaisuudessa toimivan kirjanpitolautakunnan yleisohje toimintakertomuksen laadinnasta. Kirjanpitolautakunta on kirjanpitolaissa (Kirjanpitolaki 1336/1997, 8 luku 2 § ja 3 §) määrätty toimielin, jonka tarkoituksena on antaa ohjeita ja lausuntoja kirjanpitolain noudattamisesta ja soveltamisesta. Toimintakertomuksen laadinnasta annetun ohjeen mukaan toimintakertomus on vapaamuotoinen asiakirja, jonka tulee esittää laissa ja muissa säännöksissä edellytetyt tiedot (Kirjanpitolautakunta, 2006). Kirjanpitolautakunta katsoo, että toimintakertomus tulee suunnata tulevaisuuteen ja sen tulee kuvata niitä kehityssuuntia, jotka ovat merkityksellisiä kirjanpitovelvollisen nykyisen ja tulevan toiminnan arvioimiseksi pitkän tähtäyksen tavoitteiden toteutumisen kannalta. Kun toimintakertomuksessa esitetään arvioita päättyneeltä tilikauden tuloksen merkityksellisyydestä tulevan kehityksen kannalta, liittyy arvioihin aina epävarmuus tulevasta. Tämän vuoksi tulevia riskejä ja mahdollisuuksia tulisi kuvata tasapainoisesti, jotta kirjanpitovelvollisen sidosryhmät voivat punnita yritysjohdon julkistamien toimintasuunnitelmien tarkoituksenmukaisuutta riskien ja mahdollisuuksien kannalta. Toimintakertomuksen laadintaohje ottaa myös kantaa siihen, että tulevan kehityksen yksityiskohtainen julkistaminen ei ole välttämättä perusteltua liikesalaisuuksien varjelemisen kannalta.

Kirjanpitolautakunnan (2006) antamassa yleisohjeessa kuvataan myös toimintakertomuksen laadintaperiaatteet. Yleisohjeen mukaan kirjanpitolain yleiset periaatteet koskevat myös toimintakertomusta. Yleisten periaatteiden mukaan toimintakertomukseen sisällytetään olennaiset tiedot. Olennaisuutta arvioidaan aina tapaus- ja tilannesidonnaisesti. Lisäksi toimintakertomuksen laadinnassa täytyy noudattaa johdonmukaisuutta, jolla tavoitellaan toimintakertomusten vertailtavuutta niin eri vuosien kuin muiden yhtiöiden kesken. Jatkuvuuden näkökulmasta kirjanpitolautakunnan mukaan merkityksellistä on myös se, mitä yksittäisestä seikasta tai olosuhteista on aiemmin esitetty. Toimintakertomuksen laadinnassa on myös noudatettava varovaisuusperiaatetta, joka liittyy tiedon luotettavuuteen. Koska toimintakertomus suuntaa tulevaisuuteen, liittyy siihen väistämättä epävarmuutta. Toimintakertomuksen luotettavuutta voidaan edesauttaa perustelemalla päätelmät tunnistettaviin ja todennettaviin seikkoihin sekä erottamalla selkeästi tosistaan tosiasiat, odotukset ja tulkinnat.

Toimintakertomuksen laadinnasta annetun yleisohjeen luvussa 2.7. (Kirjanpitolautakunta, 2006) kirjanpitolautakunta kuvaa kirjanpitolain tarkoittamaa toimintakertomukseen sisältyvää arviota kirjanpitovelvollisen esittämistä riskeistä ja epävarmuustekijöistä. Riskien ja muiden epävarmuustekijöiden todetaan olevan riippuvainen yrityksen toimialasta, mutta toimialasta riippumatta kirjanpitovelvollisen toimintaan katsotaan yleisesti vaikuttavan strategiset riskit,

operatiiviset riskit, rahoitusriskit ja vahinkoriskit. Yleisohjeessa on lueteltu esimerkinomaisesti erityyppisiä riskejä, mutta luettelo ei ole tarkoitettu kattavaksi ja niitä ei ole tarkoitettu käytettäväksi sellaisenaan, vaan kunkin yrityksen on arvioitava toimintaansa liittyviä riskejä ja epävarmuustekijöitä muun muassa oman toimialansa ja toiminnan laajuudesta katsottuna (Kirjanpitolautakunta, 2006). Yleisohjeessa ei suoraan mainita tietoturvaan tai kyberturvallisuuteen liittyviä riskejä, mutta yleisohjeen liitteessä 5 on esitetty esimerkkejä riskeistä. Strategisia ja operatiivisia riskejä kuvaavissa esimerkeissä on yksi kohta, joka nykyisin todennäköisesti sanoitettaisiin enemmän kyberturvallisuuden vakiintunein termein:

> *Konsernin liiketoiminta perustuu toimiville ja luotettaville tietojärjestelmille. Niihin liittyviä riskejä pyritään hallitsemaan mm. kahdentamalla kriittiset tietojärjestelmät ja tietoliikenneyhteydet, kiinnittämällä huomiota yhteistyökumppaneiden valintaan sekä standardoimalla käytössä olevia työasemamalleja ja ohjelmistoja sekä tietoturvaan liittyviä menettelytapoja.* (*Kirjanpitolautakunta, 2006, s. 55)*

Edellisen lisäksi toimintakertomukseen sisältyvistä riskeistä ja epävarmuustekijöistä on mainittu esimerkkeinä muun muassa poliittisten ja lainsäädännöllisten muutoksien vaikutus Suomen ulkopuolisten investointien arvoon sekä logististen järjestelmien muutoksesta aiheutuvat toiminnalliset häiriöt (Kirjanpitolautakunta, 2006). Yleisohje on laadittu vuonna 2006, jolloin kyberturvallisuuden näkökulmasta yritysten toimintaympäristö oli vielä hyvin erilainen. Nykyisin tietojärjestelmillä ja tietoverkoilla on suurempi rooli kuin lähes kaksikymmentä vuotta sitten yleisohjeen julkaisuajankohtana. Useille yrityksille tietojärjestelmien turvallinen ja luotettava toiminta on jopa kriittisen tärkeää. Lisäksi Suomessa ja maailmalla on ollut kyberturvallisuuteen liittyviä esimerkkitapauksia, joilla on merkittävä tai jopa katastrofaalinen vaikutus yrityksen toimintaan. Sen vuoksi tietoturvaan ja kyberturvallisuuteen liittyvien riskien esittäminen toimintakertomuksessa on perusteltua.

2.2 Tieteelliset teoriat vapaaehtoisen riskiraportoinnin taustalla

Liiketoiminnan riskejä ja epävarmuuksia kuvaava osio on pakollinen osa hallituksen toimintakertomusta, mutta hallituksella on harkintavalta julkaistavien riskien ja epävarmuuksien kuvaamisessa. Tieteellisessä tutkimuksessa on johdon motivaatioita ja ajureita vapaaehtoista riskiraportointia kohtaan kuvattu ja selitetty useilla eri teorioilla. Tässä luvussa käydään läpi signalointiteoria ja legitimiteettiteoria. Näiden teorioiden rooli tutkimuksessa on ohjaava, ja ne tukevat aineistosta tehtyä analyysia ja johtopäätöksiä.

Spence (1973) kuvasi työmarkkinoihin liittyvässä tutkimuksessaan signalointiteorian avulla työnantajan ja työnhakijan välistä epäsymmetristä informaatiota tilanteessa, jossa osapuolet eivät tunne toisiaan. Työnhakijalla on ominaisuuksia, joihin hän ei voi vaikuttaa, kuten sukupuoli, ja ominaisuuksia, joi-

hin hän voi vaikuttaa. Ominaisuuksia, joihin työnhakijan on mahdollista vaikuttaa Spence nimittää *signaaleiksi* ja esimerkkinä hän mainitsee koulutukseen. Työnhakija signaloi koulutuksellaan osaamistaan työnantajalle, eli *signaalin vastaanottajalle*, ja työntekijän on mahdollista, ainakin pidemmällä aikavälillä, kouluttautua lisää. Koulutukseen käytettyä aikaa ja rahaa Spence nimittää *signalointikustannukseksi*. Signalointiteoriaa on myöhemmin sovellettu laajasti eri tieteenaloilla (Connelly ym., 2011) ja se soveltuu myös kyberturvallisuuden kontekstiin. Signalointiteorian keskiössä on epäsymmetrinen informaatio, jonka ajatellaan tasoittuvan signaloinnin myötä (Morris, 1987). Esimerkiksi organisaation hankkimaa ISO27001-sertifiointia voidaan selittää signalointiteorian avulla. Sertifioinnilla organisaatio signaloi omaa tietoturvaprosessiaan ja sen tasoa hankkimalla yleisesti tunnustetun sertifioinnin. Organisaation sidosryhmillä ei ole käytössään täydellistä kuvaa organisaation tietoturvan tasosta, mutta sertifioinnin avulla tämä epäsymmetria pienenee. Sertifioinnin hankintaan liittyneet kustannukset voidaan katsoa organisaation signalointikustannuksiksi. Kyberriskien raportoinnin tapauksessa organisaatio signaloi sidosryhmilleen ja mahdollisesti myös kyberturvallisuutta uhkaaville tahoille tunnistaneensa kyberturvallisuuteen liittyviä riskejä ja varautuneensa niihin. Toimiva signalointi edellyttää, että signaali ei ole helposti muiden kopioitavissa ja sitä, että signalointi edustaa organisaation todellista laatua (Morris, 1987).

Legitimiteettiteoria selittää organisaatiota osana sosiaalista järjestelmää ja sopimusta, jossa organisaation olemassaolon peruste ja toiminnan oikeutus tulevat organisaation ulkopuolelta saatavasta tuesta ja hyväksynnästä (Tieteen termipankki, 2016). Suchman (1995, s. 574) on määritellyt legitimiteetin seuraavasti:

> Legitimiteetti on yleistetty näkemys tai oletus, joka tekee entiteetin toimet toivottavaksi, asianmukaisiksi ja soveltuviksi normeista, arvoista, uskomuksista ja määritelmistä rakentuvassa sosiaalisessa järjestelmässä.

Organisaation legitimiteettiä voidaan tarkastella strategisesta ja institutionaalisesta näkökulmasta. Strategisen legitimiteetin lähestymistapa korostaa toimintatapoja, joita organisaatio käyttää instrumentaalisesti yhteisön tuen saamiseksi. Institutionaalinen lähestymistapa puolestaan painottaa organisaation ulkopuolelta tulevaa kulttuurista painetta, jonka seurauksena organisaatio joutuu muuttamaan toimintaansa saadakseen sosiaalista hyväksyntää (Suchman, 1995). Näkökulmien ero on siinä, että muuttaako organisaatio toimintaansa omaehtoisesti tavoitellakseen sosiaalisen hyväksynnän mukanaan tuomia hyötyjä ja etuja vai johtuuko organisaation toiminta muun yhteiskunnan organisaatioille asettamista paineista. Institutionaaliseen legitimiteettiin liittyy myös organisaatioiden yhdenmukaistuminen eli isomorfismi. Alasoini (2016) esittää, että organisaatioiden yhdenmukaistumisen taustalla voi olla taloudellisen rationaliteetin lisäksi myös organisaatioiden pyrkimys saada institutionaalista legitimiteettiä. Isomorfismilla tarkoitetaan prosessia, jossa organisaatioiden toimintamallit ja prosessit alkavat muistuttaa toisiaan toimialasta ja sektorista riippumatta (Mänttäri-van der Kuip ym., 2018). Organisaatioiden yhdenmukaistumisen

taustalla on DiMaggion & Powellin (1983) mukaan kolme päämekanismia: 1) organisaatioiden yhdenmukaistuminen tapahtuu pakottavasta isomorfismista (engl. coercive isomorfism), joka johtuu yhteisön kulttuuristen odotusten ja muiden organisaatioiden, joista organisaatio on riippuvainen, asettamista muodollisista ja epämuodollisista paineista. Pakottavaa isomorfismia ovat esimerkiksi lainsäädäntö, toimintojen luvanvaraisuus ja yritysten raportointivelvollisuudet. 2) Organisaatioiden yhdenmukaistuminen voi tapahtua jäljittelemällä (engl. mimetic isomorfism), joka voi olla epävarmassa tilanteessa organisaatiolle edullinen toimintapa. Yhdenmukaistuminen jäljittelemällä voi tapahtua tahattomasti esimerkiksi työntekijöiden liikkuvuuden kautta, kun aiemmassa organisaatiossa sovellettuja toimintamalleja viedään uuteen organisaatioon, tai tietoisesta kopioimalla. Kyber- ja informaatioturvallisuudessa jäljittelemällä tapahtuvaa organisaatioiden isomorfismia edustavat niin sanotut parhaat käytännöt (engl. best practices), joiden avulla organisaatiot yrittävät muuttaa toimintaansa vastaamaan muiden organisaatioiden laajasti käyttämiksi esitettyjä toimintatapoja. Informaatioturvallisuuden hallinnassa jäljittelevä isomorfismi ja parhaiden käytäntöjen soveltaminen on kuitenkin saanut myös kritiikkiä (katso esim. Siponen & Willison, 2009). 3) Kolmas organisaatioiden yhdenmukaistumisen päämekanismi liittyy eri ammattiryhmien muodostamien kollektiivien normatiivisiin työskentely- ja muihin käytäntöihin (engl. normative isomorfism). Tällaisia normatiivisia käytäntöjä on laajasti esimerkiksi lääkäreillä, lakimiehillä ja tilintarkastajilla.

Legitimiteettiteoriaa on käytetty paljon taloustieteellisessä tutkimuksessa, joissa on tutkittu yritysten ympäristöön ja sosiaalisiin näkökulmiin liittyvien vapaaehtoisten tietojen julkaisemista (katso esim. Campbell, 2003; Hummel & Schlick, 2016; Magness, 2006). Kyberturvallisuuteen tai riskien raportointiin ja julkaisuun liittyvää tutkimusta, joissa olisi käytetty legitimiteettiteoriaa, ei tämän tutkimuksen kirjallisuuskatsauksen yhteydessä onnistuttu löytämään. Se ei kuitenkaan poissulje, etteikö legitimiteettiteorian näkökulmia voisi soveltaa myös kyberturvallisuusriskien analysointiin. Tässä tutkimuksessa empiirinen aineisto muodostuu suomalaisten pörssiyhtiöiden hallitusten vuosikertomuksiin sisätyvien kyber- ja tietoriskiarvioiden analyysista. Vaikka hallituksen esittämä näkemys riskeistä ja epävarmuustekijöistä on lain edellyttämä velvoite, ei laissa määritellä arvion sisältöä. Legitimiteettiteoria tarjoaa yhden viitekehyksen näiden vapaaehtoisten riskiarvioiden analysointiin.

2.3 Kyberturvallisuusinformaation julkaisusta tehty aiempi tutkimus

Tässä luvussa esitellään tämän tutkimuksen kannalta keskeinen aiemmin tehty tutkimus. Lukuun on sisällytetty tutkimuskysymyksen kannalta olennaisia tutkimuksia, jotka käsittelevät pörssiyhtiöiden julkaisemaan kyberturvallisuuteen liittyvää informaatiota osana markkinoille jaettavaa tietoa. Englanninkielisessä

kirjallisuudessa julkaisuun viitataan sanalla *disclosure.* On syytä painottaa, että käsitteellä viitataan tässä yhteydessä yksinomaan pörssiyhtiön julkiseksi saattamaa informaatiota, joka liittyy yhtiön toimintaan julkisesti noteerattuna yhtiönä. Kyber- ja tietoturvallisuutta käsittelevässä kirjallisuudessa termillä *disclosure* viitataan myös muun muassa ohjelmistoista löytyneiden haavoittuvuuksien julkaisuun (katso esim. Mitra & Ransbotham, 2015).

Listattujen yhtiöiden kyberriskien raportoinneista on tehty aiempaa tutkimusta ulkomailla, mutta suomalaisten pörssiyhtiöiden raportoimia kyberriskejä ja -uhkia ei ole tämän tutkimuksen näkökulmasta aiemmin tutkittu. Tutkimusmahdollisuuksiin vaikuttaa paljon paikallinen lainsäädäntö ja muu sääntely. Yhdysvalloissa pörssilistattujen yhtiöiden raportointia ohjaa Securities and Exchange Commission (SEC), joka on julkaissut vuosina 2011 ja 2018 kyberturvallisuutta koskevat raportointiohjeet pörssilistatuille yhtiöille. Gaon ym. (2020) tutkimuksessa *Public Companies' cybersecurity risk disclosures* selvitettiin yhdysvaltalaisten yhtiöiden raportoimia kyberriskejä määrällisin menetelmin. Tutkimuksen aineistona oli niin sanotut 10-K-raportit, jotka ovat osa yhdysvaltalaisilta listayhtiöiltä vaadittuja tietoja. Tutkimuksen tavoitteena oli selvittää raportoitujen kyberriskien sisältöä, sijaintia, käytettyä kieltä ja kyberriskien raportoinnin muutoksiin vaikuttaneita tekijöitä. Tutkimus on vahvasti sidottu yhdysvaltalaiseen sääntelyyn ja sen tutkimusasetelma ei sellaisenaan sovellu tässä tutkimuksessa sovellettavaksi. Työssä on kuitenkin muutamia menetelmällisiä valintoja, joiden soveltaminen suomalaiseen aineistoon on mahdollista. Esimerkiksi tutkijat käyttivät sanojen lukumäärää muuttajana sille, missä laajuudessa kyberriskejä oli raportoitu.

Eijkelenboom & Nieuwesteeg (2021) tutkivat alankomaalaisten yritysten kyberturvallisuuteen liittyvien tietojen raportointia yritysten vuosiraporteissa. Heidän tutkimuksensa on relevantti myös tämän tutkimuksen kannalta. Hollantialaisia yrityksiä koskee sama kansainvälinen tilinpäätösstandardi (International Financial Reporting Standard, IFRS) kuin suomalaisia. Lisäksi heidän empiirisenä aineistonansa toimi yhtiöiden vuosiraportit samoin kuin tässä tutkimuksessa. Suomesta poiketen Alankomaissa yhtiöillä ei ole kuitenkaan eksplisiittistä velvollisuutta raportoida näkemystä yhtiön merkittävistä riskeistä ja epävarmuustekijöistä. Tästä huolimatta Eijkelenboom & Nieuwesteeg mukaan 87 % alankomaalaisista listayhtiöistä mainitsi kyberturvallisuuden vuosiraporteissaan, jota voi pitää verrattain korkeana lukuna. Heidän toisena tutkimushypoteesina oli, että NIS-direktiivin piirin kuuluvat yhtiöt raportoivat vuosiraporteissaan laajemmin kyberturvallisuudesta kuin ne yhtiöt, joita NIS-direktiivi ei koske. Tätä hypoteesia he eivät pystyneet tutkimuksessaan vahvistamaan.

Ramírez ym. (2022) toteuttivat pitkittäistutkimuksen, jossa he selvittivät Latinalaisen Amerikan pörssilistattujen yhtiöiden kyberturvallisuudesta julkaistuja tietoja vuosien 2016–2020 vuosiraporteissa. Tutkimuksessaan he loivat uuden mittarin, *Cybersecurity Disclosure Indexin (CDI)*, jonka avulla tutkimuksen kohteena olleiden yhtiöiden kyberturvallisuuteen liittyvien tietojen julkaiseminen pisteytettiin. Mittarissa oli neljä kyberturvallisuuteen liittyvää ulottuvuutta: hallinto ja johtaminen, strategia, riskienhallinta ja taloudelliset vaikutukset.

Kunkin ulottuvuuden alla oli 3–13 kyberturvallisuuteen liittyvää väittämää, joiden toteutumista julkaistuissa vuosiraporteissa arvioitiin kullekin tutkimuksen otoksessa mukana olleelle yhtiölle. Jos väittämä toteutui, sai tästä väittämästä yhden pisteen. Mittarin kokonaisarvosana laskettiin väittämistä saadut pisteet yhteen ja jakamalla se väittämien lukumäärällä. Näin ollen kaikkien väittämien toteutuessa indeksin lopputulos oli 1 (100 %) ja vastaavasti jos yksikään väittämä ei toteutunut, muodostui indeksi arvoksi 0 (0 %). Tutkimuksen tuloksena havaittiin, että kyberturvallisuutta koskevat tiedot pörssiyhtiöiden vuosijulkaisuissa kasvaa tarkastelujaksolla tasaisesti, mutta keskimääräinen indeksiluku ei ylitä 40 %. Maittain tarkasteltuna indeksi kasvoi eniten Chilessä ja Meksikossa. Toimialoittain tarkasteltuna finanssisektori erottautui muista toimialoista. Finanssisektorilla indeksi oli jo tarkastelun aloitusvuonna 2016 muita selkeästi korkeampi ja se pysyi muita toimialoja selkeästi korkeammalla tasolla, vaikka muutkin toimialat yli kaksinkertaistivat keskimääräisen indeksilukunsa tarkastelun päättymisvuoteen 2020 mennessä.

Kanadalaisten pörssiyhtiöiden kyberturvallisuuteen liittyvien tietojen julkaisua käsitellyt tutkimus (Héroux & Fortin, 2020) selvitti sisällönanalyysin menetelmillä julkaistujen tietojen sisältöä vuosiraporteissa, osavuosikatsauksissa ja tiedotteissa. Tutkimuksen kohteena oli Toronton pörssin S&P/TSX 60 -indeksiin kuuluvat 60 suuryritystä. Tutkimuksessa muodostettiin 40 kohdan arviointikriteeristö Kanadan ja Yhdysvaltojen arvopaperimarkkinoita valvovien viranomaisten informaation julkaisemista koskevien ohjeiden pohjalta. Arviointikriteeristö käsitti teemoja kyberriskin määritelmästä, mahdollisten kyberturvallisuustapahtumien (engl. cybersecurity incident) vaikutuksesta, kyberturvallisuusstrategian omistajuudesta yrityksessä, kyberriskienhallinnasta, potentiaalista kyberturvallisuustapahtumista, toteutuneista kyberturvallisuustapahtumista ja muista kyberturvallisuuteen liittyvistä tiedoista. Tutkijoiden mukaan tämä kriteeristö edusti kyberturvallisuusinformaation julkaisun niin sanottuja parhaita käytäntöjä (engl. best practices), joita tutkimuksessa verrattiin todellisiin ja havaittuihin käytäntöihin. Tutkimuksen aineistona olleet dokumentit koodattiin tätä arviointikriteeristöä käyttäen ja koodien esiintymistiheydet taulukoitiin. Esiintymistiheyksien lisäksi tutkimusraportissa analysoitiin laadullisesti julkaistujen tietojen sisältöä ja aineistosta nostettiin kuvaavia sitaatteja tukemaan analyysia. Tutkimuksen johtopäätöksenä esitetään, että kyberturvallisuuteen liittyvän informaation julkaisutiheys on matala. Lisäksi julkaistujen tietojen yksityiskohtien määrässä on vaihtelua ja usein julkaistu informaatio on luonteeltaan yleistä ja vähäisessä määrin yrityskohtaista. Tutkimuksessa havaittiin myös, että vuosiraporteissa julkaistua informaatio kierrätetään uudelleen sellaisenaan muissa myöhemmin julkaistuissa dokumenteissa. Lisäksi tuloksissa painotettiin, että kyberturvallisuusinformaation julkaisussa tapahtuvien muutosten tunnistamiseksi tarvittaisiin pitkittäistutkimusta ja keskeiseksi jatkotutkimuskohteeksi nostettiin kyberturvallisuusinformaation julkaisua määrittävien tekijöiden selvittämistä.

Héroux & Fortin (2022) jatkoivat kanadalaisten pörssiyhtiöiden kyberturvallisuuteen liittyvän informaation julkaisemisen tutkimista aiemmassa (2020)

tutkimuksessaan laadittua arviointikriteeristö hyödyntäen. Tutkittava perusjoukko oli Toronton pörssin S&P/TST Composite Indexiin kuuluvat 250 yhtiötä ja aineistona näiden yhtiöiden vuosiraportit. Tutkimuksen tavoitteena oli selvittää yritysten hallitusten kokoonpanon vaikutusta kyberturvallisuusinformaation julkaisuun upper echelon -teorian ja signalointiteorian viitekehyksessä. Hallitusten kokoonpanon vaikutusta tutkittiin regressiomallin avulla, jossa selittävinä muuttujina olivat hallituksen jäsenten IT-osaaminen (%-osuus hallituksen jäsenistä, joilla oli IT-alan koulutus tai työkokemusta), hallituksen jäsenten toimivuodet hallituksessa (kaikkien jäsenten keskiarvo), hallituksen riippumattomuus[4] (%-osuus hallituksen jäsenistä), naisten osuus hallituksessa (%-osuus hallituksen jäsenistä), hallituksen jäsenten keskimääräinen ikä, erillisen kyber- ja tietoturva-asioihin keskittyvän toimielimen olemassaolo (binäärinen muuttuja, joka saa arvon 1 jos kyseinen toimielin on organisaatiossa, muussa tapauksessa muuttuja saa arvon 0). Lisäksi käytetyssä regressiomallissa oli kontrollimuuttujina yrityksen koko (taseen loppusumma), kannattavuus (koko pääoman tuottoaste), velkaantumisaste (velkojen osuus kaikista varoista), yrityksen markkina-arvo ja toimia-alaluokitus. Tutkimuksen tuloksena selvisi, että 83,6 % yrityksistä julkaisi tietoja kyberriskeistä raporteissaan. Yli puolet yrityksistä mainitsi mahdollisen kyberturvallisuustapahtuman seurauksena seuraavat viisi vaikutusta: toiminnan keskeytymisen tai viiveet, mainehaitan, luottamuksellisen tiedon vuotamisen, oikeudelliset seuraamukset ja sakot sekä tietojen häviämisen tai tuhoutumisen. Tutkimushypoteesien osalta positiivinen assosiaatio havaittiin hallituksen riippumattomuudella, hallituksen naisjäsenten suhteellisella osuudella ja erillisellä kyber- ja tietoturvaelimen olemassaololla – mitä enemmän hallituksessa oli riippumattomia jäseniä tai naisjäseniä tai jos yrityksessä oli kyberturvallisuusasioihin keskittyvä toimielin, sitä todennäköisemmin kyberturvallisuustietoja sisällytettiin vuosiraportteihin. Hallituksen IT-osaamisella oli positiivinen assosiaatio kyberriskienhallinnan kuvauksen ja tapahtuneiden kyberturvallisuustapahtumien julkaisuun vuosiraporteissa. Sen sijaan tuloksissa suurempi hallituksen IT-osaamisen osuus indikoi vähäisempää raportointia mahdollisten kyberturvallisuustapahtumien vaikutuksesta. Tutkimustuloksissa hallituksen toimivuosien määrä assosioituu siten, että suurempi toimivuosien keskiarvo indikoi vähäisempää raportointia potentiaalisista ja tapahtuneista kyberturvallisuustapahtumista. Sama assosiaatio oli myös toimivuosien määrällä ja kyberriskienhallinnan kuvauksen julkaisemisella. Hallituksen jäsenten keskimääräisellä iällä ei havaittu korrelaatiota kyberturvallisuusinformaation julkaisuun.

Edellä kuvatut tutkimukset ovat keskittyneet selvittämään mitä yritykset raportoivat ja julkaisevat kyberturvallisuudesta ja -riskeistä. Tämän näkökulman lisäksi on tutkittu kyberturvallisuuteen liittyvien tietojen julkaisemisen

[4] Englanninkielisessä kirjallisuudessa hallituksen riippumattomuudesta käytetään termiä *independence*. Riippumattomuudella tarkoitetaan muun muassa, että hallituksen jäsen ei ole työsuhteessa yhtiöön tai jäsenellä ei ole merkittävää osakkeenomistusta. Katso tarkemmin riippumattomuuden määritelmästä suomalaisessa hallintokoodissa: https://www.cgfinland.fi/wp-content/uploads/2023/05/hallinnointikoodi-2020.pdf

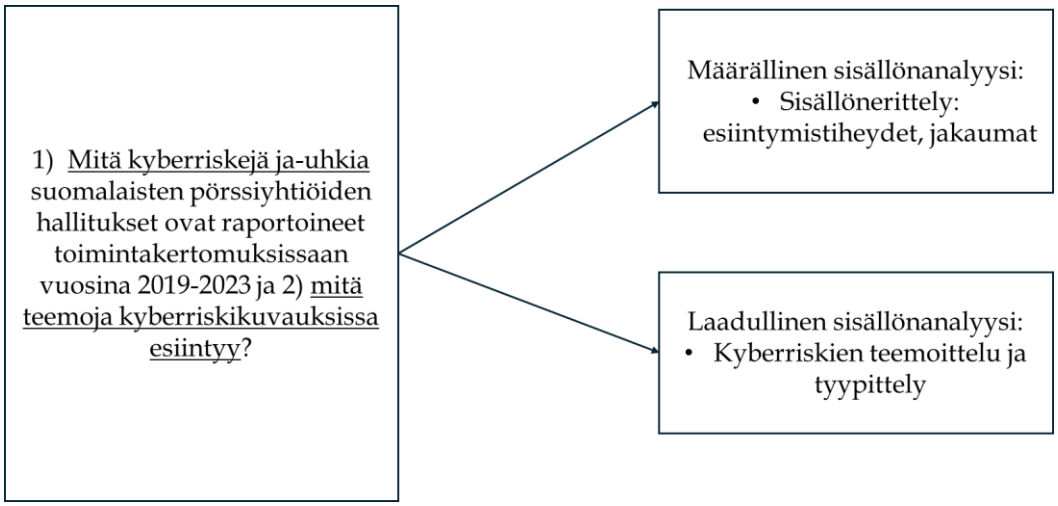
vaikutuksia. Tutkimuksissa (Berkman ym., 2018; Gordon ym., 2010) on osoitettu positiivinen korrelaatio kyberturvallisuuteen liittyvien tietojen julkaisulla ja yrityksen markkina-arvolla. Kiinnostavia tutkimuksia kyberriskien julkaisun yhteydestä tulevaisuudessa tapahtuviin tietoturvaloukkauksiin ovat toteuttaneet muun muassa Ettredge ym. (2018), Li ym. (2018) ja Wang ym. (2013). Näissä tutkimuksissa kyberturvallisuuteen liittyvien tietojen ja tulevaisuudessa tapahtuvien tietoturvaloukkausten välillä oli positiivinen assosiaatio.

Yhteenvetona tämän tutkimuksen kannalta relevantista aiemmasta tutkimuksesta voidaan todeta, että pörssilistattujen yritysten kyberturvallisuuteen liittyvien tietojen julkaisua käsittelevää tutkimusta on tehty verrattain vähän. Kyberturvallisuuden monialaista ja poikkitieteellistä luonnetta kuvastaa se, että aiempi tutkimus on julkaistu eri tieteenalojen julkaisussa. Käsitelty tutkimus on julkaistu laskentatoimea, johtamista ja hallintoa, tietojärjestelmiä, riskienhallintaa ja kestävyysraportointia käsittelevissä tieteellisissä julkaisuissa. Maantieteellisesti tutkimus painottuu yhdysvaltalaisiin yhtiöihin johtuen kyberturvallisuuteen liittyvän informaation julkaisua koskevasta pakottavasta lainsäädännöstä. Muualla kyberturvallisuuteen liittyvien tietojen julkaisu on vapaaehtoisuuteen pohjautuvaa ja tutkimuksia on tehty vähän. Suomalaisten pörssiyhtiöiden kyberturvallisuuteen liittyvän informaation julkaisua käsittelevää tutkimusta ei tämän tutkimuksen kirjallisuuskatsauksessa löytynyt. Puuttuva tutkimus suomalaisessa kontekstissa motivoi tätä tutkimusta ja toimii yhtenä perusteluna sen tarpeellisuudelle.

3 TUTKIMUKSEN TOTEUTUS

3.1 Tutkimusmenetelmät

Tutkimus on pitkittäistutkimus, jonka perusjoukkona on arvopaperipörssi Nasdaq Helsingin päälistalla vuosina 2019–2023 noteeratut yhtiöt. Koska perusjoukon suuruus on maltillinen, tutkimus toteutettiin kokonaistutkimuksena, jolloin perusjoukkoa ei rajata otannalla. Tutkimuksen aineistona olivat päälistalla noteerattujen yhtiöiden vuosiraportteihin sisältyvät hallitusten toimintakertomukset. Yhtiöiden vuosiraportit ovat yksi harvoista yhteismitallisista aineistoista, joiden avulla yhtiöiden näkemystä kyberriskeistä ja -uhkista voidaan tutkia koko perusjoukon laajuudessa. Pitkittäistutkimus on tutkimusstrategia, jossa on mukana temporaalinen eli aikaan liittyvä ulottuvuus. Pitkittäistutkimus mahdollistaa trendien ja makrotason muutosten seuraamisen ja muutosten havaitsemisen tutkittavassa ilmiössä sekä muutoksiin vaikuttaneiden tekijöiden analysoimisen (Vernon Gayle & Paul Lambert, 2020). Aineistosta muodostuu aikasarja, josta tunnistetaan trendejä ja muutoksia pörssiyhtiöiden kyberriskien raportoinnissa. Keskeisin tutkimusmenetelmä on *aineistolähtöinen sisällönanalyysi,* joka toteutetaan sekä määrällisin että laadullisin tekniikoin. Teorialla on analyysissa ja johtopäätöstenteossa ohjaava rooli. Kuvio 2 havainnollistaa tutkimuskysymyksen ja käytettävien menetelmien välistä suhdetta ilmiön kuvaamiseksi ja selittämiseksi.



KUVIO 2 Tutkimuskysymys ja -menetelmät

Tuomen ja Sarajärven (2018) mukaan sisällönanalyysista puhutaan tutkimusmenetelmäkirjallisuudessa kahdessa eri merkityksessä. Sisällönanalyysilla voidaan viitata sekä tutkittavan ilmiötä käsittelevän tekstin sisällön kuvaamiseen kvantitatiivisesti että dokumenttien sisällön kuvaamiseen sanallisesti. Heidän mukaansa näiden kahden lähestymistavan erottamiseksi tekstien kvantifioinnista tulisi käyttää nimitystä sisällönerittely ja tekstien sanallisesta kuvaamista tulisi kutsua sisällönanalyysiksi. Tässä tutkimuksessa tekstin kvantifioinnista käytetään nimitystä määrällinen sisällönanalyysi tai sisällönerittely ja sisällönanalyysillä tarkoitetaan tekstien sanallista analyysia kontekstissa, jossa ne esiintyvät.

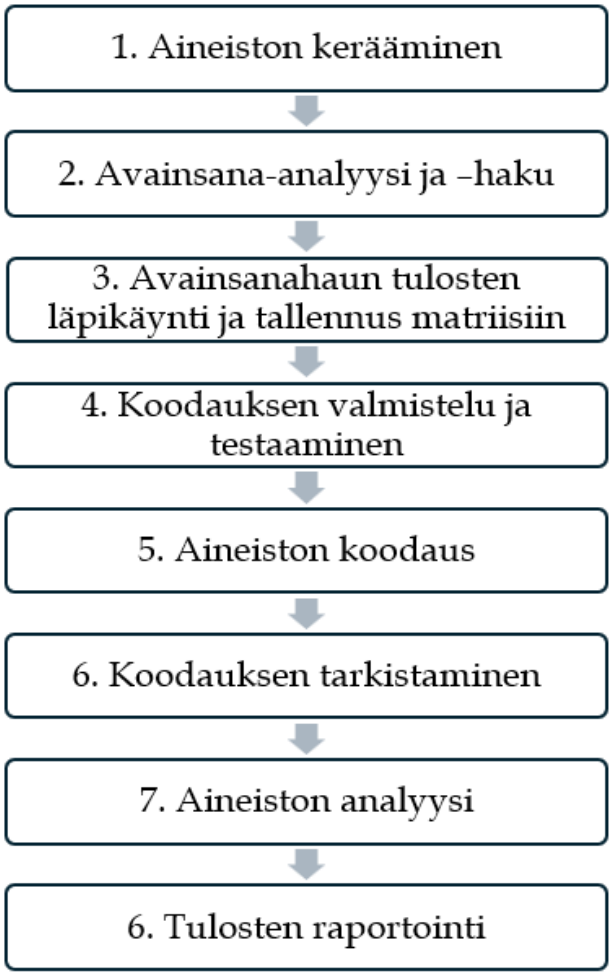
Eskola ja Suoranta (1998) jakavat laadullisen tutkimuksen analysointimenetelmät kvantitatiivisiin analyysitekniikoihin, teemoitteluun, tyypittelyyn, sisällönerittelyyn, diskursiivisiin analysointitapoihin ja keskusteluanalyysiin. Tässä tutkimuksessa käytetään edellä mainituista menetelmistä kvantitatiivisia tekniikoita, teemoittelua ja tyypittelyä. Kvantitatiivisilla menetelmillä eritellään ja kuvataan aineistossa esiintyviä kyberriskien esiintymistiheyksiä ja jakaumia. Teemoittelun avulla aineistosta tunnistetaan kyberriskikuvauksista esiin nousevia teemoja ja trendejä. Tyypittely laadullisessa tutkimuksessa tarkoittaa aineiston ryhmittelyä etsimällä samankaltaisuuksia aineistosta (Eskola & Suoranta, 1998). Tässä tutkimuksessa tyypittelyä sovellettiin muodostamalla yritysten kyberriskikuvauksien sisältöä edustava tyypittely, johon tutkittavan perusjoukon yritykset yhdistettiin kyberriskikuvausten sisällön perusteella.

Laadullinen analyysi sisältää kyberriskikuvausten tunnistamisen, koodaamisen ja luokittelun, jonka avulla tunnistetaan kyberriskien kuvaamisessa esiintyviä *teemoja* ja *muutoksia*. Määrällisessä analyysissa muodostuu kuva kyberriskien esiintymistiheyksistä, tunnistetuista uhkatyypeistä ja uhkien vaikutuksesta sekä edellä mainittujen kehityksestä.

3.2 Aineiston kerääminen, käsittely ja analysointi

Tutkimuksen aineiston kerääminen, käsittely ja analysointi toteutettiin kuviossa 3 esitetyn prosessin mukaisesti. Aineistona käytetyt vuosiraportit ladattiin joko yhtiöiden internetsivuilta, Helsingin pörssin tiedotevarastosta[5] ja vuosikertomuksia kootusti julkaisevalta internetsivustolta[6]. Vuosiraportit kerättiin kaikilta niiltä yhtiöiltä, joiden osakekurssille oli olemassa noteeraus kunkin tarkasteluvuoden viimeisenä päivänä, ja yritys oli julkaissut tilinpäätöksen tarkasteluvuodelta. Yhtiöiden julkaisemien raporttien nimeämiskäytäntö ei ole yhtenäinen ja samansisältöisestä raportista voidaan käyttää eri nimitystä. Käytettyjä nimityksiä olivat muun muassa vuosikertomus, taloudellinen katsaus, vuosikatsaus tai tilinpäätös. Lisäksi yhtiöt saattavat jakaa julkaisemansa informaation useampaan dokumenttiin esimerkiksi siten, että taloudellisista tiedoista ja yleisemmin yhtiön liiketoimintaa koskevista tiedoista julkaistaan erilliset raportit. Eriävästä nimeämiskäytännöstä huolimatta jokaiselta yhtiöltä ladattiin raportti, joka sisältää pakollisen hallituksen toimintakertomuksen. Jos yhtiö oli julkaissut toimintakertomuksen sisältävän raportin useammalla kuin yhdellä kielellä, ladattiin suomenkielinen raporttiversio. Jos suomenkielistä raporttia ei ollut julkaistu, ladattiin englanninkielinen raporttiversio. Helsingin pörssissä on listattuna yhtiöitä, jotka eivät raportoi suomalaisen kirjanpitolain mukaan. Nämä yhtiöt rajattiin tutkimuksen ulkopuolelle, koska ne eivät ole vertailukelpoisia suomalaisesta lainsäädännöstä tulevien vaatimusten osalta. Ladatut raportit tallennettiin pdf-tiedostoformaatissa tutkimuksen käytössä olleen tietokoneen levyjärjestelmälle. Vuosien 2019–2023 vuosiraporteista muodostui yhteensä 636 raporttia käsittävä aineisto. Aineiston kerääminen on loppunut 19.4.2024. Vuoden 2023 aineistossa on 3 yhtiötä, jotka eivät ole julkaisset vuosiraporttiaan aineiston keräämisen päättymiseen mennessä. Lisäksi 31.12.2023 jälkeen kahden yrityksen pörssilistaus on päättynyt yrityskaupan takia, jonka vuoksi ne eivät julkaise enää tilinpäätöksiään. Tutkimusraportin liitteessä 1 on tutkimusaineistoon sisältyneet yhtiöt ja mahdolliset poikkeukset aineistossa.

[5] https://www.nasdaqomxnordic.com/uutiset/yhtiotiedotteet
[6] https://www.vuosikertomukset.net



KUVIO 3 Aineiston kerääminen, käsittely, analyysi ja raportointi

Aineiston keräämisen jälkeen suoritetun avainsana-analyysin perusteella muodostettiin avainsanalista. Koska aineistossa oli muutamia englanninkielisiä raportteja, muodostettiin avainsanalistat sekä suomeksi että englanniksi. Suomenkielisessä avainsanalistassa oli sanat *kyber* ja *tietoturva.* Englanninkielisessä hakusanalistassa oli vastaavasti mukana sanat *cyber* ja *information security.* Suoritettu avainsanahaku etsi aineiston raporteista näiden sanojen merkkijonoesiintymiä ja huomioi myös suomen kielen taivutusmuodot sekä isot ja pienet alkukirjaimet. Avainsanalistan mukainen avainsanahaku toteutettiin Python-ohjelmointikielellä laaditulla ohjelmalla. Ohjelma kävi läpi kaikki aineiston raportit ja tunnisti aineistosta ne raportit, joissa avainsanalistan mukaiset sanat esiintyivät. Ohjelma tulosti erilliseen tekstitiedostoon tiedot niistä yksittäisistä raporteista, joissa hakusana esiintyi, sekä sivunumeron, jossa hakusana esiintyi. Avainsanahaun tulokset taulukoitiin yhtiöittäin havaintomatriisiin.

Avainsanahaussa hakusanaosumia saaneiden dokumenttien käsittelyä jatkettiin manuaalisella käsittelyllä, jossa jokainen hakuosumia saanut dokumentti käytiin läpi. Dokumenteista tunnistettiin sijainti, jossa avainsanalistan mukainen esiintymä oli. Jos hakusana esiintyi raportin muussa osuudessa kuin

pakollisessa hallituksen toimintakertomuksessa tai tilinpäätöksen liitetiedoissa, esiintymä sivuutettiin. Tämän seurauksena muun muassa yrityksen vastuullisuutta tai liiketoimintaa yleisesti käsittelevissä osuuksissa olleet hakusanaosumat karsittiin pois. Hallituksen toimintakertomuksessa esiintyneet hakusanaosumat käytiin läpi, ja tietoturvaa tai kyberturvallisuutta käsitelleet kuvaukset tallennettiin havaintomatriisin. Havaintomatriisiin tallennettiin kokonainen lause, kappale tai kappaleet, jotka käsittelivät tietoturvaa tai kyberturvallisuutta. Edellä kuvatulla menetelmällä käytiin läpi kaikki hakusanoja sisältäneet dokumentit ja lisäksi hakumenetelmän toimivuuden varmistamiseksi satunnaisesti käytiin läpi myös dokumentteja, jotka eivät olleet saaneet hakuosumia.

Seuraavaa vaihe oli aineiston koodaaminen. Koodaamisella tarkoitetaan tekstin systemaattista läpikäyntiä, jossa aineiston osia yhdistellään ja erotellaan jonkin ominaisuuden mukaan. Sen jälkeen samankaltaiset osat luokitellaan ja luokalle annetaan nimi yhteisen ominaisuuden mukaan (Juhila, 2021). Lisäksi koodaaminen ja luokittelu yhdenmukaistavat ja standardoivat dataa, joka mahdollistaa myös määrillisten analyysimenetelmien käytön tutkimuksessa (Flick, 2018). Systemaattisen koodauksen toteuttaminen edellyttää koodausjärjestelmän luomista. Tässä tutkimuksessa koodausjärjestelmä noudatti Weberin (2011) esittämää mallia:

1. *Analysointiyksikön määrittely*: tärkeä vaihe koodauksessa, jossa määritellään ne osat tekstistä, jotka koodataan. Analysointiyksikkö voi olla sana, lause, kappale tai koko teksti.
2. *Kategorioiden määrittely*: koodatut analysointiyksiköt luokitellaan. Kategorioiden määrittelyssä on päätettävä, ovatko kategoriat toisensa poissulkevia eli voiko yksittäinen koodi kuulua useampaan kuin yhteen kategoriaan. Lisäksi kategorioiden määrittelyssä on päätettävä kuinka kattavia tai yksityiskohtaisia kategoriat ovat.
3. *Koodauksen testaaminen testiotoksella*: koodaussääntöjen yksiselitteisyys ja toimivuus testataan sopivan kokoisessa otoksessa, mikä paljastaa usein myös koodaussääntöön tarvittavia muutoksia ja lisäyksiä.
4. *Tarkkuuden ja luotettavuuden arviointi testiotoksessa*: testaamisen jälkeen koodausjärjestelmän tarkkuus ja luotettavuus arvioidaan.
5. *Koodaussääntöjen tarkistus ja parantaminen*: koodaussääntöihin tehdään parannuksia kohdan 3. ja 4. perusteella.
6. *Koodauksen uudelleentestaaminen*: toistetaan koodauksen testaaminen parannetuilla säännöillä testiotoksella toistamalla vaiheet 3.–6.
7. *Koko aineiston koodaus*: Kun riittävä koodaussääntöjen tarkkuus ja luotettavuus on saavutettu, koodataan koko aineisto.
8. *Tarkkuuden ja luotettavuuden arviointi koko aineistossa*: Kun koko aineisto on koodattu, arvioidaan koodaussääntöjen luotettavuutta ja tarkkuutta koko aineistolle.

Tässä tutkimuksessa analysointiyksikön muodosti hallituksen vuosikertomuksessa mainittu kyberriskin kuvaus. Kuvauksen laajuus vaihteli yksittäisestä sa-

nasta usean kappaleen mittaisiin tekstikokonaisuuksiin. Koodauskategorioita muodostettiin neljä: *uhkatyypit*, *vaikutukset*, *teemat* ja *riskiluokittelu*. Uhkatyypit-kategoriaan luokiteltiin maininnat niistä erilaisista kyberuhkista, joita yritysten kyberriskikuvauksissa mainittiin. Vaikutukset-kategoriaan puolestaan luokiteltiin maininnat kyberriskin mahdollisista vaikutuksista yritykselle. Teemat-kategorian alle luokiteltiin kyberriskikuvauksessa mainitut muutostekijät ja trendit, jotka ovat vaikuttaneet yrityksen näkemykseen kyberriskeistä. Näiden kolmen kategorian koodit muodostettiin induktiivisesti aineiston perusteella. Neljäs kategoria, riskiluokittelu, poikkeaa kolmesta edellä mainitusta kategoriasta. Aineiston keräämisen ja siihen tutustumisen aikana kävi ilmi, että yritysten kyberriskien kuvauksien laajuudessa ja sisällössä on paljon vaihtelua. Osa kuvauksista saattoi olla pituudeltaan suhteellisen lyhyitä, mutta sisältää kuitenkin verrattain monipuolisen kuvauksen riskistä. Osalla yrityksillä kyberriskin kuvaus keskittyi esimerkiksi riskienhallintamallin kuvaamiseen varsinaisen kyberriskin kuvaamisen sijaan. Aikaisemmassa tutkimuksessa on käytetty kyberriskin kuvaamisen pituutta (sanoina) mittarina arvioitaessa riskikuvauksen sisältöä (katso esim. Gao ym., 2020). Julkaistun informaation mittaamista laskemalla, esimerkiksi sanoja, on kritisoitu argumentoimalla, että raporteissa on yleensä toistuvia rakenteita ja sanoja, jolloin mittaus vääristyy (Marston & Shrives, 1991). Lisäksi laskettuja numeroita ei voi tarkastella kontekstistaan irrallisena, vaan niiden selittämiseen tarvitaan sanallista narratiivia. Tämä sama kritiikki on yhdistettävissä myös tähän tutkimukseen: kyberriskikuvauksen pituus sanoina ei indikoi kuvauksen sisältöä tai laadullisia attribuutteja. Riskikuvauksien pituuksia voidaan käyttää yhtenä mittarina kuvaamaan trendejä, mutta kattavampaan analyysiin tarvitaan myös muita menetelmiä.

Koodaussäännöstöä testattiin ja parannettiin testaamalla sitä vuoden 2018 pörssiyhtiöiden hallitusten toimintakertomuksissa esiintyviin kyberriskien kuvauksiin. Vuoden 2018 aineistoa käytettiin ainoastaan koodisäännöstön testaamiseen ja varsinainen koodaaminen tapahtui tutkimuksen aikajänteen kattavalla vuosien 2019–2023 aineistolla. Testivaiheessa jokaiseen kategoriaan, pois lukien riskiluokittelu, muodostui laajahko määrä eri koodeja. Testaamisen aikana samasta uhkatyypistä, vaikutuksesta tai teemasta muodostui useampi eri koodi. Koodaussäännöt tarkistettiin testaamisen jälkeen ja päällekkäisyydet poistettiin sekä koodistoa harmonisoitiin. Koodaussäännöstö kirjattiin erilliseen dokumenttiin, jota käytettiin tukemaan koodausta niin testivaiheen kuin varsinaisen koodaamisen aikana.

Testaamisen ja koodaussäännöstön dokumentoinnin jälkeen koko aineisto koodattiin systemaattisesti ATLAS.ti ohjelmistolla. Koko aineisto koodattiin kahdessa vaiheessa. Ensimmäisessä vaiheessa koodaus tehtiin vuosi kerrallaan ja uudet aineistosta esiin nousseet uhkatyypit, vaikutukset ja teemat lisättiin koodistoon. Kun koko aineisto oli koodattu, koodistosta poistettiin mahdolliset päällekkäisyydet. Tämän jälkeen aineisto käytiin vielä uudestaan kokonaisuudessaan läpi ja varmistettiin, että lopullista koodistoa oli käytetty yhdenmukaisesti koko aineistoon. Tällä pyrittiin varmistamaan koodaamisen luotettavuus ja johdonmukainen soveltaminen koko aineistoon. Koodaamisen tarkkuuden ja

luotettavuuden arviointia on käsitelty tarkemmin tämän tutkimusraportin luvussa 3.3.

Määrällistä sisällönanalyysia ja erittelyä tukemaan tutkimuksen perusjoukon muodostavista yrityksistä kerättiin toimialaluokitus ja yrityksen markkina-arvoperusteinen kokoluokka. Yhtiön toimialaluokituksena käytettiin arvopaperipörssi Nasdaq Helsingin käyttämää Industry Classification Benchmark -luokittelun (ICB) mukaista toimialaluokitusta. Yrityksen kokoluokkana käytettiin vastaavasti Helsingin pörssin luokittelua pieniin, keskisuuriin ja suuriin yrityksiin. Toimiala- ja kokoluokitukset kerättiin Nasdaq Helsingin internetsivuilta.

3.3 Tutkimuksen luotettavuuden arviointi

Hyvään tutkimuskäytäntöön kuuluu tehtyjen valintojen ja menetelmien arviointi, tutkimusta ohjaavien sääntöjen tuntemus ja tutkimuksen luotettavuuskriteerien omaksuminen (Puusa ym., 2020). Määrällisen ja laadullisen tutkimuksen menetelmät poikkeavat toisistaan ja siten luotettavuuden arviointi on tutkimuksen toteutustavasta riippuvainen. Menetelmäkirjallisuudessa tutkimusmenetelmien luotettavuutta on arvioitu yleensä *validiteetin* ja *reliabiliteetin* käsitteiden avulla, joiden tausta on määrällisen tutkimuksen perinteessä (Tuomi & Sarajärvi, 2018). Määrällisessä tutkimusperinteessä validiteetilla tarkoitetaan sitä, kuinka hyvin valittu mittari mittaa todellisuudessa tutkimuksen kohteena olevaa ilmiötä tai asiaa (Puusa ym., 2020). Reliabiliteetti puolestaan tarkoittaa varsinaiseen mittaamiseen liittyvää virhettä – kuinka paljon mittaustilanne, mittaaja tai satunnaiset tekijät vaikuttavat mittaustulokseen. Validiteetin ja reliabiliteetin käyttöä laadullisessa tutkimuksessa on kritisoitu niiden määrällisen tutkimuksen taustan takia (Tuomi & Sarajärvi, 2018). Lincoln & Guba (1985) esittivät laadullisen tutkimuksen luottavuuden arvioimista *uskottavuuden* (engl. credibility), *siirrettävyyden* (engl. transferability), *varmuuden* (engl. dependability) ja *vahvistuvuuden* (engl. confirmability) näkökulmista.

Tässä tutkimuksessa on sovellettu sekä määrällisen että laadullisen analyysin tekniikoita, joten luotettavuutta on syytä arvioida niin validiteetin ja reliabiliteetin kuin uskottavuuden, siirrettävyyden, varmuuden ja vahvistettavuuden näkökulmasta. Kyberriskimainintojen, uhkatyyppien ja kyberriskin toteutumisesta aiheutuvien haittojen esiintyvyystiheyksien mittaamisen validiteetti on korkea. Mittari on luonteeltaan binäärinen eli maininta joko esiintyy aineistoissa tai ei esiinny. Mittarin reliabiliteetti ei todennäköisesti ole samalla tasolla kuin validiteetti. Aineisto käytiin läpi osin automatisoidusti ja osin manuaalisesti. Tämä on yksi mahdollinen reliabiliteettia heikentävät virhelähde. Reliabiliteettia heikentää myös se, että yhtiöiden käytännöt riskien raportoinnissa eivät ole täysin yhteneväiset. Yritysten välillä on eroa siinä, missä dokumentin osassa riskejä käsitellään ja missä laajuudessa. Vaikka hallituksen toimintakertomuksessa on kerrottava liiketoiminnan riskeistä ja epävarmuustekijöitä, on riskejä raportoitu laajasti myös esimerkiksi hallintoa käsittelevässä

osuudessa, joka oli rajattu tämän tutkimuksen aineiston ulkopuolelle. Tutkimuksen reliabiliteettia parantaa puolestaan se, että aineiston koodauksen laadittiin koodaussäännöt ja koodaaminen toteutettiin systemaattisesti. Menetelmäkirjallisuuden mukaan useampi koodaaja parantaa tutkimuksen luotettavuutta (Neuendorf, 2016). Tässä tutkimuksessa ei ollut mahdollista käyttää useampaa aineiston koodaajaa, joten tältä osin luotettavuutta ja reliabiliteettia olisi ollut mahdollista parantaa käyttämällä useampaa koodaajaa. Tutkimusmenetelmien systemaattinen käyttö ja tutkimusprosessin läpinäkyvä kuvaaminen parantavat myös tutkimuksen varmuutta (Korstjens & Moser, 2018). Varmuuden toteutumista on parannettu kuvaamalla tutkimusraportin tässä luvussa seikkaperäisesti tutkimuksen aineiston keräys, käsittely ja analyysi.

Uskottavuudella tarkoitetaan sitä, että vastaako tutkijan käsitteellistys ja tulkintansa tutkittavien käsityksestä (Eskola & Suoranta, 1998). Kuten jo tutkimusraportin johdantoluvun käsitteiden määrittelyssä todettiin, on kyberturvallisuuden käsite vakiintumaton. Kyberturvallisuus ja siihen liittyvät muut käsitteet ovat abstrakteja ja on hyvin todennäköistä, että tämän tutkimuksen kohteena olevissa yrityksissä kyberturvallisuus ymmärretään eri tavoin ja käsitys myös muuttuu ajan myötä. Kyberturvallisuutta on tässä tutkimuksessa tulkittu käytettävissä olevan aineiston kontekstissa ja ehdottoman tarkkarajaista käsitteiden määrittelyä ei edellytetä riittävän uskottavien johtopäätösten ja tulkintojen muodostamiseksi.

Yleistettävyydellä tarkoitetaan tilastollisessa tutkimuksessa otoksesta saatujen tulosten yleistämistä koskemaan tutkimuksen perusjoukkoa (Ketokivi, 2015). Tämän tutkimuksen perusjoukkona on Helsingin pörssin päälistalla noteeratut yhtiöt ja tutkimusaineisto käsitti luvussa 3.2 kuvattuja poikkeuksia lukuun ottamatta koko perusjoukon. Kvantitatiiviset tulokset voidaan siten yleistää koskemaan koko perusjoukkoa. Kvalitatiivisen tutkimuksen laadun arviointiin yleistettävyys ei kuulu (Puusa ym., 2020), mutta tutkimuksen siirrettävyydestä vastaavaan kontekstiin tai tutkimusasetelmaan tulisi arvioida (Korstjens & Moser, 2018). Aineiston laajuus parantaa tämän tutkimuksen yleistettävyyttä, mutta se ei ole erityisen ”syvä” laadullisen tutkimuksen näkökulmasta. Aineiston laajuus ja tutkimusprosessin seikkaperäinen kuvaus tutkimusraportin tässä luvussa parantaa tutkimuksen siirrettävyyttä muihin konteksteihin ja tutkimusasetelmiin.

Tutkimustulosten vahvistuvuudella tarkoitetaan sitä, että aineistosta muodostetut tulkinnat saavat tukea vastaavaa ilmiöitä käsitelleistä tutkimuksista (Eskola & Suoranta, 1998). Kirjallisuuskatsauksessa esitellään useita kansainvälisesti tehtyjä tutkimuksia, joissa tutkimuksen kohteessa, tutkimuskysymyksissä ja tutkimusmenetelmissä on vastaavuuksia tämän tutkimuksen kanssa. Tutkimusraportin luvussa 5 palataan vielä aiemmin tehtyyn tutkimukseen ja saatuja tuloksia arvioidaan myös aiemman tutkimuksen tulosten näkökulmasta tutkimuksen vahvistavuuden parantamiseksi.

4 TUTKIMUKSEN TULOKSET

4.1 Aineiston kattavuus

Tutkimusaineisto kattoi kaikki Helsingin pörssin päälistalla noteeratut yhtiöt, jotka ovat julkaisseet Suomen kirjanpitolain mukaisen tilinpäätöksen. Helsingin pörssissä kaupankäynnin kohteena on lisäksi 5 yhtiötä, joiden kotipaikka on muualla kuin Suomessa ja sen vuoksi niiden julkaisemaan informaatioon ei sisälly Suomen kirjanpitolain tarkoittamaa hallituksen toimintakertomusta. Taulukossa 1 on esitetty vuosittain Helsingin pörssin päälistalla vuoden viimeisenä päivänä noteerattujen yhtiöiden lukumäärä ja tutkimuksen aineistoon sisältyneiden yhtiöiden lukumäärä. Vuoden 2023 aineistosta puuttuu 5 yhtiön aineisto, koska niitä ei oltu julkaistu aineiston keräämisen päättymiseen mennessä. Vuoden 2023 aineisto kattaa 92,8 % ja vuosina 2019–2022 kattavuus on noin 96 % kaikista listatuista yhtiöistä.

TAULUKKO 1 Aineiston kattavuus

	2019	**2020**	**2021**	**2022**	**2023**
Päälistalla yhtiöitä 31.12.	130	129	132	137	138
Yhtiöitä aineistossa	125	124	127	132	128
Aineiston kattavuus (%)	96,2 %	96,1 %	96,2 %	96,4 %	92,8 %
Yhtiöitä, joiden aineisto puuttuu	0	0	0	0	5
Yhtiöitä analyysin ulkopuolella	5	5	5	5	5
Aineisto puuttuu (%)	0,0 %	0,0 %	0,0 %	0,0 %	3,6 %

4.2 Hakusanojen esiintymistiheyksien ja kyberriskimainintojen kehitys

Tulokset aineistolle suoritetusta avainsanahausta ja avainsanojen esiintymistiheyksistä on esitetty taulukossa 2 ja kuviossa 4. Vuonna 2019 62,4 % tutkimusaineistoon kuuluneista yhtiöistä mainitsi hakusanat *kyber, tietoturva, cyber* tai *information security* hallituksen toimintakertomuksen sisältävissä vuosiraporteissaan. Vuonna 2023 vastaava esiintymistiheys oli jo 81,1 %. Merkittävä nousu esiintymistiheyksissä on nähtävissä vuoden 2022 raporteissa, jolloin avainsanoja maininneiden yritysten määrä kasvoi 9,6 %-yksikköä. Nämä tulokset kuvaavat ainoastaan sitä, kuinka moni yritys mainitsi avainsanat raporteissaan, mutta ne eivät kuvaa maininnan sisältöä, sijaintia tai kontekstia. Avainsanahaku toteutettiin niihin yritysten julkaisemiin raportteihin, joihin sisältyy yhtiön hallituksen toimintakertomus. Kuten aiemmin luvussa 3.2 todettiin, on yritysten välillä paljon eroa, millaisia muita osiota näihin dokumentteihin sisältyy. Näin ollen esitettyihin hakusanojen esiintymistiheyksiin sisältyy myös hallituksen toimintakertomusten ulkopuoliset maininnat, joita aineistossa esiintyy muun muassa yritysten vastuullisuutta ja hallintoa käsittelevissä osuuksissa. Vaikka dokumentit eivät tältä osin ole yhteismitallisia, on tutkittava perusjoukko pysynyt koko tarkastelujakson aikana suurelta osin samana. Siten voidaan yleisesti todeta, että kyber- ja tietoturvallisuuttaa käsittelevä narratiivi on lisääntynyt yhtiöiden vuosiraporteissa vuosina 2019–2023.

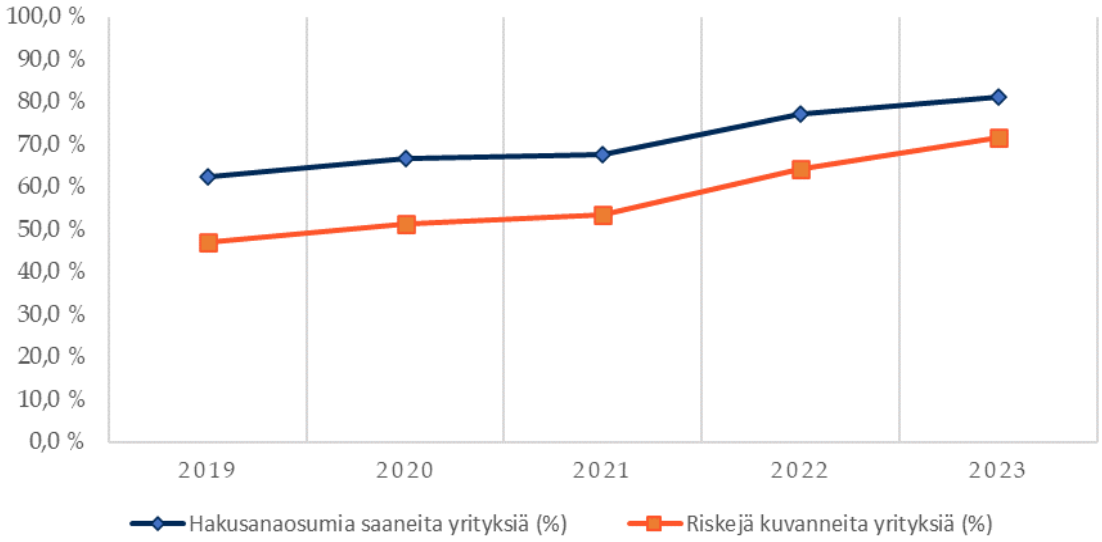
TAULUKKO 2 Hakusanojen esiintymistiheyksien kehitys vuosina 2019–2023

	2019	**2020**	**2021**	**2022**	**2023**
Hakusanaosumia saaneita yrityksiä	78	82	86	102	103
Hakusanaosumia saaneita yrityksiä (%)	62,4 %	66,7 %	67,7 %	77,3 %	81,1 %
Muutos edelliseen vuoteen (%-yksikköä)	-	4,3 %	1,0 %	9,6 %	3,8 %
Yrityksiä tutkimusaineistossa	125	123	127	132	127

Hallitusten toimintakertomusten riskejä kuvaavissa osioissa kyberriskimainintojen esiintymistiheyksissä voidaan nähdä samansuuntainen nouseva trendi kuin avainsanojen esiintymistiheyden kehityksessä. Taulukko 3 ja kuvio 4 osoittavat, että hallituksen toimintakertomuksiin sisältyvissä arvioissa liiketoiminnan riskeistä ja epävarmuustekijöistä mainitaan yhä useammin tietoturvaan ja kyberturvallisuuteen liittyvä riskejä. Vuonna 2019 47,2 % yrityksistä kuvasi näitä riskejä ja vuoteen 2023 mennessä osuus on noussut 71,7 prosenttiin. Tarkasteluajanjaksolla riskimainintojen esiintymistiheys nousi 24,5 %-yksikköä ja vuosina 2022–2023 mainintojen kasvu on selvästi edellisiä vuosia suurempaa. Vuonna lisäys 2022 oli peräti 12,4 %-yksikköä.

TAULUKKO 3 Kyber- ja tietoturvariskimainintojen esiintymistiheyksien ja kuvauksien pituuden kehitys vuosina 2019–2023

	2019	2020	2021	2022	2023
Riskejä kuvanneita yrityksiä	59	63	68	87	91
Riskejä kuvanneita yrityksiä (%)	47,2 %	51,2 %	53,5 %	65,9 %	71,7 %
Muutos edelliseen vuoteen (%-yksikköä)	-	4,0 %	2,3 %	12,4 %	5,7 %
Yrityksiä tutkimusaineistossa	125	123	127	132	127



KUVIO 4 Hakusanaosumia saaneet ja kyberriskejä kuvanneet yritykset

Toimialoittain tarkasteltuna kyber- ja tietoturvariskimainintojen kehitys vuosina 2019–2023 on esitetty taulukossa 4. Listattujen yhtiöiden määrä Helsingin pörssin päälistalla on verrattain pieni ja sen vuoksi osalla toimialoista on vain yksittäisiä yrityksiä. Tämän takia toimialojen väliseen vertailuun on suhtauduttava varauksella. Toimialakohtaisia trendejä tarkasteltaessa huomio kiinnittyy terveydenhuollon ja rahoituksen toimialojen yrityksiin. Näiden yritysten raportoimat merkittäviin riskeihin ja epävarmuustekijöihin kuuluvat tietoturva- ja kyberriskit ovat lisääntyneet eniten. Terveydenhuollon toimialaan kuuluvista yrityksistä vain 14,3 % raportoi kyber- ja tietoturvariskeistä vuonna 2019 ja vastaava luku rahoituksen toimialalla oli 30,8 %. Vuoteen 2023 mennessä kyber- ja tietoturvariskeistä raportoineiden terveydenhoitotoimialan yritysten osuus oli kasvanut 57,1 prosenttiin ja rahoitusalan yrityksissä 75,0 prosenttiin. Rahoitusalalla kyberriskejä raportoivien yritysten osuus on vuonna 2023 samalla tasolla kuin kaikista toimialoista korkeimpia suhteellisia osuuksia raportoivat kulutuspalveluiden ja -tuotteiden, perusteollisuuden ja teknologiatoimialan yritykset. Terveydenhuoltotoimialalla taso on edellisiä matalampi edelleen vuonna 2023.

TAULUKKO 4 Kyber- ja tietoturvariskejä hallituksen toimintakertomuksessa kuvanneiden yritysten suhteelliset osuudet toimialan yrityksistä

	2019		2020		2021		2022		2023		
Toimiala	**Riskin maininneita**	**n**	**Riskin maininneita**	**n**	**Riskin maininneita**	**n**	**Riskin maininneita**	**n**	**Riskin maininneita**	**n**	**Muutos 2019–2023 (%-yks.)**
Energia	0,0 %	1	0,0 %	1	0,0 %	1	100,0 %	1	100,0 %	1	100,0 %
Kiinteistöyhtiöt	20,0 %	5	25,0 %	4	25,0 %	4	25,0 %	4	25,0 %	4	5,0 %
Kulutuspalvelut	60,9 %	23	65,2 %	23	58,3 %	24	63,0 %	27	76,0 %	25	15,1 %
Kulutustuotteet	50,0 %	8	50,0 %	8	50,0 %	8	62,5 %	8	75,0 %	8	25,0 %
Perusteollisuus	62,5 %	8	75,0 %	8	71,4 %	7	77,8 %	9	77,8 %	9	15,3 %
Rahoitus	30,8 %	13	50,0 %	14	66,7 %	15	66,7 %	15	75,0 %	16	44,2 %
Teknologia	62,5 %	16	68,8 %	16	64,7 %	17	76,5 %	17	75,0 %	16	12,5 %
Teollisuustuotteet ja -palvelut	42,1 %	38	39,5 %	38	46,2 %	39	59,0 %	39	68,6 %	35	26,5 %
Terveydenhuolto	14,3 %	7	16,7 %	6	28,6 %	7	71,4 %	7	57,1 %	7	42,9 %
Tietoliikennepalvelut	75,0 %	4	66,7 %	3	66,7 %	3	100,0 %	3	100,0 %	3	25,0 %
Yleishyödylliset palvelut	50,0 %	2	50,0 %	2	50,0 %	2	100,0 %	2	66,7 %	3	16,7 %
Yhteensä	**47,2 %**	**125**	**51,2 %**	**123**	**53,5 %**	**127**	**65,9 %**	**132**	**71,7 %**	**127**	**24,5 %**

n = yrityksiä toimialalla

Yrityksen kokoluokan mukaan tarkasteltuna toimintakertomuksissa kuvatut kyberriskit jakautuvat taulukon 5 mukaisesti. Riskejä raportoivien yhtiöiden osuus on kasvanut kaikissa kokoluokissa vuosina 2019–2023, mutta kokoluokkien välillä on huomattavia eroja. Suurten yhtiöiden kokoluokassa vuonna 2019 kyberriskejä raportoitiin merkittävinä riskeinä ja epävarmuustekijöinä 57,6 prosentissa yhtiöistä ja vuoteen 2023 mennessä lähes kaikki yhtiöt (96,7 %) raportoivat niistä. Keskisuurissa yhtiöissä lähtötaso oli suuryrityksiä pienempi (48,9 %) ja osuus saavutti 70,8 prosentin tason vuoteen 2023 mennessä. Pienyhtiöiden lähtötaso (38,3 %) oli sekä suuryrityksiä että keskisuuria yrityksiä matalampi ja kasvoi tarkastelujakson loppuun mennessä 57,1 prosenttiin. Ero suuriyrityksiin vuoden 2023 aineistossa on peräti 39,5 %-yksikköä. Pienyritysten osuuden muutosnopeus on vuosina 2019–2023 keskisuuria ja suuria yrityksiä pienempi, joten ero niihin kasvoi tarkasteluajanjaksolla.

TAULUKKO 5 Kyber- ja tietoturvariskejä hallituksen toimintakertomuksessa kuvanneiden yritysten suhteelliset osuudet yrityksen kokoluokasta

	2019		2020		2021		2022		2023		
Kokoluokka	**Riskin maininneita**	**n**	**Riskin maininneita**	**n**	**Riskin maininneita**	**n**	**Riskin maininneita**	**n**	**Riskin maininneita**	**n**	**Muutos 2019–2023 (%-yks.)**
Pienet yhtiöt	38,3 %	47	39,6 %	48	41,2 %	51	54,7 %	53	57,1 %	49	18,8 %
Keskisuuret yhtiöt	48,9 %	45	54,5 %	44	53,3 %	45	63,3 %	49	70,8 %	48	21,9 %
Suuret yhtiöt	57,6 %	33	64,5 %	31	74,2 %	31	90,0 %	30	96,7 %	30	39,1 %
Yhteensä	**47,2 %**	**125**	**51,2 %**	**123**	**53,5 %**	**127**	**65,9 %**	**132**	**71,7 %**	**127**	24,5 %

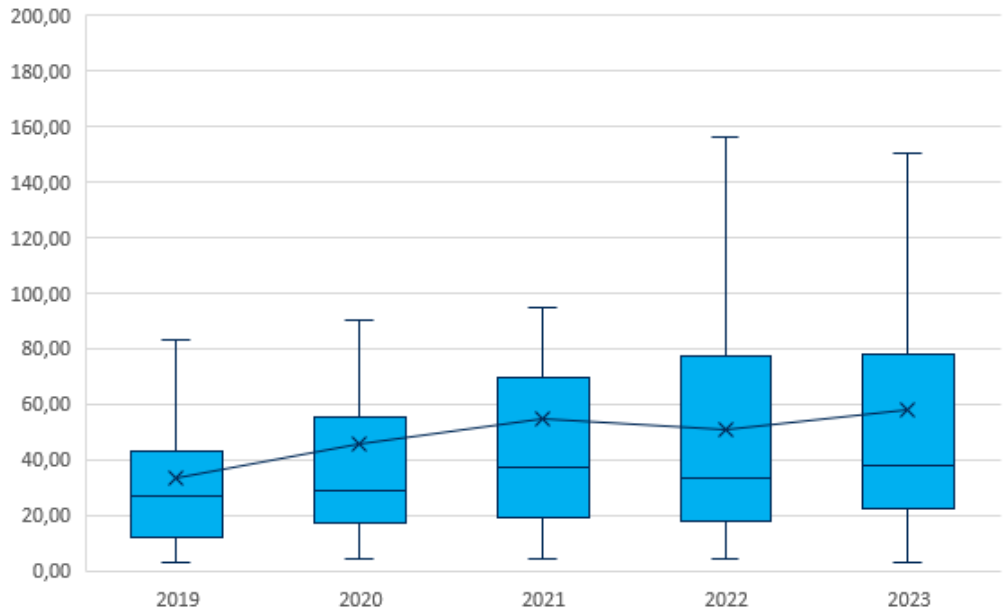
n = yrityksiä kokoluokassa

4.3 Raportoitujen kyberriskien sisältö

Kyber- ja tietoturvariskikuvausten pituus sanoina laskettiin aineistosta riskejä ja epävarmuustekijöitä kuvaavista osioista. Sanojen pituuden käyttö mittarina on mekaaninen menetelmä kuvata riskien sisältöä ja sitä kohtaan on esitetty kirjallisuudessa kritiikkiä (katso esim. Marston & Shrives, 1991). Poikittaistutkimusasetelmassa kritiikki on perusteltu, mutta usean vuoden aineistossa riskikuvausten pituuden tarkastelu mahdollistaa kehityksen ja trendien havaitsemisen. Taulukko 6 ja kuvio 5 esittävät vuosien 2019–2023 hallitusten vuosikertomuksissa esiintyvien kyber- ja tietoturvariskikuvauksien sanoina mitattujen pituuksien tunnuslukuja. Pienimmillään kuvaus on muutaman sanan minimalistinen toteamus ja pisimmillään kuvaus on 200–300 sanaa. Kuvausten pituuksien keskiarvo kasvaa tarkasteluajanjaksolla, mutta edelleen kyber- ja tietoturvariskejä kuvataan keskimäärin varsin niukkasanaisesti alle 60 sanalla – mittakaavaa antaa esimerkiksi tämä tutkimusraportin kappale, jossa on noin 100 sanaa.

TAULUKKO 6 Kyber- ja tietoturvariskikuvauksen pituuden kehitys

	2019	2020	2021	2022	2023
Maksimi	97	232	391	202	329
Minimi	3	4	4	4	3
Keskiarvo	33,2	45,3	54,4	51,1	57,6
Keskihajonta	25,8	43,0	59,6	44,9	55,8



KUVIO 5 Riskikuvauksien pituudet sanoina vuosittain

Riskikuvausten pituus ei suoraan kuvaa tunnistettujen kyber- ja tietoturvariskien sisältöä. Aineiston läpikäynnin yhteydessä riskikuvauksista erottui kuitenkin selvästi erilaisia kuvaustyyppejä. Riskikuvausten sisällön kuvaamiseksi kuvaukset tyypiteltiin seuraavien aineistosta tunnistettuihin tyyppeihin:

- Boilerplate-kuvaukset
- Kyberriskienhallintaa kuvailevat
- Yrityskohtaisia kyberriskejä kuvailevat
- Yrityskohtaisia kyberriskejä ja niiden hallintaa kuvailevat

Boilerplate-termillä viitataan amerikkalaisessa oikeuskäytännössä esiintyviin sopimustekstien yleisiin ehtoihin ja vastaaviin sisältöihin, jotka voidaan liittää sellaisinaan erilaisiin sopimuksiin sopimustyypistä ja yrityksen toimialasta riippumatta (Tieteen termipankki, 2020). Tässä yhteydessä *boilerplate-kuvauksella* tarkoitetaan sellaista kyber- tai tietoturvariskin kuvausta, joka on sisällöltään geneerinen ja se ei huomioi yritys- tai toimialakohtaisia erityispiirteitä. Boilerplate-kuvauksen sisältö jää niin ylätasolle, että sen voisi yhdistää mihin tahansa nykyaikaisessa digitalisoituneessa ympäristössä toimivaan yritykseen. *Kyberriskienhallintaa kuvailevilla* tarkoitetaan niitä kyber- ja tietoturvariskien kuvauksia, jotka keskittyvät yksinomaan näiden riskien hallitsemisen ja johtamisen kuvaamiseen, mutta ne eivät sisällä tietoja yritys- tai toimialakohtaisista erityispiirteistä. *Yrityskohtaisia riskejä kuvailevat* on tyypitys, jossa riskin kuvaus huomioi yrityksen toimintaan tai toimialaan liittyviä kyber- ja tietoturvariskejä. *Yrityskohtaisia riskejä ja niiden hallintaa kuvailevat* -tyypitys huomioi yritys- tai toimialakohtaiset piirteet riskin kuvauksessa ja kuvaa sen lisäksi riskienhallintaa.

Edellä kuvatun tyypittelyn mukaiset kyber- ja tietoturvariskien kuvaukset jakaantuvat suhteellisesti riskejä kuvanneiden yritysten kesken taulukon 7 mukaisesti. Vuonna 2019 kyber- ja tietoturvariskejä kuvanneista yrityksistä lähes 60 % tyytyi kuvailemaan riski yleisellä tasolla ottamatta kantaa yritys- tai toimialakohtaisiin piirteisiin. Boilerplate-kuvauksien taso on pysynyt koko tarkastelujakson ajan korkealla ja vuonna 2023 vielä yli kolmannes yrityksistä raportoi riskeistään tämän tyypityksen mukaisesti. Kuitenkin saman aikaan kuitenkin yrityskohtaisia riskejä, mukaan lukien riskienhallintaa ja yrityskohtaisia riskejä, kuvailevien yrityksien osuus on noussut vastaavasti vuoteen 2023 mennessä lähes 60 prosenttiin. Tämän perusteella voidaan todeta, että samalla kun kyber- ja tietoturvariskejä raportoidaan merkittävinä riskeinä ja epävarmuustekijöinä yhä useammin, ovat myös niiden kuvaukset muuttuneet enemmän yrityskohtaisiksi yleiselle tasolle jäävien kuvausten sijaan.

TAULUKKO 7 Riskikuvausten tyypittelyn suhteelliset osuudet ja niiden kehitys

	2019	2020	2021	2022	2023
Boilerplate-kuvaukset (%)	59,3 %	54,0 %	48,5 %	44,8 %	35,2 %
Kyberriskienhallintaa kuvailevat (%)	3,4 %	1,6 %	1,5 %	6,9 %	5,5 %
Yrityskohtaisia kyberriskejä kuvailevat (%)	25,4 %	36,5 %	30,9 %	31,0 %	39,6 %
Yrityskohtaisia kyberriskejä ja niiden hallintaa kuvailevat (%)	11,9 %	7,9 %	19,1 %	17,2 %	19,8 %
Yhteensä	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %
Riskejä kuvanneita yrityksiä yhteensä	**59**	**63**	**68**	**87**	**91**

Hallituksen toimintakertomuksen laadinnassa noudatettava johdonmukaisuus ja jatkuvuuden periaate ilmenevät myös kyberriskien kuvauksissa. Erityisesti, ja ehkä valitettavasti, se näkyy boilerplate-tyyppisissä kuvauksissa. Kun tämän tyyppinen riskikuvaus on kerran sisällytetty toimintakertomukseen, toistuu se todennäköisesti sellaisenaan myös tulevina vuosina. Esimerkkinä tämäntyyppisesti kyberriskin kuvaamisesta voidaan mainita seuraavat esimerkit:

> Myös tietoturvaan ja kyberuhkiin liittyvillä riskeillä voi olla haitallinen vaikutus Robitin liiketoiminnalle (Robit Oyj, 2024, s. 48).

> Kyberhyökkäykset ovat kasvavia riskejä ja ne voivat pahimmillaan haitata merkittävästi yhtiön toimintaa (HKScan Oyj, 2022, s. 24).

> Tietoturvaan ja kyberuhkiin liittyvät riskit voivat haitata Metson liiketoimintaa (Metso Oyj, 2024, s. 10).

Näiden kuvausten sisältöä ei voi kiistää, koska toteutuneilla kyberuhkilla on haitallisia vaikutuksia. Riskin luonnehdinta jää kuitenkin niin geneeriselle tasolle, että kuvausta voisi käyttää sellaisenaan yritys kuin yritys, ja sen perusteella lukijan on hankala saada kuvaa siitä, mikä kyberriskin luonne, merkitys ja vaikutus yritykselle todellisuudessa on. Kyberriskien hallintaa kuvaavista tyypityksistä esimerkkinä toimii seuraava kuvaus:

> QPR Software tarkkailee ja pyrkii minimoimaan säännöllisesti tietoturvariskejä operatiivisella tasolla sekä raportoimalla yhtiön hallitukselle. Edistämme sekä hallinnollisia että teknisiä toimia järjestelmien turvallisuuden parantamiseksi. Tietoturvariskien vähentämiseksi olemme ottaneet käyttöön tieto- ja toimittajahallintamalleja, suorittaneet kumppaneille vuosittaisia tarkastuksia, sekä järjestäneet asianmukaisia sisäisiä koulutuksia tietoturvallisuustietoisuuden parantamiseksi. QPR:n tieto- ja tuoteriskeissä ei ole tapahtunut merkittäviä muutoksia vuoden 2021 aikana (QPR Software Oyj, 2022, s. 24).

QPR Softwaren sitaatissa kuvataan niitä prosesseja ja menettelytapoja, joita yhtiö on ottanut käyttöön tietoturvariskien hallitsemiseksi. Niiden luonnehdinta on varsin yleisellä tasolla, mutta mukana on myös yrityskohtaisia elementtejä. Tietoturvariskin luonnetta, merkitystä ja vaikutusta yritykselle ei kuvauksessa ole. Myös tietoturvariskien hallinnan kuvauksissa on havaittavissa boilerplate-tyylisiä ilmaisuja. Ääriesimerkki tällaisesta on Tulikivi Oyj:n toiminnallisia ja prosessiriskejä kuvaavassa osuudessa:

> Konsernin liiketoiminta perustuu toimiville ja luotettaville tietojärjestelmille. Toiminnanohjausjärjestelmien hyödyntämiseen liittyy riskejä, mikäli liiketoimintaprosesseissa ei omaksuta uusia toimintatapoja eikä uusien järjestelmien mukanaan tuomia mahdollisuuksia nopealla aikataululla. Tietojen käyttövalmiuteen liittyviä riskejä pyritään hallitsemaan muun muassa kahdentamalla kriittiset tietojärjestelmät ja tietoliikenneyhteydet, kiinnittämällä huomiota yhteistyökumppaneiden valintaan sekä standardoimalla käytössä olevia työasemamalleja ja ohjelmistoja sekä tietoturvaan liittyviä menettelytapoja (Tulikivi Oyj, 2024, s. 85).

Yllä oleva kuvaus vaikuttaa ensisilmäyksellä harkitulta kuvaukselta siitä, millaisia toimenpiteitä yhtiössä on toteutettu tietojen saatavuuden ja toiminnan jatkuvuuden turvaamiseksi. Lähempi tarkastelu kuitenkin osoittaa, että teksti on yhtä lisättyä virkettä lukuun ottamatta kopioitu sellaisenaan Kirjanpitolautakunnan vuonna 2006 julkaistusta toimintakertomuksen laadintaa koskevan yleisohjeen esimerkinomaisista riskikuvauksista:

> Konsernin liiketoiminta perustuu toimiville ja luotettaville tietojärjestelmille. Niihin liittyviä riskejä pyritään hallitsemaan mm. kahdentamalla kriittiset tietojärjestelmät ja tietoliikenneyhteydet, kiinnittämällä huomiota yhteistyökumppaneiden valintaan sekä standardoimalla käytössä olevia työasemamalleja ja ohjelmistoja sekä tietoturvaan liittyviä menettelytapoja (Kirjanpitolautakunta, 2006, s. 55).

On toki mahdollista, että näin raportoinut yhtiö on toteuttanut kuvaamansa toimenpiteet ja toimintamallit – ne ovat kuitenkin varsin tavanomaisia ja yleisluontoisia. Tekstin suora kopiointi herättää kuitenkin epäilyksen siitä, kuinka tosiasiallisesti se kuvaa yhtiön toimenpiteitä tietoturvallisuuden parantamiseksi.

Yhä suurempi osa yhtiöistä kuvaa kyberriskejään laajemmin oman liiketoimintansa kontekstissa. Seuraava sitaatti KONE Oyj:ltä havainnollistaa kyberriskin kuvauksen tyyppiä, jossa on mukana yrityskohtaisia elementtejä:

> KONEen liiketoiminnot ovat riippuvaisia tuotantolaitosten, hankintakanavien, operatiivisten palvelujärjestelmien ja logistiikkaprosessien toimintavarmuudesta, laadusta ja luotettavuudesta. Tietotekniikka on merkittävässä roolissa KONEen sekä sen toimittajien ja asiakkaiden toiminnassa, ja KONEen liiketoiminta on riippuvainen tiedon laadusta, oikeellisuudesta ja saatavuudesta. Tämä altistaa KONEen IT-häiriöille ja kyberturvallisuusriskeille, sillä operatiiviset tietojärjestelmät ja -tuotteet voivat olla alttiita toiminnan keskeytymiselle, tiedon häviämiselle tai manipuloimiselle sekä toimintahäiriöille, mikä puolestaan voi johtaa keskeytyksiin prosessien ja tuotteiden saatavuudessa. Geopoliittiset jännitteet voivat johtaa kyber-, hybridi- ja jopa perinteisiin sodankäynnin hyökkäyksiin. Näistä voi aiheutua paikallisia ja globaaleja digitaalisia häiriöitä, joilla voi olla vaikutus KONEeseen, asiakkaisiin ja toi-

> mittajiin. Arkaluontoisen työntekijä- tai asiakasdatan tietovuodot voivat johtaa merkittäviin taloudellisiin seurauksiin ja mainehaittoihin. Tällaiset tilanteet voisivat johtua muun muassa kyberrikoksista, kyberhyökkäyksistä, kiristysohjelmista, tietovarkauksista, petoksista, väärinkäytöksistä tai KONEen työntekijöiden tai toimittajien tahattomista virheistä (KONE Oyj, 2024, s. 32).

KONEen kuvaama kyberriski on jo pituudeltaankin yleiselle tasolle jääviä luonnehdintoja laajempi. Kuvauksessa tuodaan esiin yhtiön riippuvuus toimivista tietojärjestelmistä ja niiden toimittajista. Tiedon laadun, saatavuuden ja oikeellisuuden merkitys liiketoiminnalle on tunnistettu. Kuvauksessa viitataan geopoliittisen tilanteen muutokseen ja sen mahdollisiin vaikutuksiin myös kybertilassa. Kyberriskeissä on tunnistettu laajasti erilaisia uhkia, kuten tietovuodot ja -varkaudet, petokset, kiristyshaittaohjelmat sekä työntekijöiden ja toimittajien tahattomat virheet. Lisäksi kyberriskin toteutumisen seurauksia on kuvauksessa arvioitu.

Neljäs riskikuvaustyyppi sisältää yrityskohtaisten elementtien lisäksi kuvauksen siitä, miten yritys hallitsee kyberriskejään. Tällaista kuvauksista hyvänä esimerkkinä toimii seuraava:

> Asiakkaiden, sidosryhmien ja yhteiskunnan luottamus perustuu palveluiden lähes sataprosenttiseen saatavuuteen. Palvelukatkoksia voi aiheutua esimerkiksi laitteiston tai ohjelmiston häiriöistä, sähkökatkoista, luonnonkatastrofeista sekä erityyppisistä tahallisista tai tahattomista toimista.
>
> Liiketoimintansa puitteissa Tietoevry käsittelee ja säilyttää suuria määriä luottamuksellista tietoa, johon kuuluu julkisen ja yksityisen sektorin asiakkaiden ja liikekumppaneiden tietoja sekä myös yhtiön omia tietoja. Nämä sisältävät myös arkaluonteisia henkilötietoja. Uhkaympäristö kasvaa ja muuttuu jatkuvasti. Esimerkiksi rikollisten hakkereiden tai haktivistien toiminnasta, inhimillisistä erehdyksistä tai väärinkäytöksistä ja valtioiden tukemien organisaatioiden toiminnasta voi aiheutua toiminnan häiriöitä tai kyberturvallisuusuhkia, jotka kohdistuvat Tietoevryyn, sen asiakkaisiin, alihankkijoihin tai muihin kolmansiin osapuoliin.
>
> Ainakin seuraavat uhat ovat riskitekijöitä, jotka voivat johtaa tiedon menetykseen, väärinkäyttöön tai tuhoutumiseen taikka järjestelmävirheisiin ja tällä tavoin heikentää Tietoevryn kykyä tukea, hallita tai kehittää palveluita:
>
> • kiristysohjelmat
> • hyökkäykset toimitusketjua vastaan
> • kriittiset tietoturva-aukot
> • kohdistetut hyökkäykset
> • digitaaliset petokset
> • palvelunestohyökkäykset
> • tietoturvaloukkaukset ja tietovuodot
> • sisäpiiriuhat.
>
> Näillä saattaisi olla kielteinen vaikutus yhtiön taloudelliseen kehitykseen ja maineeseen. Kyberturvallisuusrikkomusten havaitsemista ja tutkintaa varten Tietoevry on toteuttanut kattavan merkittävien tapahtumien hallinnan ja eskaloinnin prosessin, kriisienhallintaprosessin sekä tehokkaan kyberturvallisuuden suojausjärjestelmän,

> joiden korkeatasoiset uhkien tunnistus- ja reagointitoiminnot vähentävät palvelukatkoksia.
>
> Yhtiö käy säännöllisesti läpi riskienhallintaan ja kyberturvallisuuteen liittyvää toimintaansa, kouluttaa työntekijöitään parantaakseen heidän tietoisuuttaan kyberuhista ja mittaa kyberturvallisuustoimiaan jatkuvasti (Tietoevry Oyj, 2024, s. 56).

Tietoevryn hallituksen toimintakertomukseen sisältyvä kuvaus kyberturvallisuuteen liittyvistä riskeistä on monipuolinen. Siinä korostuvat alati muuttuva uhkaympäristö sekä erilaiset uhkatoimijat. Kuvauksessa kyberturvallisuusriskit saattavat realisoitua tahattoman inhimillisen toiminnan seurauksena tai tahallisesti kyberrikollisten sekä valtiollisten toimijoiden toimesta. Tietoevryn lisäksi vain yksi toinen yhtiö nimesi valtiolliset toimijat kyberuhkatoimijana. Uhkatekijöiden lisäksi Tietoevry on yksilöinyt joukon erityyppisiä kyberhyökkäyksen tai -vaikuttamisen muotoja, joilla voi olla vaikutusta sen toimintaan. Onnistuneen kyberhyökkäyksen vaikutukset yhtiön talouteen ja maineeseen on myös mainittu. Riskin kuvaamisen lisäksi Tietoevry mainitsee riskiin varautumiseen ja hallintaan liittyviä prosesseja ja toimintamalleja.

Tutkimuksen aineistosta pyrittiin tunnistamaan raportoijan itsensä määrittelemä luokittelu kyberriskeille. Luokittelua käytetään aineiston raporteissa vaihtelevasti ja terminologia ei tältä osin ole vakiintunutta. Osa yhtiöistä esittää riskit jaettuna esimerkiksi strategisiin, operatiivisiin, rahoitukseen liittyviin ja vahinkoriskeihin. Osa yhtiöistä puolestaan kuvaa riskejä luokittelematta niitä sen tarkemmin. Tämän takia aineistosta ei voi esittää yhteismitallista määrällistä kuvausta, kuinka kyberriski on luokiteltu aineiston raporteissa. Se voidaan kuitenkin todeta, että yksikään yritys ei eksplisiittisesti maininnut kyberriskejä strategisena riskinä. Jos riskien luokittelua oli käytetty, tyypillisimmin kyberturvallisuuteen liittyvät riskit käsiteltiin operatiivisten tai liiketoimintariskien otsikoiden alla. Merkille pantava huomio on se, että muutamat yhtiöt luokittelevat kyberriskit vahinkoriskeiksi. Näin ymmärrettynä kyberriski toteutuu vahinkotapahtuman seurauksena, joka on toki mahdollista, mutta se ei kata kyberriskin todellista luonnetta. Nykyään suuri osa kyberriskistä tulee organisaation ulkopuolelta ja on luonteeltaan tarkoituksellista, kuten esimerkiksi kyberrikollisuus.

4.4 Raportoitujen uhkatyyppien kehitys

Aineiston koodaamisessa kyberriskikuvauksista kerättiin niissä mainittuja uhkatyyppejä, joilla tarkoitetaan kyberuhkan konkreettista ilmenemismuotoa tai toimijaa, joka uhkan muodostaa. Uhkatyyppien koodaamisella oli tarkoituksena muodostaa kuva siitä, millaisia uhkatyyppejä kuvauksissa esiintyy ja mitkä ovat niiden esiintymistiheydet. Taulukko 8 esittää toimintakertomuksissa kuvattujen kyberuhkien suhteellista osuutta kyberriskejä raportoineista yrityksistä – kuinka monta prosenttia mainitsi kunkin uhkan kaikista kyberriskejä rapor-

toineista yrityksistä. Taulukon rivit on järjestetty alenevaan järjestykseen siten, että eniten mainintoja saanut uhka esitetään ylimpänä ja vähiten mainintoja saanut vastaavasti alimpana. Lisäksi taulukossa on koodi *nimeämätön kyber- tai tietoturvauhka,* jolle data koodattiin siinä tapauksessa, että kyberriskin kuvauksessa puhuttiin uhkasta yleisellä tasolla mitään yksittäistä uhkatyyppiä nimeämättä. Taulukosta voidaan havaita, että vuonna 2019 lähes puolet kyberriskin kuvauksista pysytteli yleisellä tasolla ja uhkatyyppejä raportoitiin harvakseltaan. Ajan kuluessa kyberuhkatyyppejä aletaan tunnistamaan ja nimeämään yksilöidymmin. Tarkemmin yksilöimättömän kyberuhkan käyttö riskikuvauksissa jatkuu kuitenkin korkeana koko tarkasteluajanjakson ajan, mutta sen rinnalla nousee käsite *kyberhyökkäys* yleisimmäksi kyberuhkaksi vuoteen 2023 mennessä. Kyberhyökkäys-käsitteenä on edelleen varsin abstrakti ja voi tarkoittaa hyvin erilaisia asioita. Siitä näyttää kuitenkin tulleen yleisnimi kuvaamaan kybertoimintaympäristössä ilmeneviä ei-toivottuja tapahtumia. Kyberrikollisuus mainitaan uhkana koko tarkasteluajanjakson aikana ja se on toiseksi useimmiten mainittu kyberuhka. Tiedotusvälineissä laajasti esillä olleet ja toteutuneet kiristyshaittaohjelmahyökkäykset ja palvelunestohyökkäykset mainitaan riskikuvaukissa verrattain harvoin.

TAULUKKO 8 Raportoiduissa kyberriskeissä esiintyneiden uhkatyyppien kehitys

Raportoitu uhkatyyppi	2019	2020	2021	2022	2023
Kyberhyökkäys	10,2 %	12,7 %	20,6 %	33,3 %	38,5 %
Kyberrikollisuus	8,5 %	11,1 %	13,2 %	13,8 %	15,4 %
Tietojen väärinkäyttö	13,6 %	12,7 %	8,8 %	9,2 %	14,3 %
Tietovuodot	5,1 %	9,5 %	10,3 %	12,6 %	13,2 %
Työntekijän virhe	8,5 %	9,5 %	10,3 %	12,6 %	12,1 %
Digitaaliset petokset	3,4 %	7,9 %	11,8 %	12,6 %	8,8 %
Toimitusketjuhyökkäykset	3,4 %	1,6 %	8,8 %	10,3 %	8,8 %
Haittaohjelmat	5,1 %	6,3 %	7,4 %	4,6 %	8,8 %
Tietovarkaus	6,8 %	6,3 %	8,8 %	13,8 %	7,7 %
Tietomurto ja luvaton pääsy järjestelmään	1,7 %	11,1 %	7,4 %	10,3 %	7,7 %
Kiristyshaittaohjelmat	1,7 %	1,6 %	4,4 %	4,6 %	5,5 %
Palvelunestohyökkäykset	0,0 %	1,6 %	2,9 %	4,6 %	4,4 %
Ohjelmistojen haavoittuvuudet	0,0 %	0,0 %	2,9 %	3,4 %	4,4 %
Tietojenkalastelu	0,0 %	1,6 %	4,4 %	3,4 %	2,2 %
Valtiolliset toimijat	0,0 %	0,0 %	1,5 %	1,1 %	2,2 %
Sisäpiiriuhat	0,0 %	0,0 %	1,5 %	1,1 %	1,1 %
Nimeämätön kyber- tai tietoturvauhka	49,2 %	52,4 %	38,2 %	44,8 %	33,0 %

4.5 Raportoitujen kyberriskien vaikutukset ja seuraukset

Yritysten raportoimista kyberriskien kuvauksista koodattiin niissä mainitut kyberriskien toteutumisesta aiheutuvat vaikutukset ja seuraukset. Taulukossa 9 esitetään yhteenveto riskikuvauksista tunnistetuista kyberriskien mahdollisista seurauksista ja vaikutuksista. Taulukossa olevat suhteelliset osuudet kuvaavat eri vaikutusten esiintyvyyttä kyberriskejä kuvanneissa yrityksissä. Koodia *määrittelemätön haitta* on käytetty silloin kun kyberriskien toteutumisella on todettu yleisesti olevan haitallinen vaikutus yritykselle. Koodia *Viranomaisten toimenpiteet* on puolestaan käytetty tilanteissa, joissa riskin raportoinut viittaa viranomaisten valvontaan, seuraamusmaksuihin, sakkoihin tai rikosseuraamuksiin. Yleinen trendi vaikutusten kuvaamisessa on samansuuntainen kuin nimetyissä uhkatyypeissä ja riskimainintojen esiintyvyydessä: tarkasteluajanjakson kuluessa maininnat kyberriskeihin liittyvistä vaikutuksista lisääntyvät ja ne ilmaistaan täsmällisemmin. Tarkasteluajanjakson päättyessä vuonna 2023 yli kolmasosa yritysten kyberriskikuvauksista mainitsee toiminnan häiriöt, taloudelliset haitat ja mainehaitat kyberriskien toteutumisen seurauksena. Yleisesti käytetty tapa kuvata kyberriskien toteutumisen vaikutuksia on myös viitata kyberturvallisuuden kirjallisuudessa laajasti käytettyyn CIA-kolmioon (katso esim. Raggad, 2010, s. 20), jolla tarkoitetaan tiedon luottamuksellisuuden, eheyden ja saatavuuden turvaamista. Mielenkiintoinen havainto on ajan kuluessa laskeva esiintymistiheys maininnoille *vaatimusten mukaisuuden vaarantumisesta.* Tämä voi

liittyä EU:n yleiseen tietosuoja-asetukseen (GDPR), jota alettiin soveltaa jäsenvaltioissa vuonna 2018. Yleinen tietosuoja-asetus lienee ollut laajasti myös yritysten hallitusten työjärjestyksissä ja yleisen tietosuoja-asetuksen muututtua enemmän päivittäiseksi operatiiviseksi toiminnaksi viittaukset vaatimusten mukaisuuden vaarantumiseen vähenevät hallitusten riskiarvioissa.

TAULUKKO 9 Kyberriskien seuraukset ja vaikutukset

Vaikutus tai seuraus	2019	2020	2021	2022	2023
Toiminnan häiriö tai keskeytyminen	16,9 %	23,8 %	39,7 %	25,3 %	37,4 %
Taloudellinen haitta	23,7 %	28,6 %	35,3 %	35,6 %	36,3 %
Mainehaitta	13,6 %	20,6 %	29,4 %	32,2 %	36,3 %
Tiedon luottamuksellisuuden vaarantuminen	11,9 %	12,7 %	11,8 %	13,8 %	14,3 %
Tiedon häviäminen tai manipulaatio	6,8 %	9,5 %	4,4 %	4,6 %	9,9 %
Tiedon eheyden vaarantuminen	6,8 %	11,1 %	8,8 %	8,0 %	8,8 %
Tiedon saatavuuden vaarantuminen	11,9 %	11,1 %	8,8 %	10,3 %	7,7 %
Viranomaisten toimenpiteet*	0,0 %	4,8 %	8,8 %	8,0 %	7,7 %
Vaatimustenmukaisuuden vaarantuminen	13,6 %	19,0 %	16,2 %	9,2 %	4,4 %
Määrittelemätön haitta	13,6 %	14,3 %	8,8 %	14,9 %	3,3 %
Sopimusrikkomus	0,0 %	1,6 %	1,5 %	1,1 %	0,0 %

*Valvonta, seuraamusmaksu, sakot, rikosseuraamukset

4.6 Kyberriskikuvauksissa esiintyvien teemojen kehittyminen vuosina 2019–2023

Tutkimus kattaa ajanjakson 2019–2023, jolloin kävi toteen useita yhteiskunnallisesti merkittäviä turvallisuuteen vaikuttavia tapahtumia ja ilmiöitä. Tutkimuksen tarkasteluajanjakson alkua edeltävä vuonna 2018 Euroopan unionissa oli alettu soveltaa yleistä tietosuoja-asetusta, jolla oli merkittäviä vaikutuksia organisaatioiden henkilötietojen käsittelyyn. Loppuvuonna 2019 Kiinasta havaitut COVID-19 tartunnat laajenivat globaaliksi pandemiaksi vuoden 2020 aikana ja vaikutti suuresti ihmisten ja yhteiskuntien toimintaan seuraavien vuosien aikana. Helmikuussa 2022 Venäjä laajensi aggressioitaan täysimittaiseksi hyökkäyssodaksi Ukrainassa, joka muutti dramaattisesti eurooppalaista turvallisuusarkkitehtuuria. Vaikka osa kyberriskien kuvauksista hallitusten toimintakertomuksissa on varsin lyhyitä ja ne kuvaavat kyberriskejä melko yleisellä tasolla, on niissä havaittavissa usein toistuvia ja myös ajan kuluessa kehittyviä teemoja. Näissä teemoissa näkyvät nykyaikaisen tietoyhteiskunnan kehitys ja ympäröivän maailmantilanteen muutokset.

Tietosuoja esiintyy aineistossa teemana läpi koko tarkasteluajanjakson. Tietosuojaan liittyviä riskejä tunnistetaan jossain määrin, mutta se ei ole hallitseva teema riskikuvauksissa. Yritysten vastuullisuusraportit eivät olleet tämän

tutkimuksen varsinaisena aineistona, mutta osalla tutkimuksen kohteena olleista yrityksistä vuosiraporttiin tai vastaavaan sisältyy myös vastuullisuutta käsittelevä osuus. Tietosuojaan ja tietoturvaan liittyvä teemoja on näissä osuuksissa käsitelty varsin usein. Tietosuoja ja -turva on selvästi yksi ulottuvuus, jonka kautta yritysten yhteiskuntavastuuta tarkastellaan ja yrityksen vastuullista toimintaa legitimoidaan.

Vuodesta 2020 alkaen hallitusten toimintakertomuksissa kuvatuissa riskeissä ja epävarmuuksissa käsitellään laajasti COVID-19 pandemiaa ja sen vaikutuksia. COVID-19 pandemiaan liittyvät sulkutoimet ja siirtyminen etätyöskentelyyn kiihdyttivät yritysten digitalisaatiota (KPMG, 2020; McKinsey & Company, 2020; Wade & Shan, 2020). Digitalisaatio lisääntyi erityisesti toimialoilla, joissa ollaan paljon lähikontaktissa toisten ihmisten kanssa, ja pienissä yrityksissä (Jaumotte ym., 2023). Näillä toimialoilla ja yrityksissä digitalisaatioasteen lähtötaso oli myös alhaisempi ennen pandemiaa, joten suhteellinen lisäys oli siten myös suurempi. Vaikka COVID-19 pandemia oli globaali ja vaikutuksiltaan laaja ilmiö, on sen mahdollisista vaikutuksista kyberturvallisuuteen kuvattu suomalaisten pörssiyritysten riskiarvioissa vain harvakseltaan. Aineistossa esiintyy vain muutamia mainintoja kyberturvallisuusriskien kasvamisesta esimerkiksi lisääntyneet etätyöskentelyn seurauksena.

> UPM:n tietojärjestelmiin voi kohdistua erilaisia tietoturvariskejä. Vihamielinen kyberhyökkäys voisi johtaa luottamuksellisten tietojen vuotamiseen, tietosuojasäännösrikkomuksiin, immateriaalioikeusvarkauksiin, tuotantokatkoksiin ja UPM:n maineen vahingoittumiseen. Nämä riskit voivat myös lisääntyä COVID-19- pandemian seurauksena. (UPM-Kymmene Oyj, 2021, s. 132)

> The COVID-19 pandemic has resulted in a number of employees working remotely in order to continue servicing customers. In this situation, Nordea has continuously been assessing the risks and introduced remediation activities. This includes technical and organisational controls, as well as an increased focus on security awareness and training for all staff. Whilst we noticed many COVID-related cyber-attacks across the industry, Nordea has maintained the high resilience level in protecting customer data and services. (Nordea Bank Abp, 2021, s. 61)

Vaikka COVID-19 pandemia ei nouse laajasti esiin kyberturvallisuusriskejä lisäävänä ilmiönä, on digitalisaatio yleisesti esillä kyberriskien kuvauksissa. Digitalisaation tunnistetaan luovan uusia liiketoimintamahdollisuuksia, mutta aiheuttavan myös uusia uhkia. Digitalisaation ohella riippuvuus tietojärjestelmistä on usein teemana läsnä kyberriskejä kuvailtaessa. Myös riippuvuus palvelutoimittajista mainitaan usein, vaikka varsinaisia toimitusketjuhyökkäyksiä ei nimetä suoraan uhkaksi kovinkaan usein. Toisaalta riippuvuutta tietojärjestelmistä voidaan pitää varsin itsestään selvänä, joten sen korostaminen riskikuvauksessa ei tosiasiallisesti heijastane yrityskohtaista riskiä verrattuna muihin yrityksiin. Lisäksi kyberuhkien luonnehditaan lisääntyneen ja niitä pidetään kehittyvänä ja monimutkaistuvana ilmiönä.

> Fiskars-konserni on yhä riippuvaisempi keskitetyistä tietoteknisistä järjestelmistä, jotka sisältävät ja joissa käsitellään kriittistä liiketoimintatietoa, sekä palvelutoimittajista, jotka käsittelevät tällaista tietoa. Fiskars-konserniin tai sen palvelutoimittajiin kohdistuvat rikkomukset, toimintahäiriöt, kyberhyökkäykset ja petosyritykset voivat aiheuttaa keskeytyksiä yhtiön toiminnoissa alueellisella tai maailmanlaajuisella tasolla. (Fiskars Oyj Abp, 2024, s. 30)

> Kyberuhkien maailmanlaajuinen lisääntyminen sekä kasvava riippuvuus digitaalisesta infrastruktuurista aiheuttavat riskejä Harvian liiketoiminnalle ja kriittiselle datalle. (Harvia Oyj, 2024, s. 69)

> Kyberriskien uhkan taso on myös lisääntynyt viime aikoina, ja viranomaiset ovat varoittaneet kyberhyökkäysten uhasta ja määrän kasvusta. On jo tullut ilmi raportoituja tapauksia kyberhyökkäyksistä yrityksiä ja valtion viranomaisia kohtaan vakavin seurauksin. (Anora Group Oyj, 2024, s. 56)

Geopoliittisten jännitteiden lisääntyminen mainitaan yritysten riskejä ja epävarmuustekijöitä kuvatessa satunnaisesti vuosina 2019–2021. Luvussa 4.1 kyberriskimainintojen todettiin lisääntyneen 12,4 % edelliseen vuoteen verrattuna. Vuonna 2022 ja 2023 geopoliittisen tilanteen muutos esiintyy riskikuvauksissa yhä useammin kyberturvallisuusuhkia lisäävänä teemana, ja yritykset tunnistavat yhä paremmin kyberturvallisuusuhkat osana laajempaa turvallisuuden kontekstia.

> Ukrainan kriisistä ja Suomen Nato-jäsenyyden hakupäätöksestä johtuen uhka erilaisiin kyberhyökkäyksiin on pysynyt korkeana ja myös Aktiaa kohtaan on esiintynyt lyhytkestoisia palvelunestohyökkäyksiä, jotka eivät kuitenkaan ole suoranaisesti vaikuttaneet palveluihin. Aktia on toiminut koko vuoden aktiivisesti yhteistyössä sekä erilaisten viranomaisten että toimialan muiden toimijoiden kanssa kyberrikollisuuden ehkäisemiseksi. (Aktia Pankki Oyj, 2023, s. 20)

> Kyberhyökkäysten riski on epävakaan geopoliittisen tilanteen vuoksi aiempaa suurempi. Lähialueilla yhä useampi elintarvikealan yritys on joutunut kyberhyökkäyksen kohteeksi. Toteutuessaan kyberhyökkäykset voisivat haitata merkittävästi yhtiön toimintaa. (HKScan Oyj, 2024, s. 25)

> Geopoliittiset jännitteet jatkuivat Euroopassa vuonna 2023. Venäjän sodalla Ukrainaa vastaan ja sen seurauksena asetetuilla Venäjän vastaisilla pakotteilla ei arvioida olevan merkittävää suoraa vaikutusta yhtiöön. Kyberriski ja tietojärjestelmien häiriöt voivat vaikuttaa tuotantoon. (Incap Oyj, 2024, s. 45)

4.7 Signalointi- ja legitimiteettiteorian näkökulma raportoituihin kyberriskeihin

Aineiston kvantitatiivisen erittelyn perusteella kyberriskien raportointi pörssiyhtiöiden hallitusten toimintakertomuksissa on lisääntynyt merkittävästi vuo-

sina 2019–2023. Selittääkö tätä samaan aikaan muutenkin yleisemmäksi tulleet kyberhäiriötilanteet ja -uhkat, vai onko muutoksen taustalla muitakin mekanismeja? Vaikka toimintakertomuksen sisältöön lakisääteisesti kuuluu johdon arvio liiketoiminnan riskeistä ja epävarmuustekijöistä, on toimintakertomuksen laatijalla harkinnanvaraa riskien sisällön, yksityiskohtien ja laajuuden kuvaamisen osalta.

Signalointiteorian näkökulmasta kyberriskeistä viestiminen, signalointi, vähentää informaation epäsymmetriaa yrityksen ja sen sidosryhmien välillä. Pörssiyhtiön sidosryhmiä ovat omistajat, ulkopuoliset rahoittajat, analyytikot ja muut tahot, joiden intresseissä on ymmärtää yritykseen liittyviä riskejä. Kertomalla kyberriskeistä yritys signaloi sidosryhmilleen huomioineensa yhteiskunnallisia muutoksia ja varautuneensa uusiin uhkiin. Tehokas signalointi edellyttäisi, että riskikuvaukset olisivat yrityskohtaisia ja riittävän yksityiskohtaisia. Aineiston perusteella kyberriskejä kuvataan yleisesti ja karkealla tasolla, jolloin signalointivaikutus jää heikoksi.

Lisääntynyt kyberriskien raportointi hallitusten toimintakertomuksissa voi olla myös seurausta raportointikäytäntöjen yhdenmukaistumisesta. Laaja boilerplate-tyyppisten kuvausten käyttö saattaisi indikoida sitä, että kyberriskeistä raportoidaan yhä useammin, koska ”muutkin raportoivat niistä”. Tällöin selittävänä mekanismina olisi jäljittelemällä tapahtuva organisaatioiden yhdenmukaistuminen tai ammattiyhteisön normatiivisista käytännöistä johtuva yhdenmukaistuminen.

Toisaalta kyberriskeistä raportoinnin voidaan ajatella rakentavan yritysten institutionaalista legitimiteettiä. Suomalaisen yhteiskunnan turvallisuus perustuu kokonaisturvallisuuden malliin, jossa yritykset ovat yksi toimija. Geopoliittisten teemojen nousu vuonna 2022 kyberriskikuvauksiin voi kertoa siitä, miten yritykset kokevat roolinsa yhteiskunnassa. Viranomaiset ovat toistuvasti tuoneet esiin kasvavat kyberuhkat ja kehottaneet kansalaisia ja yrityksiä varautumaan niihin. On mahdollista, että kyberriskien lisääntynyt raportointi hallitusten toimintakertomuksissa on keino viestiä, että yritykset ovat reagoineet viranomaisten esittämiin huoliin.

5 JOHTOPÄÄTÖKSET

Tämän tutkimuksen tavoitteena oli selvittää, mitä ja miten suomalaiset pörssiyhtiöt ovat raportoineet kyberriskeistä ja -uhkista vuosina 2019–2023 hallitusten toimintakertomuksissaan. Tutkimuksen aineisto kattoi kaikki Suomen kirjanpitolain mukaisen toimintakertomuksen julkaisseet pörssiyhtiöt vuosina 2019–2022 ja viittä yhtiötä lukuun ottamatta kaikki vuonna 2023. Tutkimusasetelma oli pitkittäistutkimus, joka mahdollistaa trendien ja muutosten havainnoimisen tutkittavassa perusjoukossa. Tutkimuskysymykseen vastattiin sekä määrällisen että laadullisen sisällönanalyysin tekniikoita systemaattisesti käyttäen.

Tutkimusaineiston avainsana-analyysin tuloksista voidaan päätellä, että kyber- ja tietoturvallisuus sekä tietosuojaan liittyvät teemat ovat osa listattujen yhtiöiden vuosiraportointia. Vaikka dokumenttien pääsisältö keskittyy taloudellisen informaation jakamiseen, on myös ei-taloudellisella informaatiolla keskeinen rooli yhtiöiden sidosryhmäviestinnässä. Digitalisoituminen on megatrendi yhteiskunnassa ja yrityksen joutuvat ottamaan kantaa digitalisoitumisen mahdollisuuksiin ja uhkiin viestinnässään. Avainsanahaun tulokset osoittivat, että kyberturvallisuuteen ja tietosuojaan liittyvät teemat ovat läsnä enemmistössä listayhtiöiden vuosiraportteja. Näistä teemoista raportoivien yritysten osuus kasvaa tutkimuksen tarkasteluajanjaksolla. Avainsanahaun osumia esiintyy niin hallitusten toimintakertomusten riskejä ja epävarmuustekijöitä kuvaavissa osuuksissa kuin yhtiön hallintoa ja vastuullisuutta kuvaavissa osuuksissa. Tutkimuskysymyksessä analyysi rajattiin koskemaan ainoastaan hallituksen toimintakertomuksen sisältäneitä osuuksia.

Tämän tutkimuksen keskiössä oli yritysten hallitusten toimintakertomuksiin sisältyneet kuvaukset kyberriskeistä. Kyberriskeistä selvitettiin niiden esiintymistiheyksiä ja riskikuvauksien sisältöä. Tutkimustuloksissa nähdään nouseva trendi kyberriskikuvauksien esiintymistiheyksissä vuosina 2019–2023. Vuonna 2019 alle puolet yrityksistä mainitsee kyberriskit merkittävänä riskinä tai epävarmuustekijänä. Vuonna 2023 kyberriskejä mainitsee 71,7 % yrityksistä. Kasvua voidaan pitää merkittävänä. Vuonna 2022 lisäys edelliseen vuoteen oli 12,4 % kun aiempina vuosina muutos oli välillä 2,3 %–5,7 %. Venäjän hyökkäysota Ukrainassa ja sen seurauksena lisääntyneet kyberuhkat ja niistä uuti-

sointi lienevät nostaneet myös kyberriskit laajemmin keskusteluun yritysten hallituksissa. Kyberriskejä raportoineiden yhtiöiden tarkastelua toimialoittain rajoittaa Helsingin pörssin päälistalla olevien yhtiöiden pieni määrä. Pienimmillä toimialoilla on vain muutamia yrityksiä, jolloin yksittäisellä yhtiöllä on suuri painoarvo koko toimialaan. Yksittäisistä toimialoista matalia kyberriskimainintojen esiintymistiheyksiä on terveydenhuollon toimijoissa ja kiinteistöyhtiöissä. Terveydenhuollon toimialaan kuuluu terveyspalveluiden tuottajia, terveysteknologiayhtiöitä ja lääkeyhtiöitä. Toimialalla käsitellään paljon henkilötietoja sekä tehdään tutkimusta ja tuotekehitystä. Tästä näkökulmasta ajateltuna kyberriskien matala esiintymistiheys on yllättävää. Kiinteistöyhtiöt ovat kiinteistöjen omistamiseen ja hallinnointiin keskittyviä yhtiöitä. Toimiala on pääomaintensiivinen ja tyypillisesti yhtiöissä on työvoimaa suhteellisesti vähemmän verrattuna saman kokoluokan yrityksiin muilla toimialoilla. Tämän takia digitalisaatio ja kyberturvallisuuteen liittyvät teemat eivät ole kiinteisyhtiöiden hallitusten riskiarvioissa korkealla. Rahoitustoimialalla kyberriskien esiintymistiheys raportoiduissa riskeissä ja epävarmuustekijöissä oli vuonna 2019 keskimääräistä pienempi, mutta vuoteen 2023 mennessä se on noussut samalla tasolla korkeimpia esiintymistiheyksiä edustavien toimialojen kanssa. Rahoitussektoriin liittyvistä kyberuhkista ja kriisinkestävyydestä on keskustelu julkisuudessa paljon ja valvontaviranomaiset ovat kehottaneet finanssialan toimijoita parantamaan suojautumistaan kyberuhkia vastaan (Finanssivalvonta, 2022). Rahoitustoimialalla on myös todennäköisesti jo valmistauduttu vuonna 2023 voimaan tulleeseen Euroopan parlamentin ja neuvoston antamaan asetukseen finanssialan digitaalisesta häiriönsietokyvystä (Digital Operational Resiliency Act, DORA), jonka soveltaminen alkaa tammikuussa 2025 (Finanssivalvonta, 2023).

Yritysten koon mukaan tarkasteltuna tutkimustulokset osoittavat, että suurien yritysten riskiarvioissa kyberriskit tunnistetaan hyvin. Vuonna 2023 lähes kaikki suuyritykset (96,7 %) raportoivat kyberriskeistä merkittävinä riskeinä ja epävarmuustekijöinä. Keskisuurten yritysten kokoluokassa esiintymistiheys (70,8 %) on vuonna 2023 selkeästi matalampi suuryrityksiin verrattuna ja pienten yhtiöiden kokoluokassa vielä matalampi (57,1 %). Tutkimuksen tavoitteisiin ei kuulunut tunnistaa yritysten kyberriskien raportointia selittäviä tekijöitä, mutta näiden tutkimustulosten perusteella yrityksen kokoluokka näyttää vaikuttavan merkittävästi siihen kuinka merkittävänä riskinä kyberriskejä pidetään.

Hallitusten toimintakertomuksissa raportoitujen kyberriskien sisällön analyysin tuloksista on tehtävissä useita johtopäätöksiä. Kyberriskien kuvauksen laajuus ja keskimääräinen pituus kasvavat tarkasteluajanjaksolla. Yritysten välillä on paljon hajontaa siinä, kuinka laajasti kyberriskejä kuvataan. Osa yrityksistä tyytyy muutaman sanan yleisluontoiseen kuvaukseen, kun taas osa yrityksistä raportoi kyberriskeistä yksityiskohtaisemmin yrityskohtaiseen kontekstiin sitoen. Tarkasteluajanjakson alussa vuonna 2019 enemmistö kyberriskikuvauksista oli geneerisiä ja sellaisenaan mille tahansa nykyaikaisessa digitaalisessa toimintaympäristössä toimivalla yritykselle sopivia kuvauksia. Näiden niin sa-

nottujen boilerplate-kuvausten osuus aineistossa vähenee vuoteen 2023 mennessä ja kuvauksista tulee enemmän yrityskohtaisia riskejä kuvaavia. Kuitenkin vuonna 2023 yli kolmannes kuvauksista jää vielä yleiselle tasolle. Vuonna 2023 yrityskohtaisia riskejä/yrityskohtaisia riskejä sekä niiden hallintakeinoja kuvailevien kyberriskikuvausten osuus on jo noin 60 %. Toimintakertomuksissa esiintyville kyberriskikuvauksille on myös tunnusomaista, että kuvauksia kierrätetään sellaisenaan seuraavien vuosien raporteissa. Tämä koskee erityisesti lyhyitä ja yleiselle tasolle jääviä kuvauksia. Näiden kuvausten lisäarvo raportteja lukevalla yleisölle jää pieneksi.

Kyberriskikuvauksissa mainituista kyberuhkissa on samansuuntainen kehitys kuin kuvausten laajuudessa. Tarkasteluajanjakson kuluessa kyberuhkat tarkentuvat yleisellä tasolla kuvatuista uhkista tarkemmin nimettyihin uhkiin. Kyberhyökkäyksestä kehittyy yleiskäsite kuvamaan yritykseen kohdistuvaa digitaalisesta toimintaympäristöstä nousevaa uhkaa. Vaikka kyberhyökkäystä käytetään paljon yleiskielessä, on se käsitteenä epätarkka ja abstrakti. Käsite ymmärretään eri tavoin ja sillä voidaan kuvata hyvin erilaisia kybertoimintaympäristön ilmiöitä. Julkisessa keskustelussa ja uutisoinnissa esiintyviä palvelunestohyökkäyksiä, kiristyshaittaohjelmia ja tietojenkalastelua mainitaan kyberriskikuvauksissa verrattain harvoin. Koko tarkasteluajanjakson ajan merkittävässä osassa kyberriskikuvauksista kyberuhkia ei yksilöidä tarkemmin.

Kyberriskikuvauksissa hallitsevia teemoja ovat digitalisaation lisääntyminen ja yritysten riippuvuus tietojärjestelmistä ja niiden toimittajista. Lisäksi merkittävät yhteiskunnalliset tapahtumat heijastuvat yritysten hallitusten riskiarviointeihin. COVID-19 pandemian vaikutuksia on riskiarvoissa käsitelty laajasti, mutta sen vaikutuksista kyberturvallisuuteen on kuvattu vain vähän. Geopoliittisten jännitteiden lisääntyminen Euroopassa sen sijaan näkyy kyberriskikuvauksista. Venäjän hyökkäyssota ja sen vaikutukset kyberturvallisuuteen heijastuvat yritysten kyberriskikuvauksiin. Kyberhäiriötilanteiden nähdään muodostavan aiempaa suuremman uhkan yrityksen toiminnan jatkuvuudelle ja aiheuttavan mahdollisesti vahinkoa yrityksen taloudelle ja maineelle.

Vaikka kyberriskejä tunnistetaan yhä paremmin, on aineistosta tehtävien johtopäätösten perusteella kyberriskinäkemyksissä vielä puutteita. Suomessa on paljon korkean teknologian ja tutkimusta tekeviä yrityksiä. Hallitusten toimintakertomuksissa kuvatuissa kyberriskeissä ei tunnisteta riittävästi valtiollisten toimijoiden luomaa uhkaa. Viranomaisten mukaan valtiollisten toimijoiden suorittama laiton tiedonhankinta, vakoilu, on siirtynyt yhä enemmän tietoverkkoihin (Suojelupoliisi, 2020, 2021a, 2022). Suojellakseen yrityssalaisuuksia ja tutkimustoiminnalla aikaan saatuja tuloksia, tulisi yritysten myös tunnistaa kybervakoiluun liittyvä uhka ja varautua siihen. Kriittisillä toimialoilla kyberturvallisuusuhkat tunnistetaan jo hyvin, mutta valtiollisten toimijoiden harjoittamaan yritysvakoiluun on myös syytä varautua.

Tutkimusaineistossa yksikään yritys ei kuvannut kyberriskiä strategisena riskinä, vaan kyberturvallisuuteen liittyvät uhkat ja epävarmuustekijät luokiteltiin useimmiten operatiivisiksi riskeiksi. Tämä havainto vahvistaa Hepferin &

Powellin (2020) esittämään väitettä siitä, että yritysten hallituksissa ei täysin ymmärretä kyberriskin strategista luonnetta.

Pystyykö signalointi- tai legitimiteettiteoria selittämään, miksi kyberriskeistä kerrotaan yhä useammin pörssiyhtiön hallituksen toimintakertomuksissa? Tutkimustulosten perusteella tätä ei voida induktiivisesti päätellä, mutta epäsuorasti pääteltynä näin voidaan ajatella. Kun yritys nostaa merkittävimpien riskien ja epävarmuustekijöiden joukkoon kyberriskin, jokin viesti siihen sisältyy. Yleinen tietoisuus kyberuhkista on lisääntynyt viime vuosina ja se ei voi olla heijastumatta myös yritysten uhka-arvioihin. Yritysten toimintaympäristö muuttuu koko ajan ja yritysjohdon tehtävä on viestiä, signaloida, kyvystään vastata muutokseen. Hallituksen toimintakertomukseen sisältyvä kyberriskikuvaukseen voidaan ajatella olevan hallituksen signaali niin sijoittajille, viranomaisille kuin laajemmalle yleisölle siitä, että kyberturvallisuuteen liittyviin uhkiin on reagoitu. Hallitus joutuu kuitenkin tasapainoilemaan viestintänsä kanssa. Liian yksityiskohtainen kyberturvallisuusjärjestelyiden avaaminen voi altistaa yhtiön kyberriskeille ja sen vuoksi julkaistavaa informaatiota joudutaan rajoittamaan. Toisaalta signaloinnin tehokkuus edellyttää viestinnältä riittävää yrityskohtaisuutta. Yleisellä tasolla kuvattujen riskien viestiminen ei ole kuitenkaan tehokas signalointistrategia.

Tutkimusaineiston ja -tulosten kontekstissa kyberturvallisuus näyttäytyy enemmän legitimiteettiä rakentavana tekijänä kuin absoluuttisena turvallisuuskysymyksenä. Kyberriskikuvausten konteksti on lakisääteinen raportointi, joka ei kuitenkaan eksplisiittisesti vaadi yrityksiä kuvaamaan liiketoimintaan liittyviä kyberturvallisuuden näkökulmia. Legitimiteettiteorian mukaan yritys muuttaa ja sopeuttaa toimintaansa saadakseen sosiaalista hyväksyntään ympäröivältä yhteisöltä. Suomalaisessa kokonaisturvallisuuden mallissa yritykset ovat yksi toimijoista ja kansallisen kyberturvallisuuden toteuttamisessa yrityksillä on suuri vastuu. Tämän vuoksi yrityksillä on paine viestiä, että niiden tietoturvaan ja kyberturvallisuuteen liittyvät järjestelyt on toteutettu asianmukaisesti. Institutionaalisen legitimiteetin tavoittelun seurauksena yritysten kyberturvallisuusriskien raportointi yhdenmukaistuu. Sen taustalla voi olla aito käsitys kyberuhkakuvan muutoksesta, mutta taustamekanismeina voi olla myös muiden organisaatioiden jäljittely tai ammattiyhteisöjen luoma normatiivinen paine. Tämän tutkimuksen sivulöydöksenä oli myös havainto, että tietoturva ja kyberturvallisuus liitetään suomalaisten yritysten vastuullisuusraportointiin. Yrityksen yhteiskuntavastuuta selitetään usein legitimiteetin rakentamisen kautta, joten siltä osin kyberturvallisuus on myös legitimiteettiä lisäävä ulottuvuus.

6 POHDINTA

Tutkimuksen aineisto tarjosi sekä mahdollisuuksia että siihen liittyy rajoitteita. Julkisesti saatavilla oleva aineisto mahdollisti tutkimuksen toteutuksen pitkittäistutkimuksena koko perusjoukolle eli suomalaisille pörssiyhtiöille. Vaikka aineistoa oli määrällisesti verrattain paljon, ei niissä kuitenkaan käsitellä kyberturvallisuutta erityisen laajasti ja syvällisesti. Tämä rajoittaa tulkintojen tekemistä aineistosta. Toisaalta pitkittäistutkimusasetelma mahdollisti trendien ja kehityksen tunnistamisen tutkittavasta ilmiöstä. Tutkimustuloksista muodostuu selkeä kuva siitä, miten ja missä laajuudessa suomalaisten pörssiyhtiöiden hallitukset kokevat kyberriskit merkittävinä riskeinä ja epävarmuustekijöinä. Aineiston avulla ei kuitenkaan ole mahdollista aukottomasti selittää lisääntyneen kyberriskiraportoinnin syitä – onko taustalla kybertoimintaympäristössä tapahtuneet muutokset vai esimerkiksi organisaatioiden yhteiskunnalliseen legitimiteettiin liittyvät tavoitteet? Todennäköisesti vastaus on sekä että.

Kyberriskit ovat vain yksi osa yritysten riskienhallinnan kokonaisuutta ja on siten ymmärrettävää, että kyberriskien laajamittainen kuvaaminen ei ole mahdollista tai tarkoituksenmukaistakaan hallituksen toimintakertomuksissa. Nykyisessä muodossa toteutuva listattujen yhtiöiden kyberriskien raportoinnilla on vähäinen lisäarvo. Verkottuneessa tietoyhteiskunnassa monet julkiset palvelut nojaavat yksityisten toimijoiden tarjoamiin ja ylläpitämiin tietoteknisiin ratkaisuihin. Kyberriskeistä ja niihin varautumisen viestimisellä on merkitystä myös muille kuin yrityksen omistajille ja ulkoisille rahoittajille. Sääntelyn lisääminen on yksi tapa lisätä yritysten huomiota kyberturvallisuutta kohtaan ja sitä tuleva Euroopan unionin tuleva kyberturvallisuutta koskeva NIS2-direktiivi ja Suomeen kansallisesti säädettävä kyberturvallisuuslaki edistävät – tosin vain yhteiskunnan kannalta kriittisillä toimialoilla. Sääntelyllä on mahdollista saavuttaa määrätty vähimmäistaso kyberturvallisuudessa, mutta lisääntynyt sääntely aiheuttaa itsessään kustannuksia. Olisi kansantaloudellisesti tehokkaampaa, jos kyberturvallisuuden merkitys osana koko yhteiskunnan turvallisuutta ymmärrettäisiin ja siihen kiinnitettäisiin huomiota omaehtoisesti ilman sääntelyä. Ylimmän johdon rooli on tässä tärkeä kyberturvallisuuskulttuurin edistäjänä.

Miten tämän tutkimuksen tulokset suhteutuvat muissa maissa toteutettujen tutkimusten tuloksiin? Tutkimusasetelmaltaan lähin verrokki on Eijkelenboomin & Nieuwesteegin (2021) tutkimus, joka selvitti kyberturvallisuusinformaation esiintymistiheyksiä hollantilaisten listattujen yhtiöiden vuoden 2018 vuosiraporteissa. Heidän tutkimuksessaan 87 % tutkituista yhtiöistä mainitsi kyberturvallisuuden vuosiraporteissaan. Vastaava luku suomalaisille listayhtiöille vuonna 2019 oli tämän tutkimuksen aineiston perusteella 62 % ja esiintymistiheys kasvaa 72 % vuoteen 2023 mennessä. Ero hollantilaisiin yhtiöihin on merkittävä. Ero voi olla todellinen tai sitä voi selittää tutkimuksen erilaiset otannat. Eijkelenboomin & Nieuwesteegin tutkimuksessa otos oli 75 yhtiötä suurten, keskisuurten ja pienten yhtiöiden kokoluokista – 25 yhtiötä kustakin kokoluokasta -, joiden osakkeilla käydään kauppaa eniten Amsterdamin pörssissä. Tämän tutkimuksen tulokset ovat samansuuntaisia kuin mitä Héroux & Fortin (2020) totesivat omassa tutkimuksessaan seuraavien tietojen osalta: suomalaisten yritysten julkaisemissa kyberturvallisuutta koskevissa tiedoissa on paljon vaihtelua ja julkaistu informaatio on luonteeltaan yleistä ja vähäisessä määrin yrityskohtaista. Lisäksi vastaavasti suomalaisten yhtiöiden havaittiin kierrättävän uudelleen myöhemmissä raporteissaan kertaalleen julkaistua informaatiota. Héroux & Fortin esittivät tarpeen kyberturvallisuusinformaation tutkimukselle pitkittäistutkimusasetelmassa, johon tämä tutkimus suomalaisessa kontekstissa vastasi. Suomalaisten yhtiöiden julkaiseman kyberriskejä ja -uhkia kuvaavan informaation havaittiin muuttuvan vuosien 2019–2023 aikana yksityis- ja yrityskohtaisemmaksi, mutta kyberriskejä yleisellä tasolla kuvaavien osuus pysyy edelleen korkealla. Kyberriskien toteutumisen seuraukset ja vaikutukset suomalaisille pörssiyhtiöille ovat tämän tutkimuksen perusteella osittain samat, jotka Héroux & Fortin (2022) totesivat omassa tutkimuksessaan kanadalaisille listayhtiöille. Molemmissa tutkimuksissa yleisimpien vaikutusten joukkoon kuuluvat toiminnan keskeytyminen tai häiriö, mainehaitta, luottamuksellisen tiedon vaarantuminen ja tiedon häviäminen. Viiden useimmiten mainitun haitan joukkoon kanadalaisessa kontekstissa sen sijaan kuuluu oikeudelliset seuraamukset ja sakot, kun taas suomalaisessa kontekstissa viiden useimmiten mainitun haitan joukkoon sisältyy taloudelliset haitat. Oikeudellisia seuraamuksia mainitaan suomalaisten pörssiyhtiöiden kyberriskien kuvauksissa vain harvoin.

Yritysten hallitusten näkemykset kyberturvallisuudesta tarjoavat paljon lisätutkimusmahdollisuuksia. Yritysten merkitys yhteiskunnallisesti kyberturvallisuuden tuottajina on keskeinen ja ylimmällä johdolla on merkittävä rooli sen toteutuksessa. Kansallisen kyberturvallisuuden kehittämisen ja varautumisen näkökulmasta lisätutkimusta tarvitaan tästä kohderyhmästä. Suomessa puuttuu tutkimusta esimerkiksi hallitusten kokoonpanon vaikutuksesta kyberturvallisuuden johtamiseen yrityksistä, vaikka vastaavia tutkimuksia on tehty ulkomailla. Hallitusten roolia selittäville laadullisille tutkimuksille on myös Suomessa tarve. Edellä mainitut EU-tason ja kansalliset sääntelyuudistukset asettavat yritysten hallitukset erityiseen ja uuteen vastuuseen kyberturvallisuuden toteuttamisesta kriittisillä toimialoilla. Niin yritysten hallitusten työtä tukemaan

kuin kansallista kyberturvallisuutta vahvistamaan tarvitaan lisää tutkimusta yritysten hallitusten roolista kyberturvallisuuden johtamisessa. Tässä tutkimuksessa käytettiin signalointi- ja legitimiteettiteoriaa analyysia ohjaavassa roolissa. Näitä teorioita on sovellettu kyberturvallisuuden tutkimuksessa vähän, mutta niiden avulla on mahdollista selittää ilmiöitä kyberturvallisuuden kontekstissa. Taloustieteen ja liikkeenjohdon tutkimuksessa on myös muita vakiintuneita tieteellisiä teorioita, joiden soveltamista kyberturvallisuuden tutkimuksen kontekstiin tutkijoita tulisi kannustaa. Lisätutkimusmahdollisuuksia on myös tutkimusmenetelmien osalta. Listattujen yhtiöiden julkaisema informaatio tarjoaa avoimen ja laajan aineiston kyberturvallisuuden tutkimukseen eri maissa ja maantieteellisillä alueilla. Tutkimusmenetelmäkehitystä tarvittaisiin, jotta eri maissa ja alueilla toteutettujen tutkimusten yhteismitallisuutta ja vertailtavuutta saataisiin paremmaksi.

LÄHTEET

Aktia Pankki Oyj. (2023). *Taloudellinen katsaus 2022*. https://attachment.news.eu.nasdaq.com/a0a6084afddca82444f6c8beaeb45bab6

Alasoini, T. (2016). *Workplace Development Programmes as Institutional Entrepreneurs - Why They Produce Change and Why They Do Not*. Aalto University. https://aaltodoc.aalto.fi/handle/123456789/19578

Anora Group Oyj. (2024). *Vuosikertomus 2023*. https://attachment.news.eu.nasdaq.com/af410895d58ca6f16989aa5426c8f9a38

Azmi, R. & Kautsarina, K. (4.7.2019). *Revisiting Cyber Definition*. 18th European Conference on Cyber Warfare and Security, Coimbra, Portugal.

Bank of England. (29.3.2023). *Systemic Risk Survey Results - 2023 H2*. https://www.bankofengland.co.uk/systemic-risk-survey/2023/2023-h2

Berkman, H., Jona, J., Lee, G. & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy*, *37*(6), 508–526. https://doi.org/10.1016/j.jaccpubpol.2018.10.003

Böhme, R., Laube, S. & Riek, M. (2019). A fundamental approach to cyber risk analysis. *Variance*, *12*(2), 161–185.

Campbell, D. (2003). Intra- and intersectoral effects in environmental disclosures: evidence for legitimacy theory? *Business Strategy and the Environment*, *12*(6), 357–371. https://doi.org/10.1002/bse.375

Connelly, B. L., Certo, S. T., Ireland, R. D. & Reutzel, C. R. (2011). Signaling Theory: A Review and Assessment. *Journal of Management*, *37*(1), 39–67. https://doi.org/10.1177/0149206310388419

Craigen, D., Diakun-Thibault, N. & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21.

DiMaggio, P. J. & Powell, W. W. (1983). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review*, *48*(2), 147–160. https://doi.org/10.2307/2095101

Eijkelenboom, E. V. A. & Nieuwesteeg, B. F. H. (2021). An analysis of cybersecurity in Dutch annual reports of listed companies. *Computer Law & Security Review*, *40*, 105513. https://doi.org/10.1016/j.clsr.2020.105513

ENISA. (2016). *Definition of Cybersecurity - Gaps and overlaps in standardisation* (V1.0). European Union Agency For Network And Information Security (ENISA). https://www.enisa.europa.eu/publications/definition-of-cybersecurity

Eskola, J. & Suoranta, J. (1998). *Johdatus laadulliseen tutkimukseen*. Vastapaino. https://www.ellibslibrary.com/jyu/978-951-768-504-7

Ettredge, M., Guo, F. & Li, Y. (2018). Trade secrets and cyber security breaches. *Journal of Accounting and Public Policy*, *37*(6), 564–585. https://doi.org/10.1016/j.jaccpubpol.2018.10.006

Financial Stability Board. (2023). *Cyber Lexicon: Updated in 2023*. https://www.fsb.org/wp-content/uploads/P130423-3.pdf

Finanssivalvonta. (20.11.2018). *IFRS-sääntely*. www.finanssivalvonta.fi. https://www.finanssivalvonta.fi/finanssisektorin-toimijalle/paaomamarkkinat/liikkeeseenlaskijat-ja-sijoittajat/ifrs/ifrs-saantely/

Finanssivalvonta. (24.11.2021). *Liikkeeseenlaskijan tiedonantovelvollisuus*. www.finanssivalvonta.fi. https://www.finanssivalvonta.fi/finanssisektorin-toimijalle/paaomamarkkinat/liikkeeseenlaskijat-ja-sijoittajat/tiedonantovelvollisuus/

Finanssivalvonta. (4.3.2022). *Finanssivalvonta kehottaa tehostettuun kyberturvallisuuden seurantaan*. www.finanssivalvonta.fi. https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/valvottavatiedotteet/2022/finanssivalvonta-kehottaa-tehostettuun-kyberturvallisuuden-seurantaan/

Finanssivalvonta. (3.11.2023). *Asetus finanssialan digitaalisesta häiriönsietokyvystä*. www.finanssivalvonta.fi. https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/valvottavatiedotteet/2023/asetus-finanssialan-digitaalisesta-hairionsietokyvysta/

Fiskars Oyj Abp. (2024). *Tilinpäätös 2023*. https://attachment.news.eu.nasdaq.com/a5527dc1f24fcbab6f8b6290aa36519ff

Flick, Uwe. (2018). *Designing Qualitative Research*. SAGE Publications, Limited. http://ebookcentral.proquest.com/lib/jyvaskyla-ebooks/detail.action?docID=6995201

Gale, M., Bongiovanni, I. & Slapnicar, S. (2022). Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead. *Computers & Security*, *121*, 102840. https://doi.org/10.1016/j.cose.2022.102840

Galinec, D. & Steingartner, W. (2017). Combining cybersecurity and cyber defense to achieve cyber resilience. *2017 IEEE 14th International Scientific Conference on Informatics*, 87–93. https://doi.org/10.1109/INFORMATICS.2017.8327227

Gao, L., Calderon, T. G. & Tang, F. (2020). Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems*, *38*, 100468. https://doi.org/10.1016/j.accinf.2020.100468

Gordon, L. A., Loeb, M. P. & Sohail, T. (2010). Market Value of Voluntary Disclosures Concerning Information Security. *MIS Quarterly*, *34*(3), 567–594. https://doi.org/10.2307/25750692

Harvia Oyj. (2024). *Tilinpäätös ja toimintakertomus 2023*. https://attachment.news.eu.nasdaq.com/a9cd5306acd8377d15bce6a887dd88c76

HE 57/2024. *Hallituksen esitys eduskunnalle kyberturvallisuusdirektiivin (NIS 2 -direktiivi) täytäntöönpanoa koskevaksi lainsäädännöksi HE 57/2024*. Noudettu 3. kesäkuuta 2024, osoitteesta https://www.finlex.fi/fi/esitykset/he/2024/20240057

Helsingin Sanomat. (15.2.2023). *Kyberhyökkäys leikkasi Uponorin liikevaihtoa kymmenillä miljoonilla*. Helsingin Sanomat. https://www.hs.fi/talous/art-2000009395531.html

Helsingin Sanomat. (15.2.2024). *Tietoevry arvioi verkkohyökkäyksen aiheuttavan miljoonien eurojen menetykset*. Helsingin Sanomat. https://www.hs.fi/talous/art-2000010229232.html

Hepfer, M. & Powell, T. C. (2020). Make Cybersecurity a Strategic Asset. *MIT Sloan Management Review*, *62*(1), 40–45.

Héroux, S. & Fortin, A. (2020). Cybersecurity Disclosure by the Companies on the S&P/TSX 60 Index. *Accounting Perspectives*, *19*(2), 73–100. https://doi.org/10.1111/1911-3838.12220

Héroux, S. & Fortin, A. (2022). Board of directors' attributes and aspects of cybersecurity disclosure. *Journal of Management and Governance*, *28*(2), 359–404. https://doi.org/10.1007/s10997-022-09660-7

HKScan Oyj. (2022). *HKScan Toimintakertomus ja tilinpäätös 2021*. https://attachment.news.eu.nasdaq.com/afdb2ae53c2d7c07a3543805522877697

HKScan Oyj. (2024). *Toimintakertomus ja tilinpäätös 2023*. https://attachment.news.eu.nasdaq.com/a0c33e9e8eafc29ef846f0e19a64cc1c5

Hummel, K. & Schlick, C. (2016). The relationship between sustainability performance and sustainability disclosure – Reconciling voluntary disclosure theory and legitimacy theory. *Journal of Accounting and Public Policy*, *35*(5), 455–476. https://doi.org/10.1016/j.jaccpubpol.2016.06.001

Incap Oyj. (2024). *Vuosi- ja vastuullisuusraportti 2023*. https://attachment.news.eu.nasdaq.com/afbc39a6dbf715a83961b5b0eb800253b

ISO. (ei pvm.). *ISO/IEC 27000:2018(en), Information technology — Security techniques — Information security management systems — Overview and vocabulary*. Noudettu 13. joulukuuta 2023, osoitteesta https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en

Jaumotte, F., Li, L., Medici, A., Oikonomou, M., Pizzinelli, C., Shibata, I., Soh, J. & Mendes Tavares, M. (2023). *Digitalization During the COVID-19 Crisis: Implications for Productivity and Labor Markets in Advanced Economies* (Staff Discussion Notes No. 2023/003). International Monetary Fund. https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2023/03/13/Digitalization-During-the-COVID-19-Crisis-Implications-for-Productivity-and-Labor-Markets-529852

Juhila, K. (2021). Koodaaminen. Teoksessa J. Vuori (toim.), *Laadullisen tutkimuksen verkkokäsikirja*. Yhteiskuntatieteellinen tietoarkisto. https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/analyysitavan-valinta-ja-yleiset-analyysitavat/koodaaminen/

Jylhä, E. & Viitala, R. (2013). *Liiketoimintaosaaminen. Menestyvän yritystoiminnan perusta*. Edita Publishing Oy. https://www.ellibslibrary.com/book/978-951-37-6412-8/liiketoimintaosaaminen-menestyvan-yritystoiminnan-perusta

Ketokivi, M. (2015). *Tilastollinen päättely ja tieteellinen argumentointi*. Gaudeamus Helsinki University Press.

Kielitoimiston sanakirja. (2022). https://www.kielitoimistonsanakirja.fi/#/riski?searchMode=all

Kirjanpitolaki 1336/1997. Noudettu 30. lokakuuta 2023, osoitteesta https://www.finlex.fi/fi/laki/ajantasa/1997/19971336

Kirjanpitolautakunta. (2006). *Yleisohje toimintakertomuksen laadinnasta*.

Kokonaisturvallisuuden sanasto. (2017). Sanastokeskus TSK.

KONE Oyj. (2024). *Vuosikatsaus 2023*. https://attachment.news.eu.nasdaq.com/ad3e0f02347a2f35b57f44c48f6b4e6e5

Korstjens, I. & Moser, A. (2018). Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *The European Journal of General Practice*, *24*(1), 120–124. https://doi.org/10.1080/13814788.2017.1375092

KPMG. (22.9.2020). *Digital acceleration - KPMG United States*. https://kpmg.com/us/en/home/insights/2020/09/digital-acceleration.html

Li, H., No, W. G. & Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, *30*, 40–55. https://doi.org/10.1016/j.accinf.2018.06.003

Liikenne- ja viestintävirasto Traficom. (2023). *Suositus kyberturvallisuuden edistämisestä raideliikenteessä*. https://www.traficom.fi/sites/default/files/media/file/Traficom_suositus_kyberturvallisuuden_edistamisesta_raideliikenteessa_2023.pdf

Lincoln, Y. S. & Guba, E. G. (1985). *Naturalistic inquiry*. Sage.

Magness, V. (2006). Strategic posture, financial performance and environmental disclosure: An empirical test of legitimacy theory. *Accounting, Auditing & Accountability Journal*, *19*(4), 540–563. https://doi.org/10.1108/09513570610679128

Marston, C. L. & Shrives, P. J. (1991). The use of disclosure indices in accounting research: A review article. *The British Accounting Review*, *23*(3), 195–210. https://doi.org/10.1016/0890-8389(91)90080-L

McKinsey & Company. (5.10.2020). *How COVID-19 has pushed companies over the technology tipping point – and transformed business forever*. https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever

McKinsey & Company. (20.3.2024). *Boards of directors: The final cybersecurity defense for industrials*. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/boards-of-directors-the-final-cybersecurity-defense-for-industrials

Metso Oyj. (2024). *Metso 2023 taloudellinen katsaus*. https://attachment.news.eu.nasdaq.com/a19575e7cef27ecc86871098572e9e71d

Mitra, S. & Ransbotham, S. (2015). Information Disclosure and the Diffusion of Information Security Attacks. *Information Systems Research*, *26*(3), 565–584. https://doi.org/10.1287/isre.2015.0587

Morris, R. D. (1987). Signalling, Agency Theory and Accounting Policy Choice. *Accounting and Business Research*, *18*(69), 47–56. https://doi.org/10.1080/00014788.1987.9729347

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A. & Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure IT or not? *Decision Support Systems*, *56*, 11–26. https://doi.org/10.1016/j.dss.2013.04.004

Mänttäri-van der Kuip, M., Tammelin, M. & Anttila, T. (2018). Organisaatioiden isomorfismi : julkiset organisaatiot ja yhdenmukaisuuden paine. *Yhteiskuntapolitiikka*, *83*(3). https://jyx.jyu.fi/handle/123456789/58823

Neil, L., Haney, J. & Buchanan, K. (4.7.2023). Analyzing Cybersecurity Definitions for Non-experts. *NIST*. IFIP International Symposium on Human Aspects of Information Security & Assurance (HAISA 2023), Kent, Iso-Britannia. https://www.nist.gov/publications/analyzing-cybersecurity-definitions-non-experts

Neuendorf. (2016). *The Content Analysis Guidebook (Second Edition)*. SAGE Publications, Inc. https://sfx.finna.fi/nelli09?url_ver=Z39.88-2004&ctx_ver=Z39.88-2004&ctx_enc=info:ofi/enc:UTF-8&rfr_id=info:sid/sfxit.com:opac_856&url_ctx_fmt=info:ofi/fmt:kev:mtx:c

tx&sfx.ignore_date_threshold=1&rft.object_id=4100000010163261&svc_val_fmt=info:ofi/fmt:kev:mtx:sch_svc&

Nieuwesteeg, B., Visscher, L. & de Waard, B. (2018). The Law and Economics of Cyber Insurance Contracts: A Case Study. *European Review of Private Law*, *26*(3), 371–420. https://doi.org/10.54648/ERPL2018027

Nordea Bank Abp. (2021). *Annual Report 2020*. https://attachment.news.eu.nasdaq.com/a6c0f30ab125d55130dcc6979b67c4c32

Oltsik, J. (2020). *Cybersecurity in the C-suite and Boardroom*. Enterprise Strategy Group. https://www.bitsight.com/resources/cybersecurity-in-the-c-suite-and-boardroom

Puusa, A., Juuti, P. & Aaltio, I. (2020). *Laadullisen tutkimuksen näkökulmat ja menetelmät*. Gaudeamus. https://www.ellibslibrary.com/jyu/9789523456167

QPR Software Oyj. (2022). *QPR Software vuosikertomus 2021*. https://attachment.news.eu.nasdaq.com/ad51a16c3b7a7c4fcf40afbfd7ed9027d

Raggad, B. G. (2010). *Information security management: concepts and practice*. CRC Press.

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 (Basel, Switzerland)*, *14*(3), 1390. https://doi.org/10.3390/su14031390

Robit Oyj. (2024). *Robit 2023 vuosikertomus*. https://attachment.news.eu.nasdaq.com/a4675612d6e7960465a8841b6c8f0e66d

Ross, Ron., Pillitteri, Victoria., Graubart, Richard., Bodeau, Deborah. & McQuaid, Rosalie. (2019). Developing cyber resilient systems: a systems security engineering approach. Teoksessa *Developing cyber resilient systems: a systems security engineering approach*. U.S. Dept. of Commerce, National Institute of Standards and Technology.

Siponen, M. & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, *46*(5), 267–270. https://doi.org/10.1016/j.im.2008.12.007

Spence, M. (1973). Job Market Signaling. *The Quarterly Journal of Economics*, *87*(3), 355–374. https://doi.org/10.2307/1882010

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

Suchman, M. C. (1995). Managing Legitimacy: Strategic and Institutional Approaches: Academy of Management Review. *Academy of Management Review*, *20*(3), 571–610. https://doi.org/10.5465/AMR.1995.9508080331

Suojelupoliisi. (2020). *Vuosikirja 2020*. https://supo.fi/documents/38197657/40760236/Supo+Vuosikirja+2020.pdf/70e75573-0726-f76c-846c-be661887c9db/Supo+Vuosikirja+2020.pdf

Suojelupoliisi. (2021a). *Vuosikirja 2021*. https://supo.fi/documents/38197657/40760236/Vuosikirja+2021.pdf/6f645216-6c88-83cd-4493-3ffad2028b62/Vuosikirja+2021.pdf

Suojelupoliisi. (28.10.2021b). *Kolumni: Onko organisaatiosi suojautunut toimitusketjuhyökkäykseltä? Näillä vinkeillä pääset alkuun*. https://supo.fi/-/kolumni-onko-organisaatiosi-suojautunut-toimitusketjuhyokkaykselta-nailla-vinkeilla-paaset-alkuun

Suojelupoliisi. (2022). *Vuosikirja 2022*. https://vuosikirja.supo.fi/documents/62399122/66519032/SUPO+Vuosikirja+2022.pdf/2650348b-77fb-ddf8-e80c-cc46a21d7074/SUPO+Vuosikirja+2022.pdf

Taherdoost, H. (2022). Cybersecurity vs. Information Security. *Procedia Computer Science*, *215*, 483–487. https://doi.org/10.1016/j.procs.2022.12.050

The Institute of Risk Management. (2014). *Cyber Risk Resources for Practitioners*. https://www.theirm.org/media/7237/irm-cyber-risk-resources-for-practitioners.pdf

Tieteen termipankki. (13.5.2016). *Oikeustiede:legitimiteettiteoria – Tieteen termipankki*. https://tieteentermipankki.fi/wiki/Oikeustiede:legitimiteettiteoria

Tieteen termipankki. (27.2.2020). *Oikeustiede:boilerplate-ehdot – Tieteen termipankki*. https://tieteentermipankki.fi/wiki/Oikeustiede:boilerplate-ehdot

Tietoevry Oyj. (2024). *Taloudellinen katsaus 2023*. https://attachment.news.eu.nasdaq.com/a705603d65ec24add2b62f3dc330f855d

Tulikivi Oyj. (2024). *Vuosikertomus 2023*. https://attachment.news.eu.nasdaq.com/ab81ffb77b0923eab74062a424213b563

Tuomi, J. & Sarajärvi, A. (2018). *Laadullinen tutkimus ja sisällönanalyysi* (Uudistettu laitos). Kustannusosakeyhtiö Tammi. https://www.ellibslibrary.com/jyu/9789520400118

UPM-Kymmene Oyj. (2021). *Vuosikertomus 2020*. https://attachment.news.eu.nasdaq.com/ab64e90b30cae2840168e328ab4a51ea8

Vernon Gayle & Paul Lambert. (2020). *Quantitative Longitudinal Data Analysis : Research Methods*. Bloomsbury Academic; eBook Collection (EBSCOhost). https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=2660389&site=ehost-live

von Solms, B. & von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information and Computer Security*, *26*(1), 2–9. https://doi.org/10.1108/ICS-04-2017-0025

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

Wade, M. & Shan, J. (2020). Covid-19 Has Accelerated Digital Transformation, but May Have Made it Harder Not Easier. *MIS Quarterly Executive*, 213–220. https://doi.org/10.17705/2msqe.00034

Wang, T., Kannan, K. N. & Ulmer, J. R. (2013). The Association Between the Disclosure and the Realization of Information Security Risk Factors. *Information Systems Research*, *24*(2), 201–218. https://doi.org/10.1287/isre.1120.0437

Weber, R. (2011). *Basic Content Analysis*. https://doi.org/10.4135/9781412983488

World Economic Forum. (2023). *Global Cybersecurity Outlook 2023*. https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf

World Economic Forum. (2024). *Global Cybersecurity Outlook 2024*. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf

Yhteiskunnan turvallisuusstrategia. (2017). [Valtioneuvoston periaatepäätös / 2.11.2017].

LIITE 1 TUTKIMUKSEN AINEISTONA KÄYTETYT YHTIÖT

X = kyseisen vuoden raportti on mukana aineistossa, E = yhtiön on päälistalla, mutta ei julkaise Suomen kirjanpitolain mukaista toimintakertomusta, NA = yhtiö on päälistalla, mutta toimintakertomusta ei saatavilla (tilanne 19.4.2024)

Kokoluokka: S=suuret yhtiöt, K=keskisuuret yhtiöt, P=pienet yhtiöt

Yhtiö	2019	2020	2021	2022	2023	ICB koodi	Sektori	Koko-luokka	Huomiot
Afarak Group	X	X	X	X	X	5510	Perusteollisuus	P	
Ahlstrom-Munksjö	X	X				5520	Perusteollisuus	S	Osakkeen listaus loppunut 19.5.2021
Alisa Pankki				X	X	3010	Rahoitus	P	Päälistalle vuonna 2022
Aktia Pankki	X	X	X	X	X	3010	Rahoitus	K	
Alma Media	X	X	X	X	X	4030	Kulutuspalvelut	K	
Anora Group	X	X	X	X	X	4510	Kulutustuotteet	K	Altia vuoteen 2020 saakka
Apetit	X	X	X	X	X	4510	Kulutustuotteet	P	
Aspo	X	X	X	X	X	5020	Teollisuustuotteet ja -palvelut	K	
Aspocomp Group	X	X	X	X	X	1010	Teknologia	P	
Atria	X	X	X	X	X	4510	Kulutustuotteet	K	
Basware	X	X	X			1010	Teknologia	K	Osakkeen listaus loppunut 9.12.2022
Biohit	X	X	X	X	X	2010	Terveydenhuolto	K	
Bittium	X	X	X	X	X	1010	Teknologia	K	
Boreo	X	X	X	X	X	5020	Teollisuustuotteet ja -palvelut	P	Yleiselektroniikka 2019 saakka
CapMan	X	X	X	X	X	3020	Rahoitus	K	
Cargotec	X	X	X	X	X	5020	Teollisuustuotteet ja -	S	

							palvelut		
Caverion	X	X	X	X	X	5020	Teollisuustuotteet ja -palvelut	K	
Citycon	X	X	X	X	X	3510	Kiinteistöyhtiöt	S	
Componenta	X	X	X	X	X	5510	Perusteollisuus	P	
Consti	X	X	X	X	X	5020	Teollisuustuotteet ja -palvelut	P	
Cramo	X					5020	Teollisuustuotteet ja -palvelut	K	Osakkeen listaus loppunut 3.6.2020
Digia	X	X	X	X	X	1010	Teknologia	K	
Digitalist Group	X	X	X	X	X	1010	Teknologia	P	
DNA	X					1510	Tietoliikennepalvelut	S	Osakkeen listaus loppunut 3.2.2020
Dovre Group	X	X	X	X	X	5020	Teollisuustuotteet ja -palvelut	P	
EAB Group	X	X	X			3020	Rahoitus	P	Päälistalle 2019. Sulautunut Evli Oyj:öön 1.10.2022
Eezy		X	X	X	X	5020	Teollisuustuotteet ja -palvelut	P	Päälistalle 2020
Elecster	X	X	X	X	X	5020	Teollisuustuotteet ja -palvelut	P	
Elisa	X	X	X	X	X	1510	Tietoliikennepalvelut	S	
Endomines				X	X	5510	Perusteollisuus	P	Endomines AB (Ruotsi) 2018-2021. Endomines Oyj 2022
Enedo	X	X	X	X		5020	Teollisuustuotteet ja -palvelut	P	Efore nimellä 25.2.2020 saakka. Osakkeen listaus päättynyt 1.6.2023
Enento Group	X	X	X	X	X	3020	Rahoitus	K	Asiakastieto vuoteen 2019 saakka
Enersense International			X	X	X	5020	Teollisuustuotteet ja -palvelut	P	Päälistalle 2021
eQ	X	X	X	X	X	3020	Rahoitus	K	
Ericsson	E	E	E	E	E	1510	Tietoliikennepalvelut	S	Rinnakkaislistaus Helsingissä. Ei julkaise Suomen kirjanpitolain mukaisesti

Etteplan	X	X	X	X	X	5020	Teollisuustuotteet ja -palvelut	K	
Evli	X	X	X	X	X	3020	Rahoitus	K	
Exel Composites	X	X	X	X	X	5020	Teollisuustuotteet ja -palvelut	P	
Finnair	X	X	X	X	X	4050	Kulutuspalvelut	K	
Fiskars	X	X	X	X	X	4020	Kulutuspalvelut	S	
Fortum	X	X	X	X	X	6510	Yleishyödylliset palvelut	S	
F-Secure	X	X	X	X	X	1010	Teknologia	K	
Glaston	X	X	X	X	X	5010	Teollisuustuotteet ja -palvelut	P	
Gofore			X	X	X	1010	Teknologia	K	Päälistalla 2021 alkaen
Harvia	X	X	X	X	X	4020	Kulutuspalvelut	K	
HKScan	X	X	X	X	X	4510	Kulutustuotteet	P	
Hoivatilat	X					5010	Kiinteistöyhtiöt	K	Osakkeen listaus loppunut 15.5.2020
Honkarakenne	X	X	X	X	X	4020	Kulutuspalvelut	P	
Huhtamäki	X	X	X	X	X	5020	Teollisuustuotteet ja -palvelut	S	
Ilkka	X	X	X	X	X	4030	Kulutuspalvelut	P	
Incap	X	X	X	X	X	5020	Teollisuustuotteet ja -palvelut	K	
Innofactor	X	X	X	X	X	1010	Teknologia	P	
Investors House	X	X	X	X	X	3510	Kiinteistöyhtiöt	P	
Kamux	X	X	X	X	X	4040	Kulutuspalvelut	K	
Kemira	X	X	X	X	X	5520	Perusteollisuus	S	
Keskisuomalainen	X	X	X	X	X	4030	Kulutuspalvelut	P	
Kesko	X	X	X	X	X	4520	Kulutustuotteet	S	
Kesla	X	X	X	X	X	5020	Teollisuustuotteet ja -palvelut	P	

KH Group	X	X	X	X	X	5020	Rahoitus	P	Sievi Capital 2023 alkaen
Kojamo	X	X	X	X	X	3510	Kiinteistöyhtiöt	S	
Kone	X	X	X	X	X	5020	Teollisuustuotteet ja -palvelut	S	
Konecranes	X	X	X	X	X	5020	Teollisuustuotteet ja -palvelut	S	
Koskisen				X	X	5510	Perusteollisuus	P	Listautuminen vuonna 2022
Kreate Group			X	X	X	5010	Teollisuustuotteet ja -palvelut	P	
Lamor					X	6510	Yleishyödylliset palvelut	P	
Lassila & Tikanoja	X	X	X	X	X	6510	Yleishyödylliset palvelut	K	
Lehto Group	X	X	X	X	NA	5010	Teollisuustuotteet ja -palvelut	P	
Lifeline SPAC I			X	X	X	3020	Rahoitus	P	Osake listattu 18.10.2021 alkaen
Mandatum					X	3020	Rahoitus	S	Listautuminen 2.10.2023
Marimekko	X	X	X	X	X	4020	Kulutuspalvelut	K	
Martela	X	X	X	X	X	4020	Kulutuspalvelut	P	
Metso	X	X	X	X	X	5020	Teollisuustuotteet ja -palvelut	S	Metso Outotec (2020-2023)
Metsä Board	X	X	X	X	X	5510	Perusteollisuus	S	
Musti Group		X	X	X	X	4040	Kulutuspalvelut	K	Listautuminen 2020
Neles		X	X			5020	Teollisuustuotteet ja -palvelut	S	Listautuminen 2020. Osakkeen listaus lop-punut 31.3.2022
Neste	X	X	X	X	X	6010	Energia	S	
Nixu	X	X	X	X	X	1010	Teknologia	P	
NoHo Partners	X	X	X	X	X	4050	Kulutuspalvelut	K	
Nokia	X	X	X	X	X	1510	Tietoliikennepalvelut	S	
Nokian Renkaat	X	X	X	X	X	4010	Kulutuspalvelut	S	
Nordea Bank	X	X	X	X	X	3010	Rahoitus	S	Englanninkielin vuosiraportti

Nurminen Logistics	X	X	X	X	X	5020	Teollisuustuotteet ja -palvelut	P	
Olvi	X	X	X	X	X	4510	Kulutustuotteet	K	
Oma Säästöpankki	X	X	X	X	X	3010	Rahoitus	K	
Optomed	X	X	X	X	X	2010	Terveydenhuolto	P	Listautuminen 2019
Oriola	X	X	X	X	X	2010	Terveydenhuolto	K	
Orion	X	X	X	X	X	2010	Terveydenhuolto	S	
Orthex			X	X	X	4020	Kulutuspalvelut	P	Listautuminen 2021
Outokumpu	X	X	X	X	X	5510	Perusteollisuus	S	
Outotec	X					5020	Teollisuustuotteet ja -palvelut	S	
Ovaro Kiinteistösijoitus	X	X	X	X	X	3510	Kiinteistöyhtiöt	P	
Panostaja	X	X	X	X	X	3020	Rahoitus	P	
Pihlajalinna	X	X	X	X	X	2010	Terveydenhuolto	K	
Plc Uutechnic Group	X	X				5510	Teollisuustuotteet ja -palvelut	P	Osakkeen listaus loppunut 19.5.2021
Ponsse	X	X	X	X	X	5020	Teollisuustuotteet ja -palvelut	K	
PunaMusta Media	X	X	X	X	X	4030	Kulutuspalvelut	P	
Purmo Group				X	X	5010	Teollisuustuotteet ja -palvelut	K	Listautuminen 2022
Puuilo				X	X	4040	Kulutuspalvelut	K	Listautuminen 2021 ja kalenterivuodesta poikkeava tilikausi
QPR Software	X	X	X	X	X	1010	Teknologia	P	
Qt Group	X	X	X	X	X	1010	Teknologia	S	
Raisio	X	X	X	X	X	4510	Kulutustuotteet	K	
Rapala VMC	X	X	X	X	X	4020	Kulutuspalvelut	K	
Raute	X	X	X	X	X	5020	Teollisuustuotteet ja -palvelut	P	
Reka Industrial	X	X	X	X	X	5020	Teollisuustuotteet ja -	P	

							palvelut		
Relais Group				X	X	4010	Kulutuspalvelut	K	Nasdaq Helsinki listaus 2022
Remedy Entertainment				X	X	4020	Kulutuspalvelut	K	Nasdaq Helsinki listaus 2022 (2017-2021 First North listaus)
Revenio Group	X	X	X	X	X	2010	Terveydenhuolto	S	
Robit	X	X	X	X	X	5020	Teollisuustuotteet ja -palvelut	P	
Rovio Entertainment	X	X	X	X	NA	1010	Kulutuspalvelut	K	
Saga Furs	X	X	X	X	X	4020	Kulutuspalvelut	P	
Sampo	X	X	X	X	X	3030	Rahoitus	S	
Sanoma	X	X	X	X	X	4030	Kulutuspalvelut	S	
Scanfil	X	X	X	X	X	5020	Teollisuustuotteet ja -palvelut	K	
Soprano	X	X	X			1010	Teknologia	P	
Siili Solutions	X	X	X	X	X	1010	Teknologia	P	
Silmäasema	X					4040	Kulutuspalvelut	P	Osakkeen listaus loppunut 5.5.2020
Sitowise Group			X	X	X	5010	Teollisuustuotteet ja -palvelut	K	Listautuminen 2021
Solteq	X	X	X	X	X	1010	Teknologia	P	
Sotkamo Silver	E	E	E	E	E	5510	Perusteollisuus	P	
SRV Yhtiöt	X	X	X	X	X	5010	Teollisuustuotteet ja -palvelut	P	
SSAB	E	E	E	E	E	5510	Perusteollisuus	S	Ei julkaise Suomen kirjanpitolain mukaista toimintakertomusta
SSH Communications Security	X	X	X	X	X	1010	Teknologia	P	2022-2020 julkaisut englanniksi ja 2019-2018 suomeksi
Stockmann	X	X	X	X	X	4040	Kulutuspalvelut	K	
Stora Enso	X	X	X	X	X	5510	Perusteollisuus	S	
Suominen	X	X	X	X	X	4520	Kulutustuotteet	K	
Taaleri	X	X	X	X	X	3010	Rahoitus	K	

Talenom	X	X	X	X	X	5020	Teollisuustuotteet ja -palvelut	K	
Tallink Grupp	E	E	E	E	E	4050	Kulutuspalvelut	K	Ei julkaise Suomen kirjanpitolain mukaista toimintakertomusta
Tecnotree	X	X	X	X	X	1010	Teknologia	K	
Teleste	X	X	X	X	X	1510	Tietoliikennepalvelut	P	
Telia Company	E	E	E	E	E	1510	Tietoliikennepalvelut	S	Ei julkaise Suomen kirjanpitolain mukaista toimintakertomusta
Terveystalo	X	X	X	X	X	2010	Terveydenhuolto	K	
TietoEVRY	X	X	X	X	X	1010	Teknologia	S	
Tikkurila	X	X				5020	Teollisuustuotteet ja -palvelut	K	Osakkeen listaus loppunut 28.10.2021
Tokmanni Group	X	X	X	X	X	4040	Kulutuspalvelut	K	
Trainers´ House	X	X	X	X	X	1010	Teknologia	P	
Tulikivi	X	X	X	X	X	5010	Teollisuustuotteet ja -palvelut	P	
United Bankers		X	X	X	X	3020	Rahoitus	P	Päälistalle 18.6.2020
UPM-Kymmene	X	X	X	X	X	5510	Perusteollisuus	S	
Uponor	X	X	X	X	NA	5010	Teollisuustuotteet ja -palvelut	S	
Vaisala	X	X	X	X	X	5020	Teollisuustuotteet ja -palvelut	S	
Valmet	X	X	X	X	X	5020	Teollisuustuotteet ja -palvelut	S	
Valoe	X	X	X	X	NA	5020	Teollisuustuotteet ja -palvelut	P	
Verkkokauppa.com	X	X	X	X	X	4040	Kulutuspalvelut	P	
Viking Line	X	X	X	X	X	4050	Kulutuspalvelut	K	
Wetteri				X	NA	4040	Kulutuspalvelut	P	
WithSecure				X	X	1010	Teknologia	K	Spin-off F-Secure Oyj:stä

Wulff-Yhtiöt	X	X	X	X	X	5020	Teollisuustuotteet ja -palvelut	P	
Wärtsilä	X	X	X	X	X	5020	Teollisuustuotteet ja -palvelut	S	
YIT	X	X	X	X	X	5010	Teollisuustuotteet ja -palvelut	K	
Ålandsbanken	X	X	X	X	X	3010	Rahoitus	K	Englanninkielinen raportti