Jonna Rantala

NIS-direktiivin kahdet kasvot – riskit ja riskienhallinta

Tietotekniikan pro gradu -tutkielma

24.9.2017

Jyväskylän yliopisto

Informaatioteknologian laitos

Tekijä: Jonna Rantala
Yhteystiedot: jonna.e.rantala@student.jyu.fi
Ohjaajat: Martti Lehto
Työn nimi: NIS-direktiivin kahdet kasvot – riskit ja riskienhallinta
Title in English: Two sides of NIS directive – risks and risk management
Työ: Pro gradu -tutkielma
Suuntautumisvaihtoehto: Ohjelmistotekniikka
Sivumäärä: 68+20

Tiivistelmä

Euroopan unionin verkko- ja tietoturvadirektiivi, eli NIS-direktiivi, annettiin heinäkuussa 2016 ja sitä on sovellettava jäsenvaltioissa viimeistään 10. toukokuuta 2018. Direktiivin tavoitteena on parantaa jäsenmaiden tietoturvaa ja sitä kautta sisämarkkinoiden toiminta-edellytyksiä. Se koskettaa suoraan digitaalisia toimijoita ja erikseen määriteltyjä keskeisiä toimijoita, mutta sen vaikutusten voidaan olettaa ulottuvan myös näiden ryhmien ulkopuolelle muun muassa palveluntarjoajiin. Vaikka direktiivi annettiin samoihin aikoihin ja sen soveltaminen aloitetaan myös samoihin aikoihin Euroopan unionin tietosuoja-asetuksen (GDPR) kanssa, on se jäänyt huomattavasti pienemmälle huomiolle kuin tietosuoja-asetus.

Tässä tutkielmassa tarkastellaan EU:n uuden verkko- ja tietoturvadirektiivin vaikutuksia yritysten toiminnalle. Vaikutuksia tarkastellaan yritysten näkökulmasta ja huomioiden direktiivin tuomat kaksi puolta: riskit ja riskienhallinnan. Vaikka direktiivi pyrkii tuomaan yrityksille tehostettua riskienhallintaa, se tuo samalla myös riskejä yrityksen liiketoiminnalle. Juurikin riskeistä johtuen GDPR on saanut niin suuren huomion. Tutkimusongelmina selvitetään, ketä direktiivi tulee koskettamaan, millaisia riskejä direktiivi tuo mukanaan sitä koskettaville yrityksille ja toisaalta, mitä direktiivi tuo yritysten riskienhallinnalle. Tutkimuksen aineistona toimi säädetty direktiivi, ja tukevana materiaalina liikenne- ja viestintäministeriön asettaman työryhmän loppuraportti sekä Suomen tietoturvallisuus strategia, joka julkaistiin keväällä 2016.

Tutkimus on laadullinen sisällönanalyysi, jossa asiaa pohditaan muiden tutkimusten ja yllä mainitun aineiston pohjalta. Koska tämä on tietotekniikan, ei oikeustieteiden tutkimus, ei lakeihin tai niiden vaikutuksiin mennä syvällisesti, vaan asiaa tarkastellaan enemmän ylätasolla ja pyritään luomaan kokonaiskuvaa aiheeseen.

Tutkimuksen tulosten perusteella todettiin, että direktiivi tuo yrityksille niin uusia riskejä, kuin riskienhallintaa tukeviakin keinoja. Vaikka toimijoiden rajaus ennen lain julkaisua on hankalaa, jo nyt voitiin todeta, että joukko tulee olemaan laajempi, kuin vain suoraan direktiivin alaisiksi määritellyt toimijat. Epäonnistuessaan direktiivi tuo yrityksille useita strategisia ja operatiivisia riskejä, jotka haittaavat yritysten toimintaa, mutta onnistuessaan se voi merkittävästi parantaa verkko- ja tietoturvallisuutta EU:n jäsenmaissa.

Avainsanat: verkko- ja tietoturvadirektiivi, NIS-direktiivi, riskienhallinta

Abstract:

The EU Directive on security of network and information systems (the NIS Directive) was adopted in July 2016, and shall be transposed into national laws throughout the Member States by May 10th, 2018. The objectives of the Directive are to improve cyber security throughout the member states, which is said to further lead into better functioning digital single market. The Directive directly affects operators of essential services and digital service providers, but its impacts can be expected to extend beyond these groups for example to service providers. Although the Directive was adopted around the same time, and it will step into force around the same time with EU's General Data Protection Regulation (GDPR), it has received far less attention than GDPR.

This thesis examines the impact of the NIS Directive on companies. The impacts are examined from the businesses point of view considering the two sides of the Directive: risks and risk management. Even though the directive aims to bring companies more effective risk management practices, it also brings risks to the company's operations. Risks are in fact one of the reasons that have brought the GDPR into the center of the attention. Research questions aim to identify, which companies are affected by the directive, what risks the Directive brings, and what does the directive bring for the companies' risk

management. The research was done by analyzing the directive itself. The final report of the Ministry of Transport and Communications' working group and Finnish Information Security Strategy, published in spring 2016, were used as supportive material. The study is limited to Finland.

The study is a qualitative content analysis that reflects the matter based on other studies and above mentioned material. Because this is an information technology thesis, not legal studies, the study does not go deeply into laws or their legal implications, but the matter is rather analyzed on higher level and the aim is to create an overall picture of the subject.

Based on the research results, it was found that the Directive brings new risks to the companies as well as provides tools for their risk management. Prior publishing the local laws it is difficult to define all the affected parties, but already now it can be concluded that the effects will spread beyond the operators directly defined in the Directive. If the directive fails it will bring the companies many strategic and operational risks, but when succeeding it can significantly improve the network and information security in EU member states.

Keywords: NIS directive, NISD

Termiluettelo

CSTB	Computer Science and Telecommunications Board
Digitaalinen toimija	NIS-direktiivin tarkoittama digitaalisen palvelun tarjoaja
Direktiivi	NIS-direktiivi
ENISA	Euroopan unionin verkko- ja tietoturvavirasto (The European Union Agency for Network and Information Security)
EU	Euroopan unioni
GDPR	Euroopan unionin tietosuoja-asetus (General data protection regulation)
IEEE	Institute of Electrical and Electronics Engineers
ISF	Information Security Forum
ITIL	Information Technology Infrastructure Library
Jäsenvaltio	Euroopan unionin jäsenvaltio
Keskeinen toimija	NIS-direktiivin tarkoittama keskeisten palvelujen tarjoaja
Loppuraportti	Liikenne- ja viestintäministeriön asettaman NIS-direktiivin kansallista täytäntöönpanoa arvioivan työryhmän loppuraportti.
NCA	National Crime Agency (UK)
NIS-direktiivi	Euroopan unionin verkko- ja tietoturvadirektiivi (The Directive on security of network and information systems)
NIST	National Institute of Standards and Technology (USA)
Resitaali	Direktiivin johdanto-osan kappale (eng. recital)
Toimija	NIS-direktiivissä määritelty keskinen tai digitaalinen toimija

EU:n NIS-direktiivissä käyttämät termit löytyvät liitteestä D

Kuviot

Kuvio 1. Riskin ja mahdollisen palkkion suhde yrityksen elinkaaren eri vaiheissa 21

Taulut

Taulu 1. Direktiivin summittaiset määritelmät 36
Taulu 2. Maineriski 36
Taulu 2. Muut compliance-riskit 38
Taulu 3. Yleiset strategiset riskit 39
Taulu 4. Yrityksen toimintojen mukauttaminen 40
Taulu 6. Tietovuodot 40
Taulu 7. Pula osaajista 41
Taulu 8. Turvallisuusohjeiden luonti 41
Taulu 9. Päällekkäinen ilmoitusvelvollisuus 42

Sisältö

1 JOHDANTO 1
1.1 Tutkimuksen tausta 1
1.2 Tutkimuksen tavoitteet ja tutkimuskysymykset 2
1.3 Aikaisemmat tutkimukset 2
1.4 Tutkimusaineisto 4
1.5 Tutkimuksen rakenne 5

2 NIS-DIREKTIIVI 7
2.1 Taustatekijät 7
2.2 Tavoitteet 9
2.3 Velvoitteet, vaatimukset ja sanktiot 11
2.4 Direktiivi kansallisella tasolla 16

3 RISKIT JA NIIDEN HALLINTA 20
3.1 Riski käsitteenä 20
3.2 Tietoriski 22
3.3 Riskien sääntely lailla ja compliance-riski 24
3.4 Riskienhallinta 25

4 TUTKIMUKSEN LÄPIVIENTI 29
4.1 Tutkimuksen tavoitteet ja aineiston hankinta 29
4.2 Tutkimusmenetelmä 30
4.3 Tutkimuksen toteutustapa 31

5 TUTKIMUSTULOKSET 34
5.1 NIS-direktiivi riskinäkökulmasta 34
5.1.1 Compliance-riskit 34
5.1.2 Strategiset riskit 38
5.1.3 Operatiiviset riskit 40
5.1.4 Taloudelliset riskit ja vahinkoriskit 42
5.2 NIS-direktiivin vaikutukset riskienhallintaan 43
5.3 Direktiivin vaikutuksenalaiset toimijat 46

6 POHDINTAA JA YHTEENVETO 50
6.1 Tutkimustulosten yhteenveto 50
6.2 Tutkimuksen rajoitukset, arviointi ja luotettavuus 52
6.3 Tutkimuksen merkittävyys ja jatkotutkimusaiheet 54

LÄHTEET 56

LIITTEET 61
A NIS-direktiivin sisältö (Euroopan parlamentti ja euroopan unionin neuvosto 2016) 61
B NIS-direktiivin keskeisten toimijoiden tyypit (direktiivin liite II) 63
C Digitaalisen palvelun tarjoajat (direktiivin liite III) 66

D Selitykset (4 artikla) 67
E Direktiivin riskit kohdittain 69

1 Johdanto

Gradussa käsitellään NIS-direktiiviä eli Euroopan unionin verkko- ja tietoturvadirektiiviä, joka alkaa velvoittaa toukokuussa 2018. Vaikka direktiivin edellyttämiä kansallisia lakeja ei vielä juurikaan ole jäsenmaissa julkaistu, voidaan direktiivin vaikutuksia arvioida teoreettisella tasolla direktiivissä lueteltujen vaatimusten pohjalta. Tässä pro gradussa aihetta käsitellään Suomen osalta ja yritysten (myöhemmin toimija) näkökulmasta, eli pyritään löytämään ne riskit ja riskienhallintaa tukevat keinot, joita direktiivi tuo toimijoille. Tutkimuksessa keskitytään ainoastaan direktiivin niihin osiin, jossa suoraan määritellään verkko- ja tietoturvallisuusvaatimuksia toimijoille. Ulkopuolelle jäävät muut alueet mm. strategian ja valvovan viranomaisen hyväksynnät, sillä näiden osioiden yksityiskohtaisella sisällöllä ei ole oleellista merkitystä toimijoille.

1.1 Tutkimuksen tausta

Viime aikoina keskustelu on ollut aktiivista vuonna 2018 täytäntöön pantavan EU:n tietosuoja-asetuksen (GDPR) ympärillä, mutta verkko- ja tietoturva direktiivi (NIS-direktiivi) on jäänyt vähemmälle huomiolle. Tietosuojavaltuutetun toimisto on julkaissut oppaan "*Miten valmistautua EU:n tietosuoja-asetukseen*" (Talus ym. 2017). Toukokuussa 2017 tehty haku Gartnerin analyysipalvelusta GDPR:lle tuottaa 68 tulosta, samaan aikaan NIS-direktiiville (hakusana: NIS directive) niitä tulee seitsemän. Sama toistuu IEEE:n haussa, joka antaa GDPR:lle 12 tulosta kun NIS-direktiivillä niitä on vain yksi. Tavallinen Google-haku kuvaa tilannetta laajemmin, mutta lopputulos on sama: hakusanalla ’tietosuoja-asetus’ saadaan 102 000 tulosta kun 'verkko- ja tietoturvadirektiivi’ antaa 241 tulosta. Vaikka verkko- ja tietoturvadirektiivi (NIS-direktiivi), joka tietosuojan sijaan keskittyy yritysten tietoturvaan, hyväksyttiin vain muutamaa kuukautta tietosuoja-asetuksen jälkeen, on se jäänyt huomattavasti vähemmälle huomiolle.

Epätasaisesta huomioinnista huolimatta tietosuoja-asetus ja NIS-direktiivi alkavat velvoittaa samoihin aikoihin, toukokuussa 2018. Koska NIS-direktiivistä keskustelu on jäänyt huomattavasti vähemmälle saattaakin tulla joillekin yllätyksenä NIS-direktiivin yrityksille

asettamat vaatimukset ja velvoitteet, ja sitä kautta yrityksen toimintaan kohdistuvat riskit. Vuonna 2015 julkaistussa FireEyen tutkimuksessa, johon osallistui yrityksiä Saksasta, Ranskasta ja Iso-Britanniasta ainoastaan 39% vastaajista koki, että heillä on kaikki NIS-direktiivin vaatimat toimenpiteet paikoillaan. Samaan aikaan 34% vastaajista koki, että heillä oli vaillinainen ymmärrys tai ei ollenkaan ymmärrystä direktiivin asettamista vaatimuksista. (IDG Connect & FireEye 2015) Tietosuoja-asetus on kerännyt ihmisten huomion suurilla sanktioillaan, jotka nousevat jopa 20 miljoonaan euroon tai 4% yrityksen globaalista liikevaihdosta, kumpi suurempi. Tämä luo selkeän, helposti numeroiksi muutettavan, riskin yrityksille, mikäli heidän toimintansa ei ole asetuksen mukaista. NIS-direktiivissä ei vastaavia sanktioita direktiivin tasolla anneta, mutta se ei tarkoita, etteikö direktiivi loisi riskejä yrityksille, ja vaatisi yritysten huomiota myös ennen voimaanastumistaan.

Tässä tutkimuksessa keskitytään kuvaamaan direktiivin mukaisia vaatimuksia eikä siinä tulla vertailemaan yksittäisen EU-maiden lakien erityispiirteitä, sillä tutkimuksen tekohetkellä ainoastaan parilla EU-maalla on NIS-direktiivin vaatimukset joko kokonaan tai osittain kattava laki.

1.2 Tutkimuksen tavoitteet ja tutkimuskysymykset

Tämä pro gradu tutkimuksen tavoitteena on kartoittaa, millaisia vaikutuksia NIS-direktiivillä tulee olemaan yritysten toimintaan ja arvioida näitä vaikutuksia riskinäkökulmasta. Tulosten perusteella yritysten on helpompi arvioida heihin kohdistuvia vaikutuksia sekä tarvittavia korjaavia toimenpiteitä. Tutkimuskysymykset:

- Tutkimuskysymys 1: Mitä riskejä NIS-direktiivi tuo yrityksille
- Tutkimuskysymys 2: Mitä direktiivi tuo yritysten riskienhallintaan?
- Tutkimuskysymys 3: Mitkä yritykset kuuluvat direktiivin vaikutuksen piiriin?

1.3 Aikaisemmat tutkimukset

Koska direktiivi on edelleen tuore, siitä ei ole juurikaan julkaistu tutkimuksia. Aihetta sivuavia tutkimuksia on kuitenkin jo tehty esimerkiksi turvallisuuspoikkeamaraportoinnista

ja lakien haittavaikutuksesta tietoyrityksille. Tässä alaluvussa käydään läpi keskeisimpiä aiheeseen liittyviä tutkimuksia. On kuitenkin huomioitava, että suurin osa aikaisemmin tehdyistä NIS-direktiiviin liittyvistä tutkimuksista, artikkeleista ja muista aihetta sivuavista julkaisuista on tehty ennen NIS-direktiivin hyväksymistä. Näin ollen ne keskittyvät enimmäkseen arvioimaan direktiivin mahdollisia vaikutuksia ja todennäköistä sisältöä. Huomioitavaa on myöskin, että pääosin tutkimukset käsittelevät jotakin toista aihetta, ja ainoastaan sivuavat NIS-direktiiviä.

Jo ennen direktiivin julkaisua sen mahdollista sisältöä arvioitiin, ja tutkittiin, miten yritykset ovat valmistautuneet direktiiviin. Tutkimuksessa todettiin, että vain 66% Saksassa, Ranskassa ja Iso-Britanniassa toimivista yrityksistä on valmistautunut direktiivin sisältöön ja yhtä suuri osuus koki, että heille on annettu vähän tai ei ollenkaan opastusta direktiivin sisältöön. (IDG Connect & FireEye 2015)

NIS-direktiivin julkaisun aikoihin kesällä 2016, siitä kirjoitettiin muutamia artikkeleita ja raportteja, jotka lähinnä kuvaavat direktiivin sisältöä (Anon 2016a; Anon 2015; Hammond 2013; Anon 2016b) tai lisäksi analysoivat sitä yleisellä tasolla (Byström 2016). Vaikka NIS-direktiivi pyrkii vähentämään yritysten kohtaamia riskejä (Byström 2016), se samalla luo myös uusia.

Julkaisuja, joissa käsitellään direktiivin mahdollisia vaikutuksia, on julkaistu muutamia. Näissä kuitenkin keskitytään kapeasti, joko tiettyyn vaikutukseen (Guibourg 2015; Holzleitner & Reichl 2017) tai tiettyyn toimialaan(Anon 2017b; Gatlin 2016; Holder ym. 2016; Weber & Studer 2016).

Hurtaud ym. analysoivat turvallisuus- ja ilmoitusvaatimuksia, joita NIS-direktiivi mahdollisesti tuo tullessaan sen piiriin kuuluville toimijoille. (Hurtaud ym. 2016) Lisäksi Euroopan unionin verkko- ja tietoturvavirasto on julkaissut digitaalisille palvelun tarjoajille suunnatun oppaan uuteen NIS-direktiiviin liittyen. Siellä käsitellään tarkemmin sitä, kuka on digitaalinen toimija ja millaisia asioita heidän tulee ottaa huomioon uuden direktiivin myötä.(ENISA 2017)

Ennen kuin EU julkaisee direktiivejä, niille tehdään vaikutusten arviointi. Arvioinnissa vertaillaan erilaisia vaihtoehtoja ja niiden tuomia muutoksia nykytilaan verrattuna. NIS-

direktiivin arvio tehtiin vuonna 2012 ja siinä verrattiin neljää eri vaihtoehtoa, miten direktiivin suunnittelussa voidaan edetä: keskeytetään nykytoimet, jatketaan nykytoimia mutta ei tehdä lisätoimenpiteitä, lisätään suosituksia ja tiedotusta, aloitetaan sääntely. Arviossa keskityttiin vertailemaan näiden vaihtoehtojen välistä paremmuutta sekä sitä, millaisia yhteiskunnallisia vaikutuksia ja millaisia rahallisia vaikutuksia sääntely toisi mukanaan. (Van Dijk Management Consultants & Time.lex 2012)

Myös lakeja ja riskejä on tutkittu eri näkökulmista. Lait keskittyvät erilaisten riskien torjumiseen kuten poliittinen tai sosiokulttuurinen riksi (Haines 2017), mutta ne myös luovat riskejä, kuten compliance-riski (Benedek 2012). Mm. Pitkänen (2005, 11-12) käsittelee väitöskirjassaan lain tuomia riskejä yrityksille, erityisesti IT-yritysten näkökulmasta. Vaikka pääsääntöisesti lait mahdollistavat liiketoiminnan, ne saattavat myös rajoittaa sitä. Lain tuomat rajoitteet luovat riskejä yritykselle ja ovat näin osa yrityksen riskienhallintaa.

1.4 Tutkimusaineisto

EU on julkaissut NIS-direktiivin Euroopan unionin virallisessa lehdessä 19.7.2016. (Euroopan parlamentti ja euroopan unionin neuvosto 2016) Direktiivi resitaaleineen ja liitteineen on 30-sivuinen ja se astui voimaan kahdentenakymmenentenä päivänä lehdessä julkaisun jälkeen, eli 8.8.2016. Jäsenvaltioiden on julkaistava direktiivin noudattamisen edellyttämät lait 9. toukokuuta 2018 mennessä, ja näiden lakien on astuttava voimaan viimeistään 10. toukokuuta 2018.

Koska Suomi ei ollut tutkimushetkellä vielä julkaissut omaa lakiluonnostaan NIS-direktiivin kansallista täytäntöönpanoa varten, tutkimusaineisto koostuu EU:n julkaisemasta NIS-direktiivistä (FI versio) sekä Liikenne- ja viestintäministeriön NIS-direktiivin kansallista täytäntöönpanoa tukevan työryhmän loppuraportista (myöhemmin loppuraportti). (Liikenne- ja viestintäministeriö 2017) Ministeriön loppuraportti on pituudeltaan 35 sivua. Direktiivi koostuu 27 artiklasta ja 75 johdanto-osan kappaleesta (myöhemmin resitaali). Artikloista 21 on oleellisia, kun määritellään direktiivin vaikutuksia yrityksen toiminnalle. Loput artiklat käsittelevät muun muassa jäsenvaltioilta vaadittavia toimenpiteitä.

1.5 Tutkimuksen rakenne

Tutkimus rakentuu kuudesta luvusta siten, että johdantoluvun jälkeen käsitellään NIS-direktiivin sisältöä ja tutkimuksessa käytettyjä teorioita. Tämän jälkeen kuvataan tutkimusmenetelmät ja itse tutkimuksen tulokset. Viimeisessä luvussa tehdään yhteenveto tutkimuksen tuloksista, käsitellään niiden merkitystä ja jatkotutkimusaiheita.

Jotta lukijalla on mahdollisuus ymmärtää tutkimuksen aihetta paremmin, luvussa kaksi esitellään yleisellä tasolla NIS-direktiivin sisältöä. Läpikäydään lyhyesti NIS-direktiivin ja kyberturvallisuuden taustoja EU:ssa eli sitä, miksi direktiivin luomiseen on päädytty. Kuvataan NIS-direktiivin tavoitteita, eli mihin sillä pyritään, sekä sitä, keneen direktiivi kohdistuu ja millaisia velvoitteita, vaatimuksia ja sanktioita näiden rikkomisesta se tälle joukolle asettaa. NIS-direktiiviä tarkastellaan myös kansallisella tasolla Suomen näkökulmasta. Nämä yhdessä auttavat ymmärtämään tutkimuksen kohdetta.

Tutkimuksen kolmannessa luvussa käsitellään riskiä ja riskienhallintaa käsitteinä, jotta voidaan ymmärtää, mitä niillä tässä tutkimuksessa tarkoitetaan. Luvussa esitellään myös tarkemmin tietoriski ja compliance-riski -käsitteet sekä riskienhallintaprosessin osa-alueita ja tavoitteita. Näiden määritelmien pohjalle rakennettiin tutkimuksen tulokset.

Tutkimuksen neljäs luku esittelee tutkimuksessa käytetyt metodit ja menetelmät. Tässä luvussa kuvataan tarkemmin sitä, mitä tarkalleen ottaen tutkittiin ja miten tutkimus suoritettiin.

Viidennessä luvussa esitellään tutkimuksen tulokset sekä prosessi, joilla näihin tuloksiin päädyttiin. Tämä tutkimus koostui useammasta vaiheesta, joissa analysoitiin tutkimusmateriaalin eri osia tuottaen tietoa tutkimuskysymyksiin vastaamiseksi. Ensin läpikäydään toimijoiden määrittämiseen liittyvä osa-alue, sitten liiketoimintariskit, joita direktiivi tuo tullessaan ja lopulta läpikäydään direktiivin tuomat työkalut verkko- ja tietojärjestelmäriskien hallintaan. Saatujen tulosten pohjalta pyritään vastaamaan annettuihin tutkimuskysymyksiin.

Viimeisestä luvusta löytyy yhteenveto tutkimuksen tuloksista sekä vastaukset tutkimuskysymyksiin. Luvussa myös arvioidaan tutkimuksen merkittävyyttä, luotettavuutta, kuvataan rajoitteita ja ehdotetaan jatkotutkimuskohteita.

2 NIS-direktiivi

NIS-direktiivi, eli EU:n verkko- ja tietoturvadirektiivi säädettiin heinäkuussa 2016 ja se astui voimaan saman vuoden elokuussa. Direktiivin täytäntöönpanevien kansallisten lakien on astuttava voimaan viimeistään toukokuussa 2018.

Tässä luvussa esitellään NIS-direktiivin taustoja, tavoitteita, sisältöä ja aikataulua. Sisältöä tarkastellaan vain niiltä osin, kun se on tutkimuksen aiheen kannalta relevanttia, eli sisältää yritysten toiminnalle merkityksellisiä asioita. Direktiivin sisältöä on kokonaisuudessaan kuvattu liitteessä A.

2.1 Taustatekijät

Kyberuhat ovat kasvava uhka yhteiskunnassa niin yritysten, yksilöiden kuin valtioidenkin taholla. Kyberhyökkäykset muuttuvat entistä hienostuneemmiksi. Samalla niiden tekninen luonne on muuttumassa enenevissä määrin strategiseksi.(Lehto & Limnéll 2016) NIS-direktiivin pyrkii vastaamaan tähän alati kehittyvään uhkaympäristöön.

Kyberturvallisuus on ollut puheenaiheena jo pitkään. Hansenin mukaan ensimmäisiä kertoja se mainittiin CSTB:n raportissa 1991.(Hansen ym. 2009) Viime vuosina Euroopan kyberturvallisuuden taso on kuitenkin joutunut enenevissä määrin koetukselle. Viroon kohdistuneet kyberhyökkäykset keväällä 2007 aiheuttivat presidentin, parlamentin ja useiden muiden hallituksen virastojen, uutistoimitusten ja kahden suurimman pankin verkkosivujen kaatumisen.(Hansen ym. 2009) Kuitenkin nyt, vain kymmenen vuotta myöhemmin, Viron katsotaan olevan yksi kyberturvallisuuden mallimaista.

Toinen esimerkki Euroopasta on Ukrainaan kohdistunut kyberisku, jonka avulla kaadettiin maan sähköverkko joulukuussa 2015. Ukrainan isku osoittaa, että kyberhyökkäykset ovat muuttumassa monimutkaisimmiksi ja niiden kerrostuneisuus lisääntyy. Sen sijaan, että kyseessä olisi ollut yksittäinen palvelunestohyökkäys, siinä yhdistyi useita hyökkäysvektoreita kuten sähköverkko-operaattorin järjestelmään ujutettu haittaohjelma ja verkkoyhtiön puhelinpalveluun kohdistettu palvelunestohyökkäys. Sama Ukrainassa käytetty haittaohjelma, BlackEnergy, on havaittu ensimmäisen kerran jo vuonna 2007 ja vuonna 2016 se

löydettiin myös Yhdysvalloissa keskeisen toimijan verkosta. (Pultarova 2016) Suomikaan ei ole säästynyt kyberhyökkäyksiltä. Hiljattain osansa niistä ovat saaneet mm. terveydenhuolto- ja pankkisektori (Paakkanen & Räisänen 2017; Härkönen 2017). Jotta alati kehittyviä hyökkäyksiä vastaan voidaan suojautua, EU on ryhtynyt toimiin yhtenäistääkseen ja kehittääkseen sen jäsenvaltioiden kyberturvallisuutta.

NIS-direktiiviä on valmisteltu vuodesta 2013. Sen juurien voidaan katsoa ulottuvan kuitenkin kauemmas, vuoteen 2001, jolloin solmittiin Budapestin yleissopimus (astui voimaan vuonna 2004). Budapestin yleissopimuksen katsotaan olevan yksi ensimmäisistä tietoverkkorikollisuutta koskevista oikeudellisista välineistä.(Weber & Studer 2016; Sisäministeriö 2013), mutta koska se keskittyy kyberrikollisuuden määrittämiseen ja rankaisemiseen (Weber & Studer 2016), se ei suoranaisesti auta yrityksiä suojautumaan kyberhyökkäyksiltä, sillä sen vaikutus alkaa vasta hyökkäyksen tapahduttua.

Rikollisuuden määritteleminen oli ensimmäinen askel kohti parempaa, mutta se ei kuitenkaan vielä yksin auta suojautumaan rikollisuudelta. Kyberrikoksissa jää myös usein epäselväksi, kuka hyökkäyksen takana oli, joten rangaistusten antaminen voi siten osoittautua hyvinkin vaikeaksi tai jopa mahdottomaksi tehtäväksi. Arvioidaan myös, että sekä yritykset, että yksilöt eivät välttämättä tee rikosilmoitusta kyberrikoksista koska eivät usko virkavallan pystyvän puuttumaan tapahtumiin tai saamaan tekijää kiinni.(NCA Strategic Cyber Industry Group 2016) Tämä osaltaan heikentää yksilöiden uskoa digitaalisiin palveluihin.(Brown 2015)

Toinen keskustelu EU:n tasolla aiheesta käytiin vuonna 2009, kun komissio julkaisi *"Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"*-paperin.(ENISA 2017) Pari vuotta myöhemmin, vuonna 2013, komissio julkaisi EU:n kyberturvallisuusstrategian, joka toimi samalla alkusysäyksenä NIS-direktiiville.(European Commission 2013) Toimien tavoitteena oli parantaa EU:n alueen kyberkestävyyttä. NIS-direktiivi hyväksyttiin heinäkuussa 2016. Kansallisten lakien tulee valmistua toukokuussa 2018 ja listaus keskeisistä toimijoista lokakuussa 2018. (Euroopan parlamentti ja euroopan unionin neuvosto 2016)

Vaikka lailla pyritään vastaamaan riskeihin, ne usein samalla myös luovat riskejä yrityksen toiminnalle. Esimerkiksi ennen EU:n kliinistä tutkimusta koskevan direktiivin (2001/20/EY) täytäntöönpanoa Britanniassa tehtiin 12 prosenttia maailman kliinisistä testeistä, tutkija Matt Ridleyn esittämän kritiikin mukaan direktiivi tuhosi testauksen Britanniassa ja se siirtyi EU:n ulkopuolella, maihin kuten Intiaan. Direktiiviä korjailtiin myöhemmin, mutta se ei enää auttanut palauttamaan toimintoja takaisin EU:n alueelle.(Bartholomew 2016) Direktiivi voi siis olla sen alaisille toimijoille joko uhka tai mahdollisuus. NIS-direktiivin kannalta uhka liittyy sääntelyn epäonnistumiseen esimerkiksi kilpailutilannetta vääristävänä toimenpiteenä. Toisaalta se tarjoaa yrityksille myös mahdollisuuksia toimintansa kehittämiseen ja työkaluja riskienhallintaan.

2.2 Tavoitteet

NIS-direktiivin katsotaan olevan tärkeä osa EU:n kyberstrategiaa, jonka tavoitteena on kehittää avoin ja turvallinen kyberympäristö, joka reagoi kyberhäiriöihin ja -hyökkäyksiin sekä pyrkii ehkäisemään niitä. Ennen direktiivin voimaantuloa kansalliset käytänteet ja yksityisen sektorin toimijoiden varautuminen kyberuhkiin vaihteli laajasti jäsenmaiden välillä ja siksi katsottiin, että yhtenäistäminen on välttämätöntä.(Europan neuvosto 2017) Epäyhtenäinen lähestymistapa loi riskin koordinoimattomista sääntelytoimista, sekavista strategioista ja toisistaan poikkeavista standardeista, jotka yhdessä ovat riittämätön suoja EU:n alueen kyberturvallisuudelle.(Weber & Studer 2016)

NIS-direktiiville on listattu seuraavat päätavoitteet, joiden tarkoituksena on unionin alueella yhdenmukaisen ja korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden saavuttaminen ja ylläpitäminen(Anon 2016b, Art. 1):

- *Parantunut kansallinen kyvykkyys jäsenvaltioissa*: koska internet on ylikansallinen toimintaympäristö tulisi kaikkien jäsenmaiden kyetä reagoimaan siellä esiintyviin häiriöihin, jotta sisämarkkinoiden toiminta ei vaarannu oleellisesti. (Euroopan parlamentti ja euroopan unionin neuvosto 2016) Direktiivissä jokaista jäsenvaliota vaaditaan kehittämään kansallinen kyberstrategia sekä direktiivin mukaiset kansalliset lait ja asetukset. Jäsenvaltioiden täytyy myös perustaa kansallisia toimielimiä,

jotka ovat vastuussa NIS-direktiivin täytäntöönpanosta sekä tietoturvaloukkauksiin reagoiva ja niitä tutkiva yksikkö eli CSIRT-toimija, joka vastaa poikkeamien käsittelystä. (Weber & Studer 2016)

- *Kehittynyt EU-tason yhteistyö*: NIS-direktiivi luo yhteistyöympäristön, jonka tavoitteena on jakaa parhaita käytänteitä sekä tietoja jäsenmaiden välillä esimerkiksi ajankohtaisista riskeistä ja uhista. Tämän nähdään myös luovan pohjaa EU:n yhteisen kyberturvallisuusrintaman luomiselle. Näiden lisäksi halutaan parantaa nykyisiä valmiuksia, sillä niiden ei katsota olevan riittävällä tasolla. Reagoinnin verkko- ja tietojärjestelmien haasteisiin edellyttää EU:n yhtenäistä lähestymistapaa. (Euroopan parlamentti ja euroopan unionin neuvosto 2016)

- *Turvallisuus- ja tietoturvatapahtuma ilmoitusvaatimukset:* direktiivillä pyritään parantamaan verkko- ja tietojärjestelmien turvallisuutta ja luotettavuutta ja sitä kautta turvaamaan sisämarkkinoiden toiminta. Järjestelmien katsotaan olevan olennaisen tärkeitä useille talouden ja yhteiskunnan toiminnoille. Jotta direktiivin pyrkimys riskienhallintakulttuurin kehittämisestä ja vakavimpien tietoturvatapahtumien raportoinnista toteutuisi, on direktiivi asetettu koskemaan keskeisiä toimijoita (Liite B) ja digitaalisia toimijoita (Liite C) (Euroopan parlamentti ja euroopan unionin neuvosto 2016). Ilmoitusvelvollisuus luo myös paremman mahdollisuuden muille toimijoille suojautua kyseiseltä uhalta (Laube & Böhme 2016)

Direktiivin suorien tavoitteiden lisäksi katsotaan, että säännösten yhdenmukaistaminen parantaa sisämarkkinoiden toimintaa ja madaltaa yritysten maasta toiseen laajentumisen kustannuksia. EU:n tekemän arvion mukaan yksittäiselle yritykselle aiheutuu 9000€ lisäkulu liiketoiminnan laajentamisesta toiseen EU-maahan. Toisaalta digitaalisten sisämarkkinoiden toteutuminen täydellisesti voisi mahdollistaa 415 miljardia euroa kasvua EU:n bruttokansantuotteeseen. Tästäkin syystä katsotaan tärkeäksi, ettei jäsenvaltioiden eroavat lainsäädännöt hidasta tai estä markkinoiden kehitystä. (Liikenne- ja viestintäministeriö 2017, 13) Toisaalta markkinoiden koetaan kärsivän luottamuspulasta, mikä hidastaa markkinoiden kehitystä. Esimerkiksi robottiautojen on ansaittava asiakaskunnan luottamus, jotta ne hyväksyttäisiin markkinoille. Luottamusta uusiin palvelumuotoihin voi heikentää joko ta-

hattomat virheet, kuten virhe koodissa tai rajapinnassa, tai tahalliset tietoturvaloukkaukset kuten palvelunestohyökkäykset tai tietomurrot (Liikenne- ja viestintäministeriö 2017, 13)

NIS-direktiivin avulla pyritään luomaan yhtenäinen ja koordinoitu lähestymistapa lainsäädännölle, kansallisille strategioille ja standardeille EU:n alueella. Näiden katsotaan tukevan EU:n kulkua kohti strategisia tavoitteitaan: avointa ja turvallista kyberympäristöä. Avoin ja turvallinen kyberympäristö myös tukee sisämarkkinoiden toimintaa sekä asiakkaiden luottamusta uusiin palvelunmuotoihin.

2.3 Velvoitteet, vaatimukset ja sanktiot

Velvoitteilla, vaatimuksilla ja sanktioilla pyritään saavuttamaan NIS-direktiiville asetetut tavoitteet. Direktiivi asettaa listan velvoitteita, kuten ilmoitusvelvollisuus, niin jäsenmaille kuin valituille yksityisen ja julkisen sektorinkin toimijoille. Se myös esittää vaatimuksia direktiivin alaisille toimijoille esimerkiksi vaatien toimenpiteitä verkko- ja tietojärjestelmäturvallisuuden riskien vaikutusten minimoimiseksi. Mikäli velvoitteita ei täytetä tai vaatimuksia noudateta on siitä direktiivin nojalla annettava sanktio.

Jotta NIS-direktiivi saavuttaisi sille asetetut tavoitteet, on se määritelty koskemaan keskeisiä toimijoita sekä digitaalisia toimijoita. Keskeiset toimijoihin kuuluu muun muassa finanssi, energia ja terveyssektorin toimijat. Jokaisen jäsenmaan tulee märittää joko listaamalla kaikki keskeiset toimijansa tai vaihtoehtoisesti antamalla kriteerit, joiden mukaan keskeiset toimijat voidaan määrittää yksiselitteisesti. Tätä listaa tulee jokaisen maan päivittää kahden vuoden välein. Direktiivin tarkoittamat digitaaliset toimijat ovat verkkomarkkinapaikat, hakukoneet ja pilvipalvelut.(Euroopan parlamentti ja euroopan unionin neuvosto 2016) Koska keskeisten palvelujen tarjoajat ja digitaalisen palvelun tarjoajat eroavat toisistaan esimerkiksi ensimmäisen ollessa suoraan linkittynyt kriittiseen infrastruktuuriin, kun taas toisen toiminta on rajoja ylittävää, on direktiivissä yksilöity kummankin toimijan kohdalta niitä koskevat määritelmät ja toimenpiteet. (resitaali 57).

Direktiivin tarkoittama keskeisen palvelun tarjoaja voi olla julkinen tai yksityinen toimija, joka on direktiivin liitteessä II esitettyä tyyppiä (listaus toimijoiden tyypeistä kts. liite B). Direktiiviä sovelletaan vain sellaisiin julkishallintoihin, joiden katsotaan olevan keskeisen

palvelun tarjoajia (resitaali 45). Jokaisen jäsenmaan tulee määrittää erikseen keskeisiksi katsomansa palvelut ja tämän perusteella keskeisten palvelujen tarjoajat, jotka toimivat jäsenmaan alueella (5 artikla) ja joiden näin katsotaan olevan direktiivin piirissä. Vaihtoehtoisesti palveluntarjoajien määrittämisen sijaan jäsenmaa voi listata kriteerit, joiden perusteella keskeisten palvelujen tarjoajat voidaan määrittää (5 artikla 7 kohta; resitaali 25). Kriteerien tulee olla määrällisesti ilmaistuja esimerkiksi käyttäjien määrä tai tuotantomäärä, jotta lain piiriin kuuluvat toimijat voidaan määrittää objektiivisesti ja yksiselitteisesti (resitaali 25). Palvelun tarjoajan katsotaan toimivan jäsenmaan alueella vain, mikäli sillä on tosiasiallista toimintaa ja kiinteä toimipaikka kyseisessä jäsenmaassa. Toimijan yritysmuodolla, tai sillä onko kyseessä tytäryhtiö tai sivuliike ei ole merkitystä (resitaali 21). Näillä toimilla EU pyrkii varmistamaan direktiivin täytäntöönpanon johdonmukaisuuden alueellansa (resitaali 19). Jäsenmaiden tulee julkaista keskeisten palvelujen tarjoajat viimeistään 9. marraskuuta 2018 (5 artikla 1 kohta). Jäsenmaiden tulee tarkastaa määritelmänsä kahden vuoden välein ja toimittaa päivitetty määritelmä EU:lle (5 artikla 7 kohta).

Direktiivin määrittämien toimialojen lisäksi toimijan tulee täyttää seuraavat kriteerit ollakseen keskeinen palvelun tarjoaja (5 artikla 2 kohta): yhteiskunnan tai talouden kriittisten toimintojen tulee olla riippuvaisia toimijan tarjoamasta palvelusta, tarjotun palvelun tulee olla riippuvainen verkko- ja tietojärjestelmistä ja poikkeaman tulee aiheuttaa merkittävää haittaa palvelun tarjoamiseen. Jäsenmaiden tulee määrittää jokaisen toimialan alueen osalta, mitkä alueen palveluista voidaan katsoa kriittisiksi, sillä kaikki palvelut vaikkakin niitä tarjoaa liitteessä B listattu keskeisen palvelun tarjoaja, eivät ole kriittisiä. Esimerkiksi lentokenttäoperaattori tarjoaa palveluita, jotka voidaan katsoa kriittisiksi kuten kiitorata, mutta myös sellaisia palveluita, mitkä eivät ole kriittisiä, kuten matkustajatilastot (resitaali 22). Palvelun kriittisyyttä arvioitaessa on otettava huomioon palvelusta riippuvaisten käyttäjien ja muiden toimijoiden määrä, toimijan markkinaosuus ja toimijan merkitys kyseisen palvelun ylläpitämisessä, maantieteellinen levinneisyys, ja vaikutus, mikä sillä saattaa olla yleiseen turvallisuuteen tai talouden ja yhteiskunnan toimintoihin (6 artikla 1 kohta). Merkittävää haittaa arvioitaessa tulee huomioida suorat ja epäsuorat vaikutukset (resitaali 27)

Keskeisten palvelujen tarjoajien ulkopuolelle tulee jättää direktiivin 2002/21/EY alaiset yleiset viestintäverkkoja tai sähköisiä viestintäpalveluja tarjoavat yritykset joihin sovelle-

taan mainitun direktiivin erityistä turvallisuutta ja eheyttä koskevia vaatimuksia. Ulkopuolelle jäävät myös asetuksen 910/2014 mukaiset luottamuspalvelun tarjoajat, sillä heihin sovelletaan kyseisen asetuksen turvallisuusvaatimuksia (resitaali 7). Lisäksi vesiliikenteelle on jo nykyisellään EU:n säädösten asettamia turvallisuusvaatimuksia tietokone järjestelmille ja verkoille. Näiden katsotaan olevan erityissäännöksiä (lex specialis), niiltä osin, kun ne ovat vähintään NIS-direktiivin säännöksiä vastaavia (resitaali 10). Vesiliikenteen palvelun tarjoajia määrittäessä tulee myös huomioida Kansainvälisen merenkulkujärjestön nykyiset ja tulevat säännöstöt, jotta lähestymistapa alan yksittäisiin palvelujen tarjoajiin on johdonmukainen (resitaali 11). Kolmas erityishuomioitava ala on pankki- ja finanssiala, jolla on jo nykyisellään olemassa olevaa monia muita aloja tiukempaa säätelyä ja sen katsotaan olevan hyvin yhdenmukaista EU:n alueella (resitaali 12). Säätelyn katsotaan olevan myös useilta osin tiukempaa kuin mitä NIS-direktiivi vaatii ja alalla on jo käytössä ilmoitusvelvollisuutta koskevia vaatimuksia. Vaatimusten noudattamista valvoo useampi viranomainen, mikä muiden seikkojen ohella on hyvä huomioida direktiivin täytäntöönpanossa (resitaali 13).

Jotta keskeisten palvelujen määritelmä on yksiselitteinen, on tärkeää, että keskeiseksi katsotut palvelut määritetään erikseen. Palvelujen listausta käytetään myös EU:n toimesta, kun määritellään jäsenvaltioiden määrittämisprosessin yhdenmukaisuuden tasoa (resitaali 23). Mikäli keskeinen palvelujen tarjoaja toimii useammassa kuin yhdessä jäsenvaltiossa, tulee jäsenvaltioiden yhdessä arvioida, onko palveluntarjoaja kriittisessä asemassa rajat ylittävien palveluiden suhteen. Samalla jäsenmailla on mahdollisuus keskustella näihin palveluihin liittyvistä riskeistä (resitaali 24).

Koska monet yritykset, myös keskeiset palvelujen tarjoajat, ovat enenevissä määrin riippuvaisia digitaalisista palveluista, haluttiin myös digitaaliset palvelut ottaa osaksi direktiivin toimivaltaa. Erityisesti tämä katsottiin tärkeäksi siksi, että usea digitaalisen palvelun tarjoaja on markkinoilla niin hallitsevassa asemassa, että käyttäjillä ei välttämättä ole vaihtoehtoista palveluntarjoajaa ja sitä kautta digitaalisen palvelun häiriö saattaa estää muiden siitä riippuvien palvelujen tarjoamisen ja siten aiheuttaa merkittävää haittaa yhteiskunnalle tai keskeisille taloudellisille toimijoille (resitaali 48). Direktiivin tarkoittama digitaalisen palvelun tarjoaja on oikeushenkilö (4 artikla 6 kohta), joka tarjoaa jotakin seuraavista digitaa-

lisista palveluista: verkossa toimiva markkinapaikka, verkossa toimiva hakukone tai pilvipalvelu (direktiivin määritelmä kts. liite C).

Verkossa toimiva markkinapaikka on toimija, joka tarjoaa kuluttajalle tai elinkeinonharjoittajalle mahdollisuuden tehdä verkossa kauppa- tai palvelusopimus elinkeinoharjoittajan kanssa. Tämä voi tapahtua joko verkossa toimivan markkinapaikan sivustolla tai elinkeinonharjoittajan verkkosivustolla silloin, kun markkinapaikka tarjoaa tietojenkäsittelypalvelun (4 artikla 17 kohta). Tarjottava tietojenkäsittelypalvelu voi olla maksutapahtuman käsittely, käyttäjien profilointi tai tietojen yhdistäminen (resitaali 15). Direktiivin tarkoittama markkinapaikka ei kuitenkaan kata välittäjäpalveluita, jotka ohjaavat käyttäjän kolmannen osapuolen sivustolle, missä sopimus lopulta tehdään. Esimerkiksi palvelu, jossa vertaillaan tuotteiden hintoja, mutta ohjataan käyttäjä valitun verkkokaupan palveluun tuotteen tai palvelun ostamiseksi, on välittäjäpalvelu, eikä näin kuulu direktiivin piiriin. Sovelluskaupat katsotaan markkinapaikoiksi siinä missä muutkin kaupalliset toimijat, jotka myyvät muiden kolmansien osapuolien tuotteita (resitaali 15).

NIS-direktiivissä hakukoneella viitataan digitaaliseen palveluun, jonka avulla käyttäjällä on mahdollisuus tehdä hakuja kaikilta verkkosivustoilta valitsemallaan hakusanan tai muussa muodossa, kuten kuvahaku, tehdyn haun perusteella (4 artikla 18 kohta). Tuloksena haulle on linkkejä, josta voi saada haettuun sisältöön liittyviä tietoja. Hakukoneella ei tarkoiteta sivuston sisällä tapahtuvia hakuja, vaikka palvelun tarjoaisi ulkoinen hakukone eikä verkkopalveluja, joissa vertaillaan tuotteiden hintoja ja käyttäjä ohjataan elinkeinonharjoittajan palveluun tuotteen ostamiseksi (resitaali 16).

Pilvipalvelu kattaa joukon digitaalisia palveluja, joiden tarkoituksena on tarjota skaalautuvia jaettavissa olevia tietoteknisiä resursseja esimerkiksi tallennustilaa tai tiettyä pilvessä toimivaa sovellusta (4 artikla 19 kohta; resitaali 17). Skaalautuvalla tarkoitetaan resursseja, jotka voidaan jakaa käyttömäärän mukaan resurssien fyysisestä sijainnista riippumatta. Jaettavissa oleva tarkoittaa, että samaa palveluresurssia jaetaan useille käyttäjille, mutta jokaisen käyttäjän käsittely tapahtuu erikseen (resitaali 17).

Digitaalisten palvelun tarjoajien oletetaan tunnistavan ja hallitsevan verkko- ja tietojärjestelmäturvallisuuteen kohdistuvia riskejä ja huomioivan järjestelmien ja fyysisenturvalli-

suuden, häiriönhallinnan, jatkuvuudenhallinnan, valvonnan, tarkastuksen ja testauksen sekä kansainvälisten standardien noudattamisen. Heidän oletetaan myös hallitsevan tapahtumien vaikutuksia verkkoturvallisuutta ja tietojärjestelmien turvallisuutta uhkaavissa tapahtumissa (16 artikla 8 kohta). Kun häiriön vakavuutta arvioidaan tulisi huomioida ainakin seuraavat: käyttäjien määrä, johon häiriö vaikuttaa, häiriön kesto, häiriön maantieteellinen levinneisyys, häiriön laajuus palvelussa, häiriön vaikutus taloudellisiin ja yhteiskunnallisiin toimintoihin. (16 artikla 4 kohta) Ilmoituksen jälkeen viranomaisella on oikeus tiedottaa häiriöstä tai vaatia digitaalista palvelun tarjoajaa julkaisemaan tiedotteen häiriöstä (16 artikla 7 kohta). Viranomaisilla on oikeus saada verkko- ja tietojärjestelmäturvallisuutta koskeva tieto käyttöönsä niiltä osin, kun se on tarpeellista palvelun tarjoajan turvallisuuden tilan arviointiin (17 artikla 2 kohta). Digitaaliset palveluntarjoajat ovat myös velvollisia tekemään vaadittavat korjaukset, mikäli tarkastuksessa ilmenee puutteita (resitaali 69).

Keskeiset palvelujen tarjoajat ja digitaalisen palvelun tarjoajat ovat itse vastuussa käyttämiensä verkko- ja tietojärjestelmien turvallisuudesta ja ilmoitusvelvollisuudesta. Sillä tuottavatko he verkko- ja tietojärjestelmiin liittyvät palvelut itse vai onko niiden ylläpito ulkoistettu kolmansien osapuolien vastuulle, ei ole merkitystä (resitaali 52). Laitteiden valmistajat ja ohjelmistojen kehittäjät eivät ole direktiivin alaisia toimijoita, mutta niiden katsotaan olevan läheisesti siihen liittyviä, sillä heidän toiminnallaan on vaikutusta myös direktiivin alaisten toimijoiden toimintaan erityisesti turvallisuuden mahdollistajana (resitaali 50).

Vaikka direktiivin vaikutukseen on valittu vain joukko toimijoita se ei tarkoita, etteikö jäsenmaat voisi laatia paikallisia verkko- ja tietojärjestelmäturvallisuutta koskevia säädöksiä, jotka koskevat laajempaa joukkoa toimijoita (resitaali 58). Jäsenmaita jopa kehotetaan luomaan verkko- ja tietoturvajärjestelmäturvallisuutta koskevia ohjeistuksia julkishallinnon toimijoille, jotka eivät kuulu direktiivin piiriin (resitaali 45). Samalla on kuitenkin huomattava, että direktiivin piirissä oleville digitaalisen palvelun tarjoajille ei saa asettaa muita turvallisuus- tai ilmoitusvaatimuksia jäsenvaltiotasolla (16 artikla 10). Direktiivin mukaan myös sen vaikutuspiirin ulkopuolella olevilla toimijoilla täytyy olla mahdollisuus ilmoittaa havaituista poikkeamista toimivaltaiselle viranomaiselle tai CSIRT-toimijalle (resitaali 67).

Direktiivin asettamissa vaatimuksissa on eroavaisuuksia digitaalisten toimijoiden ja keskeisten toimijoiden välillä. Lisäksi esimerkiksi pienet digitaaliset toimijat, joilla on työntekijöitä alle 50 ja liikevaihto alle 10 miljoona euroa, on vapautettu direktiivin turvallisuus- ja ilmoitusvaatimuksia.(Hurtaud ym. 2016) Direktiivin resitaaleissa mainitaan myös laitteiden valmistajien ja ohjelmistokehittäjien rooli verkko- ja tietojärjestelmien turvallisuudessa, vaikka nämä eivät olekaan suoraan direktiivin alaisia toimijoita. (Euroopan parlamentti ja euroopan unionin neuvosto 2016) Direktiivin toimijoille asettamat keskeiset vaatimukset liittyvät toimijoiden reagointivalmiuteen ja ilmoitusvelvollisuuteen.

Direktiivi ei suoraan määrittele, millaisia seurauksia tai sanktioita sen määräysten rikkomisesta tulisi kansallisella tasolla asettaa. Siinä kuitenkin todetaan, että *”seuraamusten on oltava tehokkaita, oikeasuhteisia ja varoittavia”*.(Euroopan parlamentti ja euroopan unionin neuvosto 2016) Direktiivin määritelmä on hyvin suurpiirteinen ja antaa jokaiselle jäsenmaalle mahdollisuuden määrittää sanktiot oman tulkintansa mukaisiksi.

Direktiivi antaa reunaehdot sille, miten sen toteutus kansallisella tasolla tulee järjestää. Direktiivin antamat ohjeistukset myös pyrkivät yhdenmukaiseen lainsäädäntöön EU:n alueella ja EU pyrkii tarvittaessa yhdenmukaistamaan säädöksiä niiden voimaanastumisen yhteydessä. Se, miten keskeiset toimijat määritellään ja mitkä tulevat olemaan lopulliset sanktiot riippuu kuitenkin pitkälti jäsenmaiden sisäisistä päätöksistä.

2.4 Direktiivi kansallisella tasolla

Suomi on parhaillaan työstämässä kansallista lainsäädäntöä, jolla täyttää NIS-direktiivin asettamat vaatimukset. Liikenne- ja viestintäministeriön työryhmä julkaisi tietoturva direktiivin kansallista täytäntöönpanoa tukevan loppuraportin keväällä 2017, jossa se arvioi kansallisia toimenpiteitä, joita direktiivin mukainen toiminta edellyttää.(Liikenne- ja viestintäministeriö 2017) Tutkimuksen tekohetkellä laista tai direktiivin mukaisista lakimuutoksista ei ollut julkaistu luonnosta, joten ne eivät sisälly tutkimukseen. Direktiivin vaatima kansallinen strategia: Suomen tietoturvallisuusstrategia julkaistiin 2016. (Liikenne- ja viestintäministeriö & Tietoturvallisen liiketoiminnan kehittämisryhmä 2016)

EU tasolla Suomi on listattu kyberturvallisuuden kärkipään toimijaksi useammassa eri tutkimuksessa.(Lehto & Limnéll 2016) Liikenne- ja viestintäministeriön (2017) työryhmän selvityksessä käy ilmi, että Suomessa on useilla aloilla jo tälläkin hetkellä riskienhallintaan ja tietoturvaan liittyviä lakien asettamia velvoitteita, ja heidän mukaansa Suomen lainsäädäntö turvaa jo tälläkin hetkellä korkeatasoisen tietosuojan ja tietoturvan verrattuna muihin jäsenmaihin. Lisäksi Suomen tietoturvallisuusstrategia (Liikenne- ja viestintäministeriö & Tietoturvallisen liiketoiminnan kehittämisryhmä 2016), jota direktiivikin vaatii, julkaistiin vuoden 2016 alkupuolella. Strategia on jatkoa vuosina 2003 ja 2008 julkaistuille tietoturvastrategioille ja 2013 julkaistulle kyberturvallisuusstrategialle. Tietoturvastrategiassa mainitaan NIS-direktiivin täytäntöönpanosta, että sen tulee olla mahdollista sovittaa osaksi yrityksen liiketoimintariskien hallintaa.

Yksi oleellisista, jo olemassa olevista laeista, on tietoyhteiskuntakaari (917/2014), joka astui voimaan vuoden 2015 alusta ja kokosi, korvasi ja täydensi useita viestintään liittyviä lakeja ja säädöksiä, kuten sähköisen viestinnän tietosuojalaki (516/2004). Tietoyhteiskuntakaaren tavoitteena on muun muassa edistää ja suojata sähköisiä viestinnän palveluita ja varmistaa niiden saatavuus koko maassa sekä *”turvata sähköisen viestinnän luottamuksellisuus ja yksityisyyden suojan toteutuminen”*(Oikeusministeriö 2014). Tietoyhteiskuntakaaressa määrätään myös, että viestintäverkkojen ja -palvelujen täytyy kestää tavallisimmat tietoturvauhat ja niihin kohdistuvat merkittävät tietoturvauhat, -loukkaukset, viat ja häiriöt täytyy kyetä havaitsemaan. Tietoyhteiskuntakaari sisältää myös häiriöistä ilmoittamisvelvoitteen ja säätää viestinnän ja palvelujen jatkuvuuden turvaamisesta. (Liikenne- ja viestintäministeriö 2017, 16)

Toinen oleelliseksi katsottu jo voimassa oleva laki on henkilötietolaki (523/1999), joka sisältää määräyksiä muun muassa henkilötiedon käsittelyyn, arkaluontoisten henkilötietojen käsittelyyn, rekisteröidyn oikeuksiin ja tiedon hävittämiseen ja korjaamiseen. Lisäksi henkilötietolain luku 7 käsittelee tietoturvallisuutta ja henkilötietojen säilytystä. Tietojen suojaamisesta rekisterinpitäjä velvoitetaan toteuttamaan *”tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen häviämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä”*.(Oikeusministeriö 1999) Henkilötieto-

laissa ei kuitenkaan nykyisellään säädetä NIS-direktiivin mukaisesta ilmoitusvelvollisuudesta. (Liikenne- ja viestintäministeriö 2017)

NIS-direktiivin alaisilta toimijoilta toimialakohtaista lakisäätelyä löytyy ainakin energia-, liikenne-, pankki-, terveydenhuoltosektorilta ja juomaveden toimittamiseen ja jakeluun liittyen. (Liikenne- ja viestintäministeriö 2017, 17-23) Vaikka Suomessa on jo olemassa olevaa lainsäädäntöä, työryhmän mukaan nämä ovat pirstaloituneita ja koskevat ainoastaan tiettyjä toimintoja, eivät kattavasti koko toimialaa. Samalla todettiin, että riskienhallinta on hyvin summittaisesti kuvattua, eikä voida yksiselitteisesti sanoa, koskeeko se myös tietoturvaan liittyviä riskejä. Velvoitteita tietoturvapoikkeamista ilmoittamisesta oli vain harvoilla toimialoilla. (Liikenne- ja viestintäministeriö 2017, 27-28)

Suomessa on nykytilanteessa useita viranomaisia, jotka hoitavat valvontatehtäviä eri toimialoilla. Tällaisia ovat esimerkiksi Trafi, Finanssivalvonta, Valvira ja Viestintävirasto. Liikenne- ja viestintäministeriön (2017) työryhmän mukaan tämä saattaakin aiheuttaa tilanteen, missä toimijoille syntyy päällekkäisiä ilmoitusvelvollisuuksia, mikäli NIS-direktiivin vaatima valvonta keskitetään yhdelle viranomaiselle. Toisaalta, mikäli tehtävä jaettaisiin nykyisten valvontaviranomaisten kesken, saatetaan näille laissa määriteltyjä toimivaltuuksia joutua laajentamaan nykyisestä.(Liikenne- ja viestintäministeriö 2017, 15)

Valtionhallinnon osalta NIS-direktiivissä todettiin, että sitä ei saa asettaa NIS-direktiivin alaiseksi toimijaksi, mutta jäsenmaita suositellaan luomaan erillisiä tietoturvaohjeita tai säädöksiä valtionhallinnon toiminnoille. Suomessa on jo useamman vuoden täytetty tämä suositus erillisillä valtionhallinnon tietoturvaohjeistuksella (VAHTI-ohje) sekä valtionneuvoston asetuksella (681/2010), jossa säädetään asiakirjojen käsittelyn tietoturvallisuusvaatimuksista, asiakirjojen luokittelusta ja luokiteltujen asiakirjojen tietoturvallisuusvaatimuksista. .(Liikenne- ja viestintäministeriö 2017)

Työryhmän mukaan nykyinen lainsäädäntö ei kata NIS-direktiivin asettamia vaatimuksia ja suositteli, että vaatimukset implementoitaisiin osaksi jo olemassa olevia toimiala kohtaisia lakeja, sillä heidän mukaansa erillinen laki ei täyttäisi samalla tavalla NIS-direktiivin vaatimuksia ja saattaisi johtaa päällekkäisyyksiin eri lakien välillä. (Liikenne- ja viestintäministeriö 2017)

NIS-direktiivin voidaan katsoa tuovan lisävelvoitteita ainakin ilmoitusvelvollisuuteen, josta nykyisellään ei ole olemassa selkeää käytäntöä verkko- ja tietojärjestelmiin kohdistuvien poikkeamien osalta.

3 Riskit ja niiden hallinta

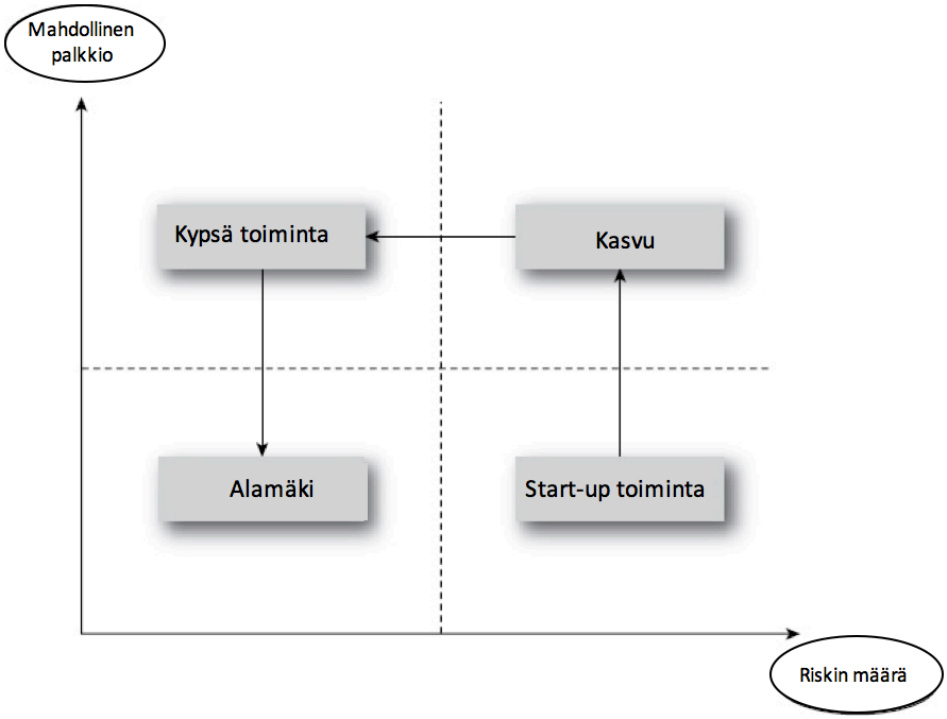
Tässä tutkielman teorialuvussa käsitellään riskin ja riskinhallinnan käsitteitä ja läpikäydään olennaisimmat riskimuodot.

3.1 Riski käsitteenä

ITILin määritelmän mukaan riski on ”*jokin mahdollinen tapahtuma, joka voi tuottaa harmia tai menetyksen, tai vaikuttaa mahdollisuuteen saavuttaa tavoitteet”*. (ITIL 2011) Riskin voikin jakaa kahteen osaan: epävarmuus tapahtumasta, esimerkiksi säähän liittyvä epävarmuus voi olla sataako huomenna, ja toiseksi, riskin epävarmuuteen liittyy aina mahdollinen negatiivinen lopputulos, sillä epävarmuus kahden positiivisen lopputuloksen välillä ei luo tilanteeseen riskiä. (Chavas 2004) Eli se, että huomenna saattaa sataa ei ole riski, mikäli säällä ei ole meille merkitystä. Sateen mahdollisuudesta tulee riski, mikäli suunnittelimme piknikiä puistossa.

Kuten Harisalo (2005) kirjoituksessaan toteaa, yrittäjyys on keksivä, uutta luova prosessi, joka myös synnyttää riskejä, joten riskien voidaankin katsoa olevan olennainen osa liiketoimintaa ja yrittäjyyttä (Ilmonen ym. 2010; Hopkin 2017). Kuten Ilmonen ja kumppanit (2010) toteavat *”liiketoiminta on pohjimmiltaan riskin ottamista”* ja *”liiketoiminnan logiikalle olisi vierasta pyrkiä poistamaan kaikki yrityksen riskit”*. Liiketoiminta onkin pohjimmiltaan juuri tasapainottelua riskin ja mahdollisen palkkion välillä.

Riskin määrä suhteessa mahdollisesti saavutettavaan palkkioon vaihtelee yrityksen elinkaaren eri vaiheissa. Kuten Hopkin (2017) esittää, riskin määrä mahdollisen palkkion suuruuteen on suurimmillaan yrityksen aloitusvaiheessa (Kuvio 1).



Kuvio 1. Riskin ja mahdollisen palkkion suhde yrityksen elinkaaren eri vaiheissa
(käännös alkuperäisestä Hopkin 2017)

Suominen (2003) toteaa, että kattavaa listaa liikeriskeistä on mahdotonta muodostaa. Lisäksi riskiympäristö kehittyy ja muuttuu nopeasti, joten myös yritykseen kohdistuvat riskit muuttuvat ympäristön mukana. Ilmosen ja kumppaneiden esittelemän mallin mukaan yritystoiminnan riskit voidaan kuitenkin lajitella neljään kategoriaan: strategiset riskit, taloudelliset riskit, operatiiviset riskit ja vahinkoriskit.(Ilmonen ym. 2010) Strategiset riskit liittyvät yrityksen pitkänaikavälin strategisiin päätöksiin, joten niiden lopputulos voi olla joko positiivinen tai negatiivinen. Operatiiviset riskit liittyvät yrityksen päivittäisiin toimintoihin ja taloudelliset riskit yrityksen rahaprosesseihin liittyviin toimintoihin kohdistuviin riskeihin. Vahinkoriskit nimensä mukaisesti liittyvät yritykselle tapahtuviin vahinkoihin, kuten työtapaturmat ja ympäristövahingot. Vahinkoriskit ovat usein myös niitä riskejä, jotka voidaan vakuuttaa.(Ilmonen ym. 2010)

Riskinottohalu vaihtelee suuresti yritysten välillä. Osa yrityksistä välttää riskejä, kun toiset ovat riskinottohaluisia. Yrityksen riskinotto haluun vaikuttaa myös toimiala, toimialan kehittymisaste sekä yksittäisten johtohenkilöiden suhtautuminen riskeihin. (Hopkin 2017)

3.2 Tietoriski

Jotta voidaan paremmin ymmärtää NIS-direktiiviä, sen sisältöä ja mahdollisia siihen liittyviä uhkia, on hyvä ymmärtää, miltä sillä yritetään suojautua. Parantamalla verkko- ja tietoturvaympäristöä EU:ssa, samalla pyritään vähentämään tietoriskiä.

Suomisen (2003, 79) mukaan tietoriskit ovat ”*tietoihin ja niiden käyttöön kohdistuvan tapahtuman uhka*”. Suominen (2003) kirjoittaa tietoriskien kumpuavan riippuvuudesta tietojärjestelmiin ja niiden avulla tarjottuihin palveluihin. Lisäksi hän toteaa *”julkisten ja yksityisten verkkojen yhdistäminen, hajautetun tietojenkäsittelyn yleistymisen sekä palveluiden ulkoistamisen heikentäneen organisaatioiden mahdollisuuksia valvoa tehokkaasti tietoturvallisuuttaan.”*. Ilmosen et kumppaneiden (2010) mukaan IT-riskit, jonka olennainen osa tietoriskikin on, jää edelleen usein yksittäisten yksikköjen varaan, vaikka sen pitäisi olla osa yrityksen kokonaisriskienhallintaa. Heidän mukaansa ongelmana usein on se, että liiketoiminnalta ja IT-osastolta puuttuu yhteinen kieli. (Ilmonen ym. 2010) Tietoriskin lisäksi IT-riskeihin kuuluu it-palveluiden hankintaan, tuottamiseen ja hallintaan liittyvät riskit. (Ilmonen ym. 2010)

NIS-direktiivin kuvauksen mukaan ”*... tietojärjestelmien turvallisuudella tarkoitetaan järjestelmien kykyä suojautua tietyllä varmuudella toimilta, jotka vaarantavat tallennettujen tai käsiteltyjen tietojen ... saatavuuden, aitouden, eheyden tai luottamuksellisuuden.*” (Anon 2017a) Täten tietoriski on riski, joka kohdistuu yllämainittuihin tiedon saatavuuteen, aitouteen, eheyteen tai luottamuksellisuuteen. Tietoriskit ovat luonteeltaan vahinkoriskejä, eli niihin ei liity tuotto-odotuksia vaan ne johtavat lähes aina menetyksiin (Suominen 2003), ja kuten usein vahinkoriskien kohdalla myös tietoriskejä vastaan on saatavilla vakuutuksia. (Saarelainen 2016)

Kuten Suominen toteaa kirjassaan Riskienhallinta (2003, 79) *”organisaatiot joutuvat hyväksymään sen, että tietojärjestelmiä ei ole suunniteltu turvalliseksi”.* Jotta järjestelmähaavoittuvuuksia ja niiden luomia riskejä voidaan tarkastella, tulee organisaation ensin tunnistaa liiketoimintaprosessinsa. Vasta tämän jälkeen kyetään tarkastelemaan liiketoimintaprosesseihin liittyviä tietojärjestelmiä, niihin liittyviä riskejä ja lopulta itse tietoihin kohdistuvia riskejä. (Ilmonen ym. 2010)

Tietoriskejä voidaan jakaa osa-alueisiin esimerkiksi ISO27001 tietoturvastandardin mukaisesti. Tietoturvallisuutta voidaan kehittää valitsemalla jokaiselle osa-alueelle, niille parhaiten sopivat turvamekanismit. (Suominen 2003) Suomisen (2003) mukaan ”*Turvallisuusvaatimusten tunnistamisen apuna on kolme pääasiallista lähdettä:*

1. *Tietoriskien kartoitus, jossa tunnistetaan uhat sekä arvioidaan uhan toetutumisen todennäköisyys ja vahingot*
2. *Lait, asetukset ja sopimukset, jotka velvoittavat organisaatiotta.*
3. *Tietojenkäsittelyyn liittyvät periaatteet, jotka organisaatio on määritellyt toimintansa tueksi.”*

Kuten kaikessa riskienkartoituksessa, myös tietoriskikartoituksen tavoitteena on löytää suurimmat uhkatekijät sekä arvioida niiden todennäköisyyttä sekä uhan suuruusluokkaa. Tietoriskien kohdalla tulee kuitenkin huomioida, että niillä on erityisominaisuuksia verrattuna yleisiin riskeihin. Suomisen (2003) mukaan tärkein erityisominaisuuksista on tiedon abstraktisuus, jonka takia tiedon arvoa ja sitä uhkaavia riskejä on hankalampi määritellä. Myös tiedon rahallisen arvon määrittäminen on haastavaa ja lisäksi välittömien vaikutusten lisäksi tietoriskeihin liittyy paljon välillisiä vaikutuksia. (Suominen 2003; Ilvonen 2013)

Yritykset tunnistavat tietoriskien luoman uhan, mutta silti niihin varaudutaan edelleen huonosti. PricewaterhouseCoopersin (2017) maailmanlaajuisessa yritysjohdolle tehdyssä tutkimuksessa, 62% vastaajista uskoi kyberriskin, joka on läheistä sukua tietoriskeille, aiheuttavan haittaa seuraavan 3 vuoden aikana. Silti ainoastaan 26% vastaajista sai kyberturvallisuuden nykytila-arviosta arvosanaksi keskitason tai yli keskitason ja 74% sai arvosanaksi huonon tai olemattoman. Tutkimuksessa lisäksi todettiin, että yritykset, jotka olivat hyvin varautuneet kyberriskeihin, oli myös ylipäätään parempi kokonaisriskikulttuuri. Eli kyberuhka, joka on laajempi kuin vain tietoturvaan kohdistuva uhka, tiedostetaan, mutta nykyisellään siihen ei vielä ole varauduttu. NIS-direktiivi pyrkii vaatimuksillaan kehittämään yritysten tietoturvan tasoa sekä uhkilta suojautumista ja niihin varautumista.

Kuten kaikki liiketoimintariskit, myös tietoriskit tulee tiedostaa yrityksen johdon tasolla. Tietoriskien kohdalla tulee myös muistaa, että kyse on liiketoiminnan ongelmasta, ei teknisestä ongelmasta. (Von Solms & Von Solms 2004)

3.3 Riskien sääntely lailla ja compliance-riski

Riskien pienentäminen lakikeinoin ei ole uusi asia. Suomessa on useita voimassaolevia lakeja, joiden tavoitteena on uhkien vähentäminen ja sitä kautta riskien pienentäminen, ja jotka asettavat yritysten toiminnalle velvoitteita ja rajoitteita. Tällaisia ovat esimerkiksi pelastuslaki (säädetty 2011) ja työturvallisuuslaki (säädetty 2002), jotka molemmat asettavat vaatimuksia yritykselle ja sen toiminnalle. Riskienhallintaosioita sisältyy myös mm. kemikaali-, liikenne-, palo- ja pelastustoimen, rakennus-, tuotevastuu-, väestönsuojelusekä ympäristölainsäädäntöön. Lainsäädännön ohella riskienhallintanormeja sisältyy myös esimerkiksi valtioneuvoston päätöksiin. (Suominen 2003) Riskien sääntely lailla sekä näiden lakien asettamat rajoitteet, ohjeet ja vaatimukset eivät siis ole NIS-direktiivin alaisille toimijoillekaan uusi asia. Eroja eri toimijoiden välillä toki on ja osa toiminnoista on vahvemmin säänneltyä, esimerkiksi rahoitusala, kuin toiset, esimerkiksi hakukoneet.

Yksi näkökulma lakien tuomiin uhkiin on Compliance-riski, joka voi olla hallinnollinen, oikeudellinen, taloudellinen tai maineriski, joka seuraa lakien, asetusten tai muiden hallinnollisten määräysten noudattamatta jättämisestä tai niiden rikkomisesta. (Sampo Group 2017) Compliance-riskillä voi olla myös vakavia seurauksia esimerkiksi niillä aloilla, joilla toiminta on vahvasti säänneltyä tai luvanvaraista, kuten pankkiala. Näissä tapauksissa noudattamatta jättäminen voi johtaa jopa toiminnan lakkauttamiseen. (Hopkin 2017) Toisaalta compliance on ongelmallinen esimerkiksi silloin, kun kyseessä on yritys, jonka taloudellinen tilanne on ennestään heikko. Tällainen yritys ei välttämättä kykene suoriutumaan uuden lain vaatimista investoinneista, vaikka ne eivät suoraan vaikuttaisi marginaalikustannuksiin. Tällöin yritykselle jää vain vähän vaihtoehtoja. Se voi joko lakkauttaa toimintansa, tai hyväksyä riskin, jolloin toiminta jatkuu, kunnes viranomainen puuttuu siihen.

Maine on yrityksen aineetonta pääomaa ja maineriskillä tarkoitetaan uhkaa siitä, että sidosryhmien mielikuva yrityksestä huononee tai yritykseen liitetään negatiivisia mielikuvia,

mitkä osaltaan voivat heikentää yrityksen asemaa ja liiketoimintamahdollisuuksia. (O'Callaghan 2007) Maineriskin vaikutuksia on vaikea mitata, sillä maineriskillä on myös useita välillisiä vaikutuksia ja toteutuessaan riskin haitat voivat vaihdella vähäisistä merkittäviin.(Bebbington ym. 2008) Maineriski tulisikin siis katsoa yrityksen omaisuuteen kohdistuvaksi, jostakin toisesta riskistä kumpuavaksi haitan mahdollisuudeksi. Se, että tämä toinen riski toteutuu, ei vielä automaattisesti tarkoita, että yrityksen maine kärsii, vaan kyseisen riskin toteutuminen luo maineriskin.

Mikäli lakia, joka pyrkii pienentämään tunnistettua uhkaa ei valvota, lain tavoitteen toteutuminen on epätodennäköistä. Osa yrityksistä voi päättää, että noudattamisen tuomat kustannukset tai riskit ovat liian suuret ja mikäli he peittelevät toimintaansa, ei kukaan saa koskaan selville, että lakia ei noudateta. (Laube & Böhme 2016) Tähän ongelmaan saatetaan törmätä esimerkiksi NIS-direktiivin ilmoitusvelvollisuuden kohdalla.

Compliance-riskin kohdalla ongelmana nähdään myös lakeihin liittyvä epämääräisyys. Siinä, missä lainsäätäjät haluavat riittävän joustavan lain, joka mukautuu toimintaympäristön muutokseen ja teknologian kehittymiseen, yrityksillä voi olla vaikeuksia tulkita lakia sen tarkoittamalla tavalla, ja näin yritys saattaa tietämättään syyllistyä lain rikkomiseen. (Hutter & Power 2000)

Vaikka sääntelyllä pyritään poistamaan uhkia lait ja asetukset voivat myös tuoda mukanaan ongelmia, kun asiaa tarkastellaan yritysten näkökulmasta. Laeista voi esimerkiksi tulla normitaso, jonka yläpuolelle ei enää haluta pyrkiä ylimääräisten kustannusten pelossa. Eli todetaan, että lain täyttävä taso on riittävä. Kyberturvallisuuden kohdalla lain asettamat vaatimukset ovat kokonaistasoon nähden nykyisellään matalia.

3.4 Riskienhallinta

Suomisen mukaan riskienhallinnalla tarkoitetaan *"prosessia, jonka avulla yritystä uhkaavia vaaroja voidaan torjua ja niistä aiheutuvia menetyksiä minimoida."*.(Suominen 2003) Riskienhallinnassa tavoitteena on tarjota yrityksen johdolle riittävästi tietoa, jotta he voivat tehdä päätöksiä tietoisina yrityksen kokonaisriskeistä ja siitä, millainen vaikutus tehtävällä päätöksellä on tähän riskien kokonaisuuteen. (Ilmonen ym. 2010). Koska yritykseen ja sen

liiketoimintaan kohdistuvat riskit muuttuvat ja kehittyvät jatkuvasti, myös riskienhallinnan täytyy olla jatkuva prosessi. Riskienhallintaa käytetään yleisesti lähestymistapana tiedon turvaamiseen ja sitä kautta tietoriskeihin. (Ilvonen 2013)

Jotta riskejä voidaan hallita, tulee ne ensin tunnistaa.(Suominen 2003) Harrington ja Niehaus (1999) kuvaavat riskienhallintaprosessin viisi vaiheisena seuraavasti:

- Merkittävien riskien tunnistaminen
- Vahinkojen todennäköisyyden ja vakavuuden arviointi
- Riskienhallintamenetelmien kehittäminen ja sopivien valitseminen
- Riskienhallintapäätökset
- Toteutettujen riskienhallintaratkaisujen arviointi

Riskienhallinnan avulla kyetään tekemään tietoisia valintoja riskien suhteen. Tarkoituksena ei ole välttää kaikkia riskejä, vaan tunnistaa riskit, tiedostaa niiden mahdolliset vaikutukset ja ymmärtää vaikutusten vakavuus. Suominen (2003) antaa riskin kokonaisuuden vaikutusten arvioinnille kaavan:

> *Riski = todennäköisyys x (henkilövahinkoarvio + omaisuusvahinkoarvioi + riskin yhteiskunnalliset vaikutukset)*

Myös ITIL on samoilla linjoilla Suomisen kanssa, sillä heidän mukaansa *”riskiä mitataan uhan todennäköisyydellä, omaisuuden haavoittuvuudella suhteessa tähän uhkaan ja vaikutuksella, joka sillä on toteutuessaan.”*. (ITIL 2011) Riskin todennäköisyyden ja vakavuuden arviointi on oleellinen osa riskienhallintaprosessia. Sillä ainoastaan sen avulla kyetään tunnistamaan liiketoimintaa uhkaavat kriittisimmät riskit ja valitsemaan asianmukaiset ja oikein suhteutetut toimenpiteet niiltä suojautumiseksi. Riskiä määritettäessä tulee kuitenkin muistaa, että vaikka riskilaskelma antaa yksiselitteisesti lukuarvon riskille, tulee muistaa, että luku perustuu arvioivan tahon näkemykseen riskistä, eivätkä näkemykset ole objektiivisia (Ilvonen 2013, 50-51).

Shameli-Sendin, Aghababaei-Barzegarin ja Cherietin mallin mukaan tunnistetulle riskille mahdolliset toimenpiteet voidaan jakaa seuraaviin: hyväksyminen, välttäminen, siirtäminen tai lieventäminen (Shameli-Sendi ym. n.d.). Eli kun riskit on tunnistettu, on yrityksen

johdon tehtävä päätös, pyrkiikö se poistamaan riskin vai hyväksyykö se riskin mahdollisuuden. Esimerkiksi sähköjen katkaiseminen rakennuksesta poistaisi sähköpalojen riskin, mutta tuskin olisi liiketoiminnan kannalta sovelias ratkaisu. Tulipalon riskiä voidaan kuitenkin lieventää automaattisella sammutusjärjestelmällä, mutta se ei tarkoita, etteikö tulipalo voisi silti syttyä.

Kun riskit on tunnistettu, arvioitu ja päätökset niihin suhtautumisesta tehty, on yrityksen tarpeen tehdä toimenpidesuunnitelma ainakin kriittisille riskeille. Suunnitelman tulee sisältää ainakin vastuuhenkilö ja aikataulu jokaiselle riskille.(Suominen 2003) Ilman toimenpidesuunnitelmaa on jälkikäteen vaikeaa arvioida, miten suunnitellut riskienhallinta ratkaisut on toteutettu ja kuinka ne ovat onnistuneet.

Riskienhallinnan on tarkoitus tukea yrityksen toimintaa. Jotta riskienhallintaprosessi täyttäisi sen perimmäisen tehtävänsä, eli yrityksen toiminnan tukemisen ja kehittämisen, se tulisi olla osa liiketoiminta prosesseja, ei niistä irrallinen prosessi. (Suominen 2003) Ollakseen toimiva osa liiketoimintaa, riskienhallinnan toiminnan tulisi tukeutua yrityksen strategiaan ja arvoihin, eikä siitä saa tehdä liian teoreettista tai monimutkaista (Ilmonen ym. 2010). Ilmonen et kumppaneiden (2010) mukaan hyvin toteutettua riskienhallintaa voidaan pitää, jopa yrityksen myyntivalttina. Usein riskienhallinnan taso tulee asiakkaille ilmi, kun tapahtuu jotain, mikä osoittaa, että riskienhallinta prosessit eivät olleet asianmukaisella tasolla. Tähän liittyykin myös vahvasti yrityksen maineriski. Esimerkiksi viimeaikoina valloille päässeet kiristyshaittaohjelmat, kuten WannaCry tai Petya, ovat aiheuttaneet ongelmia useille suurille toimijoille kuten Britannian kansallinen terveydenhuolto (Graham 2017) tai kansainvälinen lääkeyhtiö Merck. (Fortune 2017)

Riskienhallinnassa apuna voidaan käyttää myös erilaisia standardeja ja laatujärjestelmiä, kuten ISO 9000 laadunhallintastandardi tai ISO 27000 tietoturvallisuuden hallinta -standardi. Ne mahdollistavat kattavan ja järjestäytyneen lähestymisen riskeihin ja mahdollistavat riskienhallinnan toiminnan jatkuvuuden. Standardeja voidaan hyödyntää kokonaisuuksina tai yritykselle parhaiten soveltuvin osin. Standardeja usein myös hyödynnetään oman toiminnan laadun takeena ja osalla toimialoista saatetaan jopa vaatia standardien mukaista sertifiointia. (Ilmonen ym. 2010) Sertifikaatti osoittaa, että yritys on selvittänyt

laadukkaan toiminnan perusteet ja että arviointihetkellä ne ovat olleet kunnossa. Sertifikaatti täytyy uusia aika-ajoin, joten se myös edellyttää, että yrityksen toiminta pysyy vaaditulla tasolla. Sertifikaattien kohdalla tulee kuitenkin muistaa, että ne keskittyvät vain tiettyyn riskialueeseen eikä se kata koko riskikenttää.(Suominen 2003) Eli vaikka yrityksen toiminta täyttäisi ISO9000 laadunhallintastandardin vaatimukset, ei se kerro mitään yrityksen tietoturvan tasosta.

Riskejä ei esiinny vain yrityksen sisällä, vaan yritystä ympäröi aina erilaisten sidosryhmien ja riippuvuuksien vyyhti. Tämä sidosryhmien verkosto koostuu osista, jotka ovat toisiinsa joko tiiviisti tai löyhästi yhdistettyjä. Verkon osia voivat olla esimerkiksi alihankkijat, kuljetusliikkeet, asiakkaat, tavaran- tai palveluntoimittajat ja jälleenmyyjät.(Suominen 2003) Deloitten suuryrityksille tekemän kansainvälisen johtajatutkimuksen mukaan 74% vastanneista oli kohdannut ainakin yhden verkostosta johtuvan välikohtauksen viimeisen vuoden aikana, mutta ainoastaan 11% vastanneista oli täysin varautunut kolmansien osapuolten luomiin riskeihin.(Deloitte Touche Tohmatsu Limited 2017)

4 Tutkimuksen läpivienti

Tässä luvussa läpikäydään tutkimuksen teon vaiheet siten, että tutkimus on tarvittaessa toistettavissa. Luvussa kuvataan käytetyt tiedonhankinnan keinot ja vaiheet, perustellaan tehdyt valinnat, läpikäydään aineiston kuvaamisen tekniikat sekä aineiston analyysin tekniikat.

4.1 Tutkimuksen tavoitteet ja aineiston hankinta

Tutkimuksen tavoitteena oli selvittää, millaisia vaikutuksia NIS-direktiivillä on yritysten toimintaan riskinäkökulmasta tarkasteltuna. Tutkielman aineisto muodostuu NIS-direktiivistä ja Liikenne- ja viestintäministeriö NIS-direktiivin kansallista täytäntöönpanoa arvioivan työryhmän loppuraportista, jossa jo otettiin kantaa siihen, miten Suomessa mahdollisesti halutaan lähteä direktiiviä toteuttamaan. Itse direktiivin kansalliseen täytäntöönpanoon tähtäävää lakia ei ollut tutkimushetkellä vielä julkaistu, ei edes luonnosasteella, joten tätä osuutta ei pystytty tutkimuksessa hyödyntämään. Tämän voidaankin katsoa olevan yksi tutkimuksen rajoituksista, sillä tuloksia ei kyetä todentamaan ennen lain julkaisua ja täytäntöönpanoa. Tutkimuksessa ei käsitelty direktiivin niitä osia, joilla ei katsota olevan vaikutusta suoraan yritysten toimintaan. Tutkimukseen sisällytetyt osa-alueet on kuvattu liitteessä A. Tutkimus rajoittuu käytännössä Suomeen, mutta vaikutusten voi olettaa olevan samankaltaisia kaikissa maissa, sillä direktiivi myös rajoittaa tietyiltä osin kansallista toimeenpanoa.

Tutkimuksen kirjallisuuskatsaus vaiheessa pyrittiin tunnistamaan muita mahdollisia tutkimuksia, artikkeleita ja muita kirjallisia lähteitä, joista olisi apua tutkimuksen teossa tai joita olisi voinut käyttää lähteenä tutkimukseen. Luotettavaa aineistoa oli kuitenkin niukasti tarjolla, ja suurin osa saatavilla olevasta aineistosta oli kirjoitettu ennen direktiivin julkaisemista. Tutkimuksen tueksi päädyttiin valitsemaan myös kaksi muuta dokumenttia tutkittavan direktiivin lisäksi, sillä näiden katsottiin sisältävän tutkimuksen kannalta mahdollisesti oleellista tietoa. Dokumentit olivat Suomen tietoturvastrategia ja Liikenne- ja viestintäministeriön NIS-direktiivin kansallista täytäntöönpanoa pohtineen työryhmän loppuraportti.

Koska itse NIS-direktiivin tai jopa GDPR:n vaikutuksista Suomalaisiin yrityksiin ei ollut juurikaan tietoa saatavilla. Kirjallisuuskatsausta laajennettiin koskemaan myös aikaisemmin tehtyjä tutkimuksia muiden direktiivien vaikutuksista. Löydetyt tutkimukset kuitenkin keskittyivät yrityksien toimintaa rajoittaviin direktiiveihin, kuten rikkidirektiivi (Attila ym. 2012; Jurvelin 2014) tai muihin lain mukanaan tuomiin rajoituksiin kuten maarajoitukset (Koski ym. 2015).

4.2 Tutkimusmenetelmä

Vaikka kyseessä on hyvin vahvasti lakiin liittyvä aihe, analysoidaan sitä muilla kuin lakitieteellisillä keinoilla. Kuten Pitkänen väitöskirjassaan toteaa, lakitiede usein käyttää tutkimuksessaan oikeudenkäyntejä ja valmistelevia teoksia lähteinä ja johtaa teorioita niitä analysoimalla.(Pitkänen 2005, 56-57) Näiden metodien pohjalta on kuitenkin vaikea analysoida tulevaisuutta ja tilannetta, jossa oikeudenkäyntejä tai edes lopullista lakiehdotelmaa ei vielä ole saatavilla. Tästä syystä analyysi tehdäänkin muilla menetelmin.

Alasuutarin mukaan (2011, 82) ”*Jotta aineiston havainnot voidaan erottaa tutkimuksen tuloksista tarvitaan selkeä tutkimusmetodi”* eli menetelmä. Tässä tutkimuksessa käytetty tutkimusmenetelmä on laadullinen, millä tässä yhteydessä viitataan suoraan käännökseen termistä Qualitative Research. Alasuutarin mukaan laadullinen analyysi sisältää kaksi vaihetta: havaintojen pelkistäminen ja arvoituksen ratkaiseminen.(Alasuutari 2011, 39) Eli ensin pyritään luokittelemaan tai ryhmittelemään tehtyjä havaintoja yhtenevien tekijöiden mukaan, jonka jälkeen havaintojen perusteella pyritään ratkaisemaan asetettu tutkimuskysymys tai -ongelma.

Kuten Mäkelä (1990, 53) toteaa, on tärkeää suunnitella etukäteen, kuinka tutkimuksen aineisto saadaan hallittavaan muotoon prosessointia varten. Tutkimustulosten analysointi on aineistolähtöinen sisällönanalyysi. Tuomi & Sarajärven mukaan aineistolähtöisessä analyysissä tavoitteena on luoda tutkimusaineistosta teoreettinen kokonaisuus, jossa analysoitavat yksiköt valitaan tutkimuksen tarkoituksen mukaisesti ja jonka toteuttamiseen tai lopputulokseen aikaisemmilla teorioilla, havainnoilla tai tiedoilla ei pitäisi olla vaikutusta. (Tuomi & Sarajärvi 2009, 95) Sisällön analyysillä pyritään keräämään aineistoa johtopäätöksen

tekemiseksi ja kuten Tuomi ja Sarajärvi toteavat, tulee tutkimusta tehdessä olla tarkkana, ettei käytä analyysin tuloksia lopullisena tutkimustuloksena. (Tuomi & Sarajärvi 2009, 103-104)

Tutkittavan aineiston luonteesta ja laajuudesta, tai lähinnä rajoitetusta laajuudesta, johtuen määrällinen analyysi ei ole mahdollinen. Tuloksia ei myöskään kyetty vielä tutkimusvaiheessa todentamaan, sillä direktiiviin perustuvaa lakia ei ole julkaistu eikä näin ollen siitä myöskään ole oikeudellisia päätöksiä tai yritysten kokemuksia, joilla sen soveltamista voisi todentaa. Näistä syistä tutkimus perustuu puhtaasti yllä mainittuun aineistoon.

4.3 Tutkimuksen toteutustapa

Kerättyä ja luokiteltua ainestoa lähdettiin analysoimaan riskinäkökulmasta. Alasuutarin mukaan analyysissa tulee kiinnittää huomiota ainoastaan niihin seikkoihin, jotka ovat teoreettisen viitekehyksen ja tutkimuskysymyksen kannalta oleellisia.(Alasuutari 2011, 40) Edelleen riskinäkökulman avulla tietoja luokiteltiin riskiryhmiin kuten operatiivinen tai strateginen riski. Tällä saavutettiin Alasuutarin neuvojen mukainen havaintomäärien karsiminen ja mahdollistettiin havaintojen yhdistäminen. (Alasuutari 2011, 40)

Tutkimuksen ensimmäisessä vaiheessa käytiin läpi NIS-direktiivin sisältö ja luokiteltiin se niiltä osin, kun se oli merkityksellistä tutkimukselle. Samalla NIS-direktiivistä poimittiin ne osa-alueet, joilla on vaikutusta suoraan tai välillisesti yritysten toimintaan. Nämä osa-alueet lajiteltiin kolmeen kategoriaan: keskeisiä toimijoita koskevat, digitaalisia toimijoita koskevat ja muita toimijoita koskevat artiklat tai niiden osat. Yksi osa-alue saattaa koskea yhtä tai useampaa toimijaa. Direktiivistä on poimittu myös ne osa-alueet, jotka koskevat direktiivin taustoja, tavoitteita, sanktioita tai aikataulua, sillä nämä kaikki ovat oleellisia direktiivin vaikutuksia arvioitaessa.

Direktiiville tehdyssä luokittelussa käytettiin seuraavia tunnisteita:

DIGI - vaikuttaa digitaalisiin toimijoihin

KES - vaikuttaa keskeisiin toimijoihin

M - vaikuttaa muuhun toimijaan

AIK - sisältää aikatauluun liittyvää tietoa

KAN - vaikuttaa kansalliseen toteutukseen

TAV - kuvaa tavoitteita

TA - kuvaa taustaa

! - viittaus muualle, tarkasta

Tämän avulla direktiivistä saatiin kerättyä relevantti aineisto tutkimuksen seuraavaan osaan, joka jakautuu kolmeen: direktiivin vaikutuksen alaiset toimijat, direktiivin tuomat riskit yrityksille ja direktiivin tuomat riskienhallintakeinot.

Aineistoa täydennettiin vielä läpikäymällä huutomerkillä merkityt osa-alueet ja viittausten takana olevat lähteet. Nämä sisälsivät pääosin termien määrityksiä, jotka oli esitelty jossain toisessa EU:n direktiivissä, asetuksessa tai muussa aineistossa. Lisäksi läpikäytiin muu oleellinen materiaali: Suomen tietoturvallisuusstrategian sekä Verkko- ja tietoturvadirektiivi kansallista täytäntöönpanoa tukevan työryhmän loppuraportti. Näiden osalta sisältö jaoteltiin tarpeellisiin ja tarpeettomiin osioihin sen mukaan oliko osiolla merkitystä tutkittavaan aiheeseen vai ei.

Kertyneen aineiston pohjalta lähdettiin käsittelemään sitä, kehen direktiivi vaikuttaa. Tämä suoritettiin analysoimalla kerätyn aineiston sisältöä sekä ottamalla huomioon ja arvioimalla mahdollisia välillisiä vaikutuksia. Tutkimuksessa punnittiin myös kolmannen osapuolen riskiä, eli miten, jos mitenkään, direktiivi vaikuttaa kolmansiin osapuoliin, kuten laitetoimittajiin tai palveluntarjoajiin.

Kun aineistosta oli poimittu yrityksiin vaikuttavat tekijät, suoritettiin analyysin, missä arvioitiin, millaisia riskejä nämä vaikutukset mahdollisesti tuovat yrityksille. Riskejä arvioitaessa käytiin läpi kappaleessa 3 esitellyt riskit: strategiset riskit, taloudelliset riskit, operatiivinen riskit ja vahinkoriskit. Riskejä arvioitaessa direktiiviä käsiteltiin sekä kokonaisuutena, että sen osa-alueita läpikäytiin yksitellen. Tutkimuksen tämän vaiheen tulokset on kuvattu luvussa 5.1.

Tutkimuksen kolmannessa osiossa keskityttiin direktiivin niihin osiin, jotka kuvailevat riskienhallintaa tukevia mekanismeja. Riskienhallinta on direktiivin päätarkoitus, joten myös sitä tukevia elementtejä haluttiin tuoda tutkimuksessa esiin. Nämä pääkohdat sekä niiden merkitys yrityksille on kuvattu luvussa 5.2. Riskienhallinta osiossa aihetta tutkitaan laajemmin kuin mitä riski osiossa, sillä mukaan tulee myös ne riskit, mitä vastaan direktiivi pyrkii taistelemaan eli verkko- ja tietojärjestelmien turvallisuus.

Lopuksi tutkimuksen tulosten perusteella pyrittiin vastaamaan tutkimuskysymyksiin ja tuloksista tehtiin yhteenveto. Nämä löytyvät luvusta 6.

5 Tutkimustulokset

Tässä luvussa läpikäydään tutkimuksen tulokset ja annetaan alustavat vastaukset määriteltyihin tutkimuskysymyksiin.

5.1 NIS-direktiivi riskinäkökulmasta

Direktiivi pyrkii hallitsemaan verkko- ja tietojärjestelmäturvallisuuteen liittyviä riskejä valittujen toimijoiden osalta. Samalla se kuitenkin luo riskejä samaisille toimijoille. Riskejä on kahdenlaisia, sellaisia, jotka liittyvät direktiiviin kokonaisuutena, kuten compliance-riski ja sellaisia, jotka liittyvät direktiivin tiettyihin osiin. Tässä luvussa kerätään direktiiviin liittyvät tunnistetut riskit, jotta saadaan kokonaiskuva direktiivin sen alaisille toimijoille tuomista liiketoimintariskeistä.

Tunnistetut riskit on kerätty tauluihin samankaltaisuuksien mukaan. Riskien numerointi viittaa direktiivin artikloihin ja kohtiin. Kirjainmerkinnöillä erotellaan, mikäli samaan direktiivin kohtaan liittyy useampi riski. Riskit ja direktiivit sekä resitaalit, joihin ne viittaavat on tarkemmin listattu liitteessä E ’Direktiivin riskit kohdittain’.

Suurin tutkimuksessa havaittu direktiivin tuoma riski on compliance-riski. Lisäksi direktiivin todettiin tuovan sekä operatiivisia riskejä että strategia riskejä. Osa riskeistä liittyy direktiivin tiettyyn osaan ja osa direktiiviin kokonaisuudessa. Direktiivin tunnistettiin tuovan yritysten toiminnalle useita riskejä.

5.1.1 Compliance-riskit

Kuten kaikkeen lainsäädäntöön myös NIS-direktiiviin liittyy compliance-riski. On mahdollista, että yrityksen toiminta ei täytä lain vaatimuksia, jolloin toimintaa täytyy mukauttaa lakiin sen noudattamiseksi ja riskin minimoimiseksi. NIS-direktiivin tapauksessa tämä voi olla esimerkiksi yrityksen puutteelliset turvallisuusohjeet (15 artikla 1 kohta) tai yrityksessä vallitseva heikko turvallisuustaso. Toinen ääripää on lain tietoinen rikkominen. Tällöin hyväksytään compliance-riski osaksi liiketoiminnan kokonaisriskiä. NIS-direktiivi ei suosittele digitaalisille palvelun tarjoajille aktiivista seurantaa, vaan seuranta perustuu ilmoi-

tuksiin ja epäilyihin rikkomuksista. Tämä pienentää näiden yrityksen riskiä ja on mahdollista, että yritys jää odottamaan viranomaisten kantaa korjausten tarpeesta. Asioiden päivittäminen luo kustannuksia ja liiketoiminnassa ylimääräistä rahaa ei ole, sillä yritysten perimmäinen tavoite on tuottaa voittoa omistajilleen. Näiden kahden ääripään välille jää alue, johon sijoittuvat yritykset, jotka haluavat noudattaa lakia mutta eivät välttämättä täysin ymmärrä sen sisältöä tai tulkitsevat sisältöä eri tavalla kuin viranomaiset ovat tarkoittaneet.

NIS-direktiivissäkin on useita alueita, joissa jätetään tulkitsemisvaraa (kts. Taulu 1. Direktiivin summittaiset määritelmät). Esimerkiksi 14 artiklan 1 kohdan käyttämät termit ”asianmukaiset ja oikeasuhteiset” tai 16 artiklan 3 kohdan ”merkittävä vaikutus” jättävät tulkitsijalle suuren liikkumavaran. Compliance-riski kumpuaakin siitä, että yritys ei voi olla varma onko heidän tulkintansa laista, sen vaatimuksista ja rangaistuksista täysin oikea, joten väärinymmärryksen mahdollisuus tulisi ottaa huomioon myös silloin kun yritys omasta mielestään täyttää vaatimukset.

(5.2.) Direktiivissä annetut määritelmät ovat laajoja ja tulkinnanvaraisia, mikä vaikeuttaa niiden tulkintaa ja kasvattaa compliance-riskiä. Kansallisella täytäntöönpanolla ja sen yksiselitteisyydellä on suuri merkitys riskin realisoitumiselle.

(6.1.a) Direktiivin antamat määritelmät ovat summittaisia eivätkä anna yksiselitteistä määritystä sille, miten merkittävä haitallinen poikkeama tunnistetaan. Tämä kasvattaa compliance-riskiä. Kansallisella toteutuksella on suuri merkitys siihen, miten riski realisoituu.

(14.1.a) ’Asianmukaiset ja oikeasuhtaiset riskienhallinta toimenpiteet’ on laaja käsite ja sisältää riskin, että yritys ei tunnista viranomaisen vaatimaa tasoa ja joko yli-investoija tai ali-investoida.

(14.1.b) Riski, että viranomaisella ja elinkeinonharjoittajalla on eri näkemys siitä, mikä on uusimman tekniikan taso. Tämä voi vaihdella suuresti, sillä kaikki kaupalliset ohjelmistot tai laitteistot eivät ole sopivia jokaiselle toimialalle käytettäviksi tai eivät kustannuksiltaan ole mahdollisia hankkia.

(14.4.) (16.3.) Ilmoitusvelvollisuuden määritelmä on direktiivissä hyvin häilyvä ja vaikeas-

ti tulkittava. Riski, että yritys jättää ilmoituksen tekemättä, koska se tulkitsee määritelmää eri tavalla kuin lain laatija. (16.1.) Direktiivi asettaa vaatimuksia digitaalisen palvelun tarjoajien toiminnalle, mutta koska vaatimukset eivät ole selkeästi määriteltyjä (”oikeasuhtaiset tekniset ja organisatoriset toimenpiteet”) niitä on vaikea noudattaa, mikä kasvattaa compliance-riskiä. (17.1.) Compliance-riski. Mikäli yrityksen toiminnot eivät vastaa viranomaisen tulkintaa kyseisestä pykälästä kohtaavat he kurinpitomenettelyn.

Taulu 1. Direktiivin summittaiset määritelmät

Direktiivi luo yritykselle compliance-riskin osana myös maineriskin, sillä se voi vaatia yritystä tiedottamaan niiden kohtaamista tietoturvapoikkeamista (Taulu 2. Maineriski). Tiedottamisvelvollisuus luo maineriskin direktiivin alaisille toimijoille kahta eri kautta. Direktiivin vaatimukset voivat johtaa suoraan maineriskiin, mikäli yritys joutuu viranomaisten vaatimuksesta tiedottamaan kohtaamastaan turvallisuuspoikkeamasta julkisuuteen. Toisaalta, mikäli tiedottamisen tekee virallinen taho ilman, että se yksilöi poikkeaman kohteena ollutta toimijaa, saattaa mainehaitta kohdistua koko toimialaan, vaikka kyseessä olisikin yksittäisen toimijan leväperäinen toiminta. Maineriskiä kasvattaa myös se, että direktiivi velvoittaa jäsenvaltioita jakamaan tietoa niiden alueella kohdatuista poikkeamista toisille jäsenmaille. Kun tietoa jaetaan tahojen kesken, se lisää riskiä tiedon vuotamisesta ulkopuolisille ja sitä kautta tuo riskin yrityksen maineelle.

(14.6.) (16.7.) Tiedottamisvelvollisuus luo yritykselle maineriskin. Riski, on myös niissä tilanteissa, jolloin poikkeama ei kohdistu yritykseen itseensä, vaan johonkin toiseen saman alan toimijaan, mutta julkisuuteen kerrotaan vain toimiala, ei toimijaa. (16.6.) (17.3.) Kun tietoja jaetaan uusille tahoille, lisää se riskiä tiedon joutumisesta vääriin käsiin tai julkisuuteen, joko tahallisesti tai vahingossa. Riippuen tiedon laadusta voi se aiheuttaa haittaa joko maineelle tai liiketoiminnalle.

Taulu 2. Maineriski

NIS-direktiivi tuo mukanaan myös useita muita compliance-riskejä (Taulu 3. Muut compliance-riskit). Taloudellinen compliance-riski kumpuaa direktiivin yrityksille määrittämistä sanktioista. Mikäli yrityksen katsotaan rikkovan direktiiviä, voi siitä seurata oikeudellisia tai hallinnollisia menettelyjä ja sitä kautta myös merkittävää taloudellista haittaa yrityksen toiminnalle tai haittaa yrityksen maineelle. Direktiivin rikkominen voi johtaa myös Sanktioiden suuruutta ei vielä ole määritelty, mutta ”*tehokkaita, oikeasuhteisia ja varoittavia*” (NIS-direktiivin 21 artikla). Voidaan myös olettaa, että EU valvoo direktiivin sanktioiden samansuuntaisuutta EU-maiden välillä.

(6.1.b) Mikäli yritys kasvaa nopeasti saattaa se täyttää nämä asiat, vaikka muuten ei kuuluisikaan direktiivin piriin. Sama saattaa tapahtua, mikäli ala on kausiluontoista tai muuten voimakkaasti vaihtelevaa. Riski, että yritykset eivät tunnista kuuluvansa direktiivin piiriin.

(6.1.c) Mikäli määritys tulee voimassaolevien lakien alakohdaksi ja virastojen päätettäväksi (työryhmän ehdotus), voi olla edelleen vaikea arvioida onko yritys lain piirissä, ellei sitä selkeästi määritellä laissa. Eli jos osa lain tai viraston valvonnan alle kuuluvista on direktiivin piirissä ja osa ei.

(14.2.) (16.2.) Jotta poikkeamien vaikutuksia kyetään minimoimaan, on mahdolliset poikkeamat ja niiden mahdolliset vaikutukset ensin tunnistettava. Riski, että yritykset eivät tunnista poikkeamia ja yli- tai ali-investoivat niiden ehkäisemiseen.

(14.3.) (16.3.) Riski, että yritykset käyttävät enemmän aikaa ilmoituksen tekemiseen ja sitä kautta itse poikkeaman korjaaminen viivästyy. Pelkästään poikkeaman laajuuden analysointiin ja ilmoitusvelvollisuuden täyttymisen arviointiin voi kulua tarpeettoman paljon aikaa, mikäli ongelma ei ole etukäteen tunnettu. Aiheettoman viivytyksen määritelmä on epätarkka ja monitulkintainen, mikä kasvattaa compliance-riskiä.

(18.2-3.) Myös EU:n ulkopuolisten digitaalisten palvelun tarjoajien täytyy arvioida kuulumisensa direktiivin piiriin, mikäli heillä on asiakkaita EU:n alueella. Direktiivi luo heille compliance-riskin.

(21) Sanktiot ovat osa compliance-riskiä. Mikäli lain noudattamatta jättämisellä ei ole mi-

tään seuraamuksia, siihen liittyvä riski on myöskin vähäinen.

Taulu 3. Muut compliance-riskit

Compliance-riskiä voi ehkäistä NIS-direktiivinkin mainitsemilla standardeilla. Näin toimintojen oikeellisuus ei jää pelkästään yrityksen itsensä arvioitavaksi ja puutteet on helpompi havaita ja niihin puuttua. Toinen vaihtoehto on käyttää sisäisiä tarkastajia ilman erillistä sertifiointia. Sisäisessä tarkastuksessa prosessi on kevyempi, mutta siitä ei saa todistukseksi sertifikaattia, jota voisi käyttää todisteena yrityksen ulkopuolelle. Compliance-riski vähenee sitä mukaa kun laki tulee voimaan ja sen noudattamisesta saadaan viranomaispäätöksiä tai oikeuden päätöksiä.

5.1.2 Strategiset riskit

Direktiiviin liittyy myös strategisia riskejä. Strategiset riskit liittyvät esimerkiksi yrityksen kasvusuunnitelmiin, verkko- ja tietoturvallisuuden kehittymiseen ja alueen toiminnan kehittämiseen yrityksessä ja yrityksen maineeseen. Strategista riskiä voidaan vähentää tunnistamalla direktiivin vaatimukset ja varautumalla niihin ennakolta. Myös compliance-riskin pienentäminen pienentää yritykseen kohdistuvia strategisia riskejä, sillä suurin osan riskin realisoitumisesta vaatii compliance-riskin toteutumista.

NIS-direktiivi koskee vain tietyn suuruisia digitaalisia toimijoita ja vain tietyillä toimialoilla toimivia keskeisiä toimijoita (Taulu 4. Yleiset strategiset riskit). NIS-direktiivi tuokin strategisen riskin digitaalisille toimijoille, jotka suunnittelevat liiketoiminnan kasvattamista, ja yrityksille, jotka suunnittelevat toimintojensa laajentamista sellaisille toimialoille, jotka katsotaan keskeisiksi direktiivin määritelmässä. Esimerkiksi, mikäli vakuutusyhtiö suunnittelee sairaalan avaamista. Sairaalat ovat selkeästi direktiivin alaisia toimijoita, mutta vakuutusyhtiöt eivät.

Yrityksen liiketoimintaan voivat vaikuttaa myös NIS-direktiivin noudattamiseksi annetut viranomaismääräykset (Taulu 4. Yleiset strategiset riskit). Mikäli viranomainen katsoo, että yrityksen toiminta ei nykyisellään noudata direktiivin vaatimuksia, voi se langettaa yrityksille lisämääräyksiä. Direktiivi ei myöskään nykyisellään velvoita digitaalisia toimi-

joita ilmoittamaan poikkeamista keskeisille toimijoille, joten keskeisten toimijoiden on itse huolehdittava ilmoitusten toteutumisesta sopimuksellisesti digitaalisten toimijoiden kanssa. Ilmoituksesta sopiminen on olennaista, jotta keskeiset toimijat voivat täyttää direktiivin heille asettaman ilmoitusvelvollisuuden.

(6.1.b) Mikäli yritys kasvaa nopeasti saattaa se täyttää nämä asiat, vaikka muuten ei kuuluisikaan direktiivin piriin. Sama saattaa tapahtua, mikäli ala on kausiluontoista tai muuten voimakkaasti vaihtelevaa. Riski, että yritykset eivät tunnista kuuluvansa direktiivin piiriin.
(15.3.) Viranomaisten antamat sitovat ohjeet voivat luoda riskin yrityksen liiketoiminnalle, mikäli ne vaativat suuria muutoksia sen keskeisiin toimintoihin tai nykyiseen toimintamalliin. Lisäksi tällaiset määräykset tulevat usein julkisuuteen ja sitä kautta aiheuttavat maineriskin.
(16.5.b) Direktiivi ei itsessään velvoita digitaalisen palvelun tarjoajaa tiedottamaan poikkeamasta keskeisten palvelujen tarjoajalle, joten tästä täytyy erikseen sopimuksellisesti sopia.

Taulu 4. Yleiset strategiset riskit

Direktiivin jättää laajan tulkitsemisvaran sille, mikä on se taso, millä toimijoiden oletetaan suorittavan toimenpiteitä riskienvälttämiseksi ja pienentämiseksi (Taulu 5. Yrityksen toimintojen mukauttaminen). Tämä voi johtaa joko siihen, että yritykset eivät tee toimenpiteitä ennen kuin viranomaiskanta selkiytyy, eivätkä näin investoi riittävällä tasolla verkko- ja tietoturvallisuuteen. Toisena ääripäänä on mahdollista, että yritys käyttää liikaa resursseja verkko- ja tietoturvallisuuden kehittämiseen. Tämän rahan voidaan olettaa olevan pois muista oleellisista investoinneista. Direktiivi myös vertaa yritysten tietoturvallisuuden tasoa uusimman tekniikan tarjoamiin mahdollisuuksiin. Uusin tekniikka ei kuitenkaan välttämättä ole soveltuvaa tai yhteensopivaa kaikilla liiketoiminta-alueilla tai toimialoilla. Tällainen vaatimus saattaa johtaa yrityksen turhiin investointeihin ja toimimattomiin ratkaisuihin, jotka eivät todellisuudessa paranna direktiivin tavoitteiden mukaisesti verkko- tai tietoturvallisuutta. Määritelmän epäselvyys saattaa helposti johtaa myös tilanteeseen, missä päätetään, että on parempi olla tekemättä mitään, kun vaatimusten taso on epäselvä.

(14.1.a) ’Asianmukaiset ja oikeasuhtaiset riskienhallinta toimenpiteet’ on laaja käsite ja sisältää riskin, että yritys ei tunnista viranomaisen vaatimaa tasoa ja joko yli-investoi tai ali-investoi. (14.1.b) Riski, että viranomaisella ja elinkeinonharjoittajalla on eri näkemys siitä, mikä on uusimman tekniikan taso. Tämä voi vaihdella suuresti, sillä kaikki kaupalliset ohjelmistot tai laitteistot eivät ole sopivia jokaiselle toimialalle käytettäviksi tai eivät kustannuksiltaan ole mahdollisia hankkia.

Taulu 5. Yrityksen toimintojen mukauttaminen

5.1.3 Operatiiviset riskit

Kolmas direktiiviin liittyvä riskikategoria on operatiiviset riskit. Operatiivisiin riskeihin kuuluu direktiivin tuoma riski yrityksen liikesalaisuuksien pääsystä vääriin käsiin samalla, kun tietoa jaetaan toimijoiden kesken poikkeamista (Taulu 6. Tietovuodot). Vaikka direktiivissä sanotaan, että yrityssalaisuuksia tai muita liiketoimintaa riskeeraavia tietoja ei saa jakaa, jää kuitenkin kyseenalaiseksi tunnistavatko viranomaiset sen, mikä on liikesalaisuuteen kuuluvat tietoa eri toimialoilla ja mikä on jaettavissa olevaa tietoa.

(1.5.a) Riski, että yrityksen liikesalaisuuksia pääsee vääriin käsiin, sillä direktiivin nojalla myös liikesalaisuuksien alainen tieto voidaan jakaa muille jäsenmaille, mikäli sen katsotaan olevan direktiivin nojalla tarpeellista. (1.5.b) Vaikka tiedonjaossa painotetaan luottamuksellisen tiedon jakamisen haitan arviointia yritykselle, on riski, että viranomainen ei tunnista eri alojen keskeisiä liikesalaisuuksien alaisia toimintoja ja tietoja sekä niiden kriittisyyttä, ja näin ollen aliarvioi tietojen jakamisesta yrityksille aiheutuvan haitan. (1.5.c) Riski, että luottamuksellista tietoa esim. liikesalaisuuksia päätyy vääriin käsiin.

Taulu 6. Tietovuodot

Kun verkko- ja tietojärjestelmäturvallisuuteen liittyvät vaatimukset lisääntyvät, on mahdollista, että myös henkilöstöön tarvitaan lisää osaajia tälle alalle (Taulu 7. Pula osaajista). Mikäli direktiivi lisää osaajien tarvetta, voidaan sen katsoa lisäävän sitä huomattavasti, sillä direktiivi implementoidaan koko EU:n alueella samaan aikaan. Osaajista on jo nykyisellään pulaa (Center for Strategic and International Studies 2016), ja mikäli yrityksellä on puutteellinen substanssiosaaminen direktiivin kattamalla alueella, voi se hankaloittaa yrityksen direktiivin mukaista toimintaa tai yrityksen toiminnan mukauttamista direktiivin vaatimuksiin nähden.

(14.1.c) Mikäli organisatoriset toimenpiteet edellyttävät esimerkiksi verkko- ja tietojärjestelmäturvallisuuden osaajaa yritykseen, tulee osaajista olemaan pulaa, sillä jo nyt kysyntää on enemmän kuin tarjontaa kyberturvallisuuden osaajista. (Center for Strategic and International Studies 2016)

Taulu 7. Pula osaajista

Mikäli yrityksessä ei ole olemassa olevaa toimintakulttuuria verkko- ja tietoturvapoikkeamien raportoinnille tai toimintaprosessien dokumentoinnille, on riski, että direktiivin vaatimat turvallisuusohjeet laaditaan ainoastaan direktiiviä varten, eikä niitä todellisuudessa noudateta (Taulu 8. Turvallisuusohjeiden luonti). Mikäli ohjeet luodaan vain direktiivin vaatimusten täyttämiseksi, on erittäin todennäköistä, että ne eivät sovellu yrityksen liiketoiminnan tarpeisiin, eivätkä näin vastaa yrityksen kohtaamaan todelliseen uhkakuvaan.(Von Solms & Von Solms 2004) Tällöin direktiiviin riskienhallintanäkökulma ei toteudu suunnitellulla tavalla.

(15.2.) (17.2.) Riski, että turvallisuusohjeet luodaan ainoastaan sen takia, että direktiivi vaatii, eivätkä ne näin vastaa yrityksen todellisia tarpeita.

Taulu 8. Turvallisuusohjeiden luonti

Operatiivisten riskien näkökulmasta direktiiviin liittyy myös riski päällekkäisestä ilmoitusvelvollisuudesta, mikä tarkoittaa, että yritys joutuu käyttämään enemmän aikaa ilmoitusten

tekemiseen, mikä saattaa pahimmillaan olla pois itse poikkeaman korjaamisesta (Taulu 9. Päällekkäinen ilmoitusvelvollisuus). Päällekkäinen ilmoitusvelvollisuus voi sattua niin GDPR:n kanssa kuin sekä digitaalisen, että keskeisen toimijan joutuessa tekemään ilmoituksen samasta poikkeamasta.

(15.4.) Mikäli NIS-direktiivin toimivaltaisen viranomaisen ja tietosuojaviranomaisen yhteistyö ei toimi, aiheutuu yritykselle tuplatyö ilmoittamisvelvollisuuden osalta, mikäli poikkeama vaarantaa henkilötietoja.
(16.5.a) Mahdollinen päällekkäinen ilmoitusvelvollisuus, sillä digitaalisen palvelun tarjoajalla on ilmoitusvelvollisuus samasta poikkeamasta, mikäli se on heidän kannaltaan merkittävä ja tämän mukaisesti myös keskeisten palvelujen tarjoajalle syntyy ilmoitusvelvollisuus samaisesta poikkeamasta. Riski, että aika menee ilmoitusvelvollisuuksien hoitamiseen poikkeaman korjaamisen sijaan.

Taulu 9. Päällekkäinen ilmoitusvelvollisuus

5.1.4 Taloudelliset riskit ja vahinkoriskit

Direktiivi ei tuo suoria taloudellisia riskejä, mutta osana compliance-riskiä tulee mahdollisten sanktioiden mukanaan tuoma taloudellinen riski. Tässä tapauksessa taloudellisen riskin toteutuminen kuitenkin vaatii compliance-riskin toteutumista, joten sitä ei näissä tuloksissa katsota omaksi riskialueekseen. Toinen ilmoitusvelvollisuuden mukanaan tuoma välillinen taloudellinen riski voidaan katsoa olevan yksityishenkilöiden kuten asiakkaiden tuomat tappiot (Laube & Böhme 2016). Mikäli yksityishenkilöt kokevat, että heille on aiheutunut haittaa yrityksen turvallisuusloukkauksesta, mikäli esimerkiksi sen seurauksena heidän henkilötietonsa ovat vuotaneet. Tämäkään ei kuitenkaan ole suora taloudellinen riski yritykselle vaan enneminkin osa operatiivisia riskejä, jolla on taloudellinen vaikutus.

Tietoturvapoikkeama voi johtua henkilön vahingossa suorittamasta toimenpiteestä, esimerkiksi joku saattaa irrottaa väärän piuhan palvelinkeskuksessa, jolloin yrityksen järjestelmät lakkaavat toimimasta. Ei kuitenkaan voida katsoa, että direktiivi sinänsä toisi uusia vahinkoriskejä. Korkeintaan sen voidaan katsoa lisäävän vahinkoriskin vaikutusta siinä tapauk-

sessa, että yrityksen katsotaan rikkovan direktiivin asettamia velvoitteita tai että yritys joutuu tekemään direktiivin seurauksena lisätoimenpiteitä aikaisempaan nähden vahingon sattuessa. Tämä voisi toteutua esimerkiksi ilmoitusvelvollisuuden muodossa. Yrityksen noudattaessa direktiivin vaatimuksia ja kehittäessään tietoturvaansa direktiivin vaatimusten mukaan, vahinko riskin voidaan joissakin olosuhteissa katsoa jopa pienentyvän. Tätä päätelmää ei voida kuitenkaan yksiselitteisesti suoraan tehdä, sillä tietoturvapoikkeamiin vaikuttavat myös ulkoiset tekijät.

5.2 NIS-direktiivin vaikutukset riskienhallintaan

Jotta NIS-direktiivin vaikutuksia voidaan kokonaisvaltaisesti vertailla, voidaan todeta, että sillä on vaikutuksia yrityksen riskienhallintaa. Direktiivin tavoitteissakin mainitaan, että direktiivin avulla pyritään vähentämään verkko- ja tietoturvallisuuspoikkeamien, eli tiettyjen toimintaan liittyvien riskien, toteutumista.

Direktiivin mukaan, vastuu turvallisuuden rakentamisesta ja ylläpitämisestä jää suurilta osin direktiivin alaisten toimijoiden itsensä vastuulle (resitaali 44). Direktiivissä kehotetaan jäsenmaita sääntelyvaatimusten ja vapaaehtoisten käytäntöjen avulla tukemaan toimijoiden riskienhallintakulttuuria, jonka osana yritykset toteuttaisivat riskiarviointeja ja käynnistäisivät asianmukaisia toimenpiteitä tunnistettujen turvallisuusuhkien torjumiseen (resitaali 4; resitaali 44). Liikenne- ja viestintäministeriön työryhmän loppuraportissa (2017) todetaankin, että direktiivin käyttöönotossa tulisi huomioida yritysten mahdollisuus sisällyttää direktiivin vaatimat toimet osaksi liiketoimintariskiensä hallintaa, jotta toimenpiteiden hallinnolliset kulut tai vaatimat resurssit eivät kasvaisi liian suuriksi. Direktiivin implementoinnin onnistuessa, yritys voisi saada tukea riskiensä hallintaan ilman, että se joutuisi tekemään merkittäviä muutoksia nykyisiin riskienhallintakäytänteisiinsä.

Yksi direktiivissä mainituista tukitoimista on toimijoiden kannustaminen standardien käyttöönottoon (19 artikla 1 kohta), ja sitä kautta itseohjaukseen, jotta verkko- ja tietojärjestelmiin kohdistuvien poikkeamien vaikutuksen vähenevät. Samalla tavoitteena on myös vähentää poikkeamien toteutumista. Direktiivi kehottaa myös kansainväliseen yhteistyöhön standardien ja tiedonvaihdon kehittämiseen (resitaali 43). Jäsenvaltioita jopa kehotetaan

edistämään tiettyjen turvallisuusstandardien käyttöä ja niiden mukaista toimintaa (resitaali 66). Liikenne- ja viestintäministeriön työryhmän loppuraportissa strategiseksi tavoitteeksi on mainittu, että Suomessa ja EU:ssa toivotaan standardien helpottavan tietoturvasta huolehtivien sopimuskumppanien valintaa. (Liikenne- ja viestintäministeriö 2017) Mikäli viranomainen kykenee nimeämään standardeja, joiden mukaan toimittaessa yritys täyttää direktiivin vaatimukset, vähentää se direktiivin tuomaa compliance-riskiä. Samalla yrityksen on mahdollista vähentää sen verkko- ja tietoturvallisuuteen kohdistuvaa vahinkoriskiä.

Direktiivi asettaa vaatimuksen, että sen piiriin kuuluvilla yrityksillä tulee olla turvallisuussuunnitelmat. Jotta turvallisuussuunnitelma on tehokas, tulee sen perustua tunnistettuihin riskeihin. (Von Solms & Von Solms 2004) Yrityksen onkin siis ensin kartoitettava ja arvioitava turvallisuusuhkaympäristönsä ennen suunnitelman luomista, jotta direktiivin oletuksenmukainen riskienhallinta toteutuisi. Kuten direktiivissäkin todetaan riksienhallintatoimenpiteet koostuvat mahdollisten poikkeamien riskien tunnistamisesta, etsimisestä, havaitsemisesta ja käsittelystä, millä pyritään lieventämään poikkeamien haitallistavaikutusta ja siten riskejä (resitaali 46). Turvallisuutta ja mahdollisia poikkeamia mietittäessä tulee huomioida tiedon tallennus, siirtäminen ja käsittely (resitaali 46).

Direktiivin nojalla jäsenvaltioiden tulee jakaa tietoja niiden alueella tapahtuneista tietoturvapoikkeamista sisältäen tietoja poikkeamien määrästä, kestosta ja vakavuudesta (resitaali 33). Direktiivi ei ota kantaa siihen, saako tai tuleeko tietoja jakaa toimijoille, mutta mikäli tiedottamiseen päädytään mahdollistaa se toimijoiden paremman ymmärryksen vallitsevasta uhkakuvasta ja sitä kautta paremman varautumisen näihin uhkiin. Täytyy kuitenkin muistaa, että tästä saadaan etua vain, mikäli toimijat tekevät ilmoitukset kansallisille yhteyspisteille direktiivin vaatimusten mukaan, mikäli tieto kulkee yhteyspisteiden välillä ja mikäli yhteyspiste päättää jakaa tiedon myös toimijoille. Direktiivi kehottaa myös toimijoita suoraan keskinäiseen yhteistyöhön ja kehottaa jäsenmaita tukemaan tällaista yhteistyötä esimerkiksi kutsumalla sidosryhmiä keskusteluihin (resitaali 35). Tällainen suora yhteistyö mahdollistaa nykyistä tehokkaamman parhaiden käytäntöjen jakamisen toimijoiden kesken.

Direktiivi kehottaa jäsenvaltioita tukemaan toimijoita rikosilmoituksen tekemisessä, mikäli se katsoo, että poikkeama on aiheutunut vakavaan rikollisen toiminnan seurauksena. Mikäli toimivaltaisen viranomaisen ja lainvalvontaviranomaisen välinen yhteistyö toimii hyvin, seuraa siitä etua toimijalle, sillä parhaimmassa tapauksessa päällekkäisten ilmoitusten sijaan, toimija voisi hoitaa molemmat toimenpiteet yhdellä ilmoituksella ja viranomaiset voivat keskenään hoitaa tarvittavan tiedonjaon (resitaali 62). Mikäli kyberrikoksista tehtäisiin enemmän rikosilmoituksia, mahdollistaisi se lainvalvontaviranomaisen puuttumisen, vaikkakin kyber rikokset selviävät vain harvoin. NCA:n raportin mukaan Britanniassa kyberrikokset ohittivat tavalliset rikokset jo vuonna 2015. Samalla yksi suurimmista kyberrikoksiin puuttumisen ongelmista on se, etteivät rikoksen kohteet raportoi rikoksia. (NCA Strategic Cyber Industry Group 2016) Eli raportoinnin kehittymisen voidaan katsoa olevan olennainen tekijä kyberrikosten torjunnassa.

Direktiivin tuomia riskejä arvioitaessa yhdeksi riskiksi nostettiin tietoturvaosaajien saatavuus. Liikenne- ja viestintäministeriön työryhmän loppuraportissa ongelmaan on tartuttu ja direktiiviin liittyvistä tavoitteeksi on nostettu tietoturvaan liittyvän osaamisen kartoitus ja osaajien saatavuuden parantaminen. Tavoitteissa lisäksi mainitaan, että halutaan varmistaa, että tietoturvakoulutukseen olisi saatavilla riittävä määrä resursseja.(Liikenne- ja viestintäministeriö 2017) Strategia ei kuitenkaan selvennetä, millaista koulutusta tällä tarkoitetaan, eli kyseessä voi olla kokonaisvaltainen tietoturvatietoisuuden lisääminen tai tietoturvaan erikoistuneiden asiantuntijoiden kouluttaminen.

Direktiivin vaikutukset yritysten riskienhallintaan ovat rajalliset. Direktiivi ei suoraan anna riskienhallinta keinoja yritysten käytettäväksi, mutta direktiivi kuitenkin tuo mukanaan useita välillisiä keinoja yritysten riskienhallinnan parantamiseen. Direktiivin tuomiksi pääriskienhallintakeinoiksi tunnistettiin tiedonjakamisen kehittäminen, standardien kehittäminen, tietoturvaan liittyvän riskienhallinnan kehittäminen mm. turvallisuussuunnitelman muodossa sekä rikosilmoitusten tekemisen lisääntyminen. Jotta riskienhallinta keinot toteutuvat on direktiivin mukaisen toiminnan toteuduttava ja kansallisen lainsäädännön onnistuttava. Lisäksi kansallisen täytäntöönpanon tulisi tukea toimijoita direktiivin ehdottamilla tavoilla.

5.3 Direktiivin vaikutuksenalaiset toimijat

Direktiivissä todetaan, että se ulottuu suoraan keskeisten palvelujen tarjoajiin ja digitaalisiin palvelun tarjoajiin. Lisäksi voidaan katsoa, että sen ulottuvuus tulee kattamaan myös kolmansia osapuolia kuten ohjelmistokehittäjiä tai järjestelmätoimittajia. Tässä kappaleessa käsitellään tarkemmin sitä, ketä direktiivi velvoittaa ja ketkä kuuluvat sen piiriin. Jotta vaikutuksia ja niiden tuomia riskejä voidaan arvioida kattavasti, tulee myös ymmärtää, ketä vaikutusten piiriin kuuluu.

Keskeisen palvelujen tarjoajille on direktiivissä eniten suoraan asetettuja velvoitteita. Se onko toimija keskeisen palvelujen tarjoaja, pitäisi olla helposti selvitettävissä, sillä jäsenmaiden on yksiselitteisesti joko listattava keskeisten palvelujen tarjoajat tai määritettävä määrälliset kriteerit sille, miten keskeinen palvelujen tarjoaja määritetään. Elinkeinonharjoittajan tulee tarkastaa määritelmä siinä maassa, missä sillä on toimintaa oikeushenkilönä. Tämä voi siis kattaa yhden tai useamman maan, mikäli yrityksellä on esimerkiksi tytäryhtiöitä useissa EU-maissa.

Jäsenvaltioiden tekemän määrityksen perusteella elinkeinonharjoittajalle pitäisi olla yksiselitteistä ja selkeää, kuuluuko hän keskeisten palvelujen tarjoajien joukkoon vai ei. Keskeisten palvelun tarjoajien tulisi myös huomioida lista niistä palveluista, jotka katsotaan keskeisiksi, sillä vaikka he ovat keskeisten palvelujen tarjoaja kaikki heidän suorittamansa toiminnot eivät välttämättä ole direktiivin mukaisia keskeisiä palveluja, ja tällaisten toimien osalta direktiivi ei ole velvoittava. Esimerkiksi sähköyhtiön tuskin oletetaan tekevän ilmoitusta, mikäli heidän verkkosivustoillaan toimiva etuohjelmaosio on hetkellisesti poissa toiminnasta palvelinrikon vuoksi, siitäkin huolimatta, että tämä vaikuttaisi suurimpaan osaan yhtiön asiakkaista. Jos sama palvelin kuitenkin ohjaa myös sähkön tuotantoa, voi ilmoitusvelvollisuus täyttyä. Huomioitavaa kuitenkin on, että vaikka direktiivi ei ole velvoittava, saattaa kansallinen laki asettaa ilmoitusvelvollisuuden myös sellaisten palveluiden osalta, jotka eivät ole keskeisiä, mutta joiden tarjoaja on keskeisten palveluntarjoajien listalla.

Liikenne- ja viestintäministeriön työryhmä toteaa raportissaan (2017) useaan otteeseen (mm. s.9, 29, 32), että osana NIS-direktiivin vaatimuksia jäsenmaiden tulee määritellä luet-

telo keskeisistä palveluista, joiden pohjalta keskeiset palveluntarjoajat kyetään määrittämään. Työryhmän loppuraportti kuitenkin sivuuttaa keskeisten palvelujen määrittämisen ja hyppää suoraan keskeisten palveluntarjoajien määrittämiseen (s. 32-34), mikä direktiivin kannalta on nurinkurista. Raportissa ehdotetaan, että keskeisten palvelujen tarjoajaksi määrätään automaattisesti kaikki, jotka ovat alakohtaisen sääntelyn piirissä esimerkiksi sähkömarkkinalaki. Tällaiseen lähestymistapaan sisältyy riski, että sitä ei katsota EU:n taholta riittävän yhdenmukaistettavaksi muiden jäsenmaiden tekemien määritelmien kanssa. NIS-direktiivi antaa ymmärtää, että keskeisten palvelujen määrittäminen täytyy tehdä yksityiskohtaisemmin juurikin siksi, että yhdenmukaistaminen olisi mahdollista. Työryhmän raportti ei siis anna selkeää vastausta sille, miten keskeiset toimijat tullaan lopulta määrittämään. Se lähinnä vain suosittelee, että määrittely pitäisi tehdä osana alakohtaista lainsäädäntöä.

Perustuen NIS-direktiivin määritelmään sekä Liikenne- ja viestintäministeriön työryhmän loppuraporttiin, voidaan olettaa, että keskeisten toimijoiden listalla ei tule olemaan suuria yllätyksiä, vaan määrittäminen tehdään pääosin nykyisten toimialakohtaisten lakien pohjalta. Toimialakohtaisiin lakeihin saattaa kuitenkin tulla lisärajoituksia määrittämään, millainen palvelu voidaan katsoa keskeiseksi, sillä työryhmä ei suositellut erillisen toimijalistauksen tekemistä. EU:n vuoden 2010 tietojen pohjalta tekemän selvityksen mukaan Suomessa on energia-, liikenne-, rahoitus- ja terveyssektorilla yhteensä 966 toimijaa, jotka tulevat kuulumaan direktiivin piiriin. (Van Dijk Management Consultants & Time.lex 2012, 32-45)

Digitaaliset palvelun tarjoajia ei jäsenvaltiot erikseen määrittele, vaan vastuu jää itse yritykselle tunnistaa kuuluuko se direktiivin määritelmän piiriin vai ei. Direktiivi rajaa digitaaliset palvelut kolmeen luokkaan: hakukoneet, markkinapaikat ja pilvipalvelut. Digitaalisten toimijoiden osalta on hyvä huomioida, että mikroyritykset on vapautettu direktiivin vaatimuksista, joten se ei koske pienimpiä yrityksiä.

Digitaalisten toimijoiden osalta direktiivin täytäntöönpano lähtee riskienhallinnasta. Digitaalisille toimijoille on annettu vaatimuksia, mutta niiden mukainen toiminta tarkastetaan vain, mikäli virheellistä toimintaa epäillään. Tämäkin tarkastus tulee todennäköisesti rajoit-

tumaan viranomaisten resursseihin ja jää nähtäväksi, miten korkea tai matala kynnys tarkastukseen tekemiseen lopulta on.

Ne yritykset, joilla ei ole oikeushenkilöä EU:n alueella, mutta joiden katsotaan tarjoavan siellä palveluita, tulee valita EU:n alueella toimiva edustaja. Edustajan valinta määrittää myös sen, minkä maan lainsäädäntöä toimijan on noudatettava. Digitaalisten toimijoiden osalta EU kuitenkin pyrkii yhdenmukaistamaan digitaalisiin toimijoihin kohdistuvia toimenpiteitä. sillä toimijoiden toiminta kohdistuu usein useampaan kuin yhteen maahan. Mikäli lait ja määritelmät siitä, kuka on digitaalinen toimija eivät olisi yhdenmukaisia, ei myöskään yksi direktiivin tavoitteita: täydellinen sisämarkkina, voisi toteutua.

Digitaalisen palvelun tarjoajien sääntely on Suomessa ehdotettu otettavaksi osaksi tietoyhteiskuntakaarta (tietoyhteiskuntakaari kts. luku 2.4) (Liikenne- ja viestintäministeriö 2017, 38).

Kolmannet osapuolet ovat sellaisia toimijoita, joita direktiivi ei suoraan kosketa, mutta joiden voidaan katsoa ulottuvan välillisten vaikutusten piiriin. Vaikka direktiivin alaiset toimijat, keskeiset toimijat ja digitaaliset toimijat, ovat itse vastuussa direktiivin mukaisesta ilmoitusvelvollisuudesta, tulee kolmannen osapuolen olla kyvykäs tarjoamaan ilmoitusvelvollisuuden vaatimat tiedot, mikäli se haluaa tarjota palveluitaan direktiivin alaisille toimijoille. Mikäli kolmasosapuoli ei kykene direktiivin mukaisten ilmoitusten tekemiseen direktiivin alaiselle toimijalle, vahva oletus on, että yhteistyö tulee päättymään.

Sovelluskehittäjät, jotka tarjoavat sovelluksiaan direktiivin alaisille toimijoille, voidaan katsoa olevan yksi kolmansista osapuolista. Mikäli he haluavat jatkossakin tarjota ohjelmistojaan NIS-direktiivin alaisille toimijoille, on tärkeää huomioida, että sovellukset tukevat direktiivin mukaista toimintaa niin turvallisuuden osalta kuin ilmoitusvelvollisuudenkin osalta. NIS-direktiiviä tukevien ominaisuuksien voidaan jatkossa olettaa myös olevan myyntietu sellaisten sovellusten osalta, jotka sivuavat verkko- tai tietojärjestelmiä tai niiden turvallisuutta. Toinen selkeästi direktiivin alainen toimija on laitevalmistajat. Tällaisia laitevalmistajia ovat esimerkiksi verkkolaitevalmistajat tai erilaiset tietoturvallisuutta parantavat laitteistot ja palvelimet.

Koska kolmannen osapuolen toimijat eivät ole suoraan vastuussa direktiivin mukaisista toimista, voidaan heidän kohdallaan direktiiviä tukevan toiminnan olla ennemminkin myyntivaltti, heidän tarjotessaan palveluitaan direktiivin alaisille toimijoille. Tulee toki huomioida, että näitä kolmannen osapuolen toimijoita koskee kaikesta huolimatta tuotevastuuta koskeva säännöstö, eli hekin saattavat joutua vastuuseen ohjelmistojen virheistä.

Direktiivissä tuodaan esille uusimman tekniikan verkko- ja tietoturvallisuuden tason määrittämisessä (14 artikla 1 kohta; 16 artikla 1 kohta; resitaali 53). Tämä osaltaan tukee kolmansien osapuolten, lähinnä laitevalmistajien ja sovelluskehittäjien, mahdollisuutta auttaa NIS-direktiivin alaisia toimijoita kehittämällä uusia tietoturvallisuutta korostavia tuotteita. Direktiivin määritelmä saattaa myös nopeuttaa uusien laite- ja sovellusteknologioiden ja innovaatioiden markkinoille adaptointia.

Direktiivi voidaan katsoa aiheuttava myös välillisiä riskejä, ei vain sen piirissä oleville toimijoille, vaan myös muille. Kuten Laube & Böhmen (2016) tutkimuksesta ilmenee, koska tietoturvallisuusympäristö on keskenään riippuvainen, yhden yrityksen tietoturvainvestoinnin voidaan katsoa kasvattavan muiden yritysten alttiutta tietoturvaloukkauksille. Tästä näkökulmasta tarkasteltuna, voidaan todeta, että direktiivi luo riskejä paljon laajemmalle joukolle kuin vain direktiivin alaiset toimijat.

6 Pohdintaa ja yhteenveto

Tässä luvussa läpikäydään tutkimuksen tulokset ja pohditaan niiden vastaavuutta tutkimuskysymyksiin. Kantaa otetaan myös tulosten merkityksellisyyteen, luotettavuuteen ja käytettävyyteen sekä arvioidaan oleellisia jatkotutkimuskohteita.

6.1 Tutkimustulosten yhteenveto

Tämän pro gradu tutkielmassa tavoitteena oli selvittää, millaisia vaikutuksia EU:n verkko- ja tietoturvadirektiivillä tulee olemaan yritysten toimintaa riskinäkökulmasta tarkasteltuna. Vaikutuksia pyrittiin selvittämään analysoimalla direktiivin sisältöä, ja Liikenne- ja viestintäministeriön työryhmän loppuraportin sisältöä. Sisällöstä poimittiin ne osa-alueet, joilla katsottiin olevan vaikutus yrityksiin ja tämän jälkeen arvioitiin, liittyykö vaikutukseen riskiä. Lopuksi direktiivistä poimittiin riskinhallintaa tukevia toimenpiteitä. Lisäksi pyrittiin selvittämään, keitä direktiivin piiriin kuuluu. Myös tämän selvittämiseen käytettiin itse direktiivin sisältöä ja työryhmän loppuraporttia.

Ensimmäisen tutkimuskysymyksen tavoitteena oli selvittää, mitä riskejä NIS-direktiivi tuo yrityksille. Liiketoimintariskiä luovat tapahtumat, joiden lopputulos saattaa aiheuttaa sattuessaan negatiivisen vaikutuksen yrityksen toiminnalle. NIS-direktiiviin tunnistettiin liittyvän kolmenlaisia liiketoimintariskejä: compliance-riskejä, strategisia riskejä ja operatiivisia riskejä. Osa riskeistä liittyi direktiiviin kokonaisuutena ja osa direktiivin johonkin tiettyyn osa-alueeseen. Direktiiviin liittyen suurimmaksi riskiksi tunnistettiin compliance-riski, jota aiheuttaa direktiivi kokonaisuutena, mutta jota myös vahvistaa direktiivin useat osa-alueet. Compliance-riskiin läheisesti liittyivät strategiset riskit, joihin kuului myös NIS-direktiivin tuoma maineriski. Operatiivisiin riskeihin tunnistettiin liikesalaisuuksien pääsy vääriin käsiin, mikäli viranomaiset jakavat varomattomasti poikkeamiin liittyviä tietoja muiden jäsenmaiden viranomaisten kanssa, ja mahdollinen päällekkäinen ilmoitusvelvollisuus muiden lakien kanssa. Operatiivisia riskejä olivat myös riski, että turvallisuusohjeet luodaan ainoastaan direktiiviä varten, ei yrityksen liiketoimintaa ja, että osaajista, joista on jo nyt pulaa, tulee olemaan vieläkin suurempi pula tulevaisuudessa. Tunnistetuista riskeistä selkeästi todennäköisin oli compliance-riski. Compliance-riskin vaikutukset kuitenkin ovat

pienemmät, mikäli yritys toimii yhteistyössä viranomaisten kanssa ja on halukas kehittämään toimintaansa ohjeiden ja määräysten mukaiseksi. Strategisten ja operatiivisten riskien toteutumisen voidaan olettaa olevan epätodennäköisempää, mutta niiden tapahtuessaan aiheuttama haitta esimerkiksi yrityssalaisuuksien vuodon aiheuttamat liiketoiminnan tappiot voivat olla todella suuret.

Toinen tutkimuskysymys oli, mitä direktiivi tuo yritysten riskienhallintaan. Direktiiviin liittyen tunnistettiin useampia riskienhallintaa tukevia keinoja, joita se implementointinsa onnistuessa kykenee tuomaan yritysten toiminnan tueksi. Direktiivi jättää suuren vastuun turvallisuuden parantamisesta ja seurannasta sekä tietoturvallisuussuunnitelmien kehittämisestä ja ylläpitämisestä yritykselle itselleen, mutta kehottaa viranomaisia tukemaan yritysten riskienhallinnan toimenpiteitä. Myös standardien kehitystä ja käyttöä tullaan direktiivin pyrkimyksien mukaan tukemaan. Standardien kohdalle on kuitenkin hyvä huomioida Enisan arvio, jonka mukaan standardit on nykyisellään direktiivissä rajattu liian tiukasti koskemaan ainoastaan Euroopan parlamentin ja neuvoston asetuksen (No 1025/2012) mukaisiin standardeihin. Enisan mukaan tämä jättää ulkopuolelle suuren määrän laajasti markkinoilla käytössä olevia standardeja kuten NIST, ISF ja W3C (ENISA 2016). Direktiivi kehittää myös parhaiden käytänteiden jakamista ja poikkeamatietoutta niin kansallisella tasolla kuin EU:n laajuisestikin. Direktiivin voidaan myös olettaa lisäävän rikosilmoitusten tekemistä kyberrikoksista ja sitä kautta antaa virkavallalle mahdollisuuden puuttua rikolliseen toimintaan. Direktiivin voidaan olettaa tuovan yrityksille uusia riskienhallinnan työkaluja ja lisää mahdollisuuksia vaikuttaa ja puuttua keskeisimpiin verkko- ja tietoturvallisuutta vaarantaviin riskeihin nykyistä tehokkaammin. Lukumäärällisesti tunnistettuja riskienhallintakeinoja oli vähemmän kuin mahdollisia riskejä, mutta täytyy ottaa huomioon, että riskienhallintakeinot ovat kokonaisvaltaisempia ja toteutuessaan sama riskienhallintakeino kattaa useita riskikokonaisuuksia.

Kolmas tutkimuskysymys oli, mitkä yritykset kuuluvat direktiivin vaikutuksen piiriin. Tutkimuksen tekohetkellä selkein näistä ryhmistä oli digitaaliset toimijat, sillä niihin lukeutuvat kaikki riittävän suuret digitaaliset markkinapaikat, hakukoneet ja pilvipalvelut, jotka tarjoavat palveluitaan Euroopan unionin alueella. Toinen ryhmä on keskeiset toimijat. Vaikka direktiivi luettelee keskeisiin toimijoihin kuuluvat toimialat, on se jättänyt jäsen-

maille vielä erillisen vaatimuksen siitä, että näiden täytyy itse määrittää kriteerit, joiden perusteella keskeiset toimijat määräytyvät tai listata kaikki alueellansa toimivat keskeiset toimijat. Tutkimuksen tekohetkellä Suomi ei tällaista listausta ollut vielä tehnyt, mutta kansalliset työryhmän mukaan toteutus kannattaisi tehdä määritelmän kautta suoraan toimialakohtaisiin jo olemassa oleviin lakeihin. Tarkempaa määritelmää siitä, ketkä nämä toimijat Suomessa olisivat ei siis vielä tutkimuksenteko hetkellä ollut saatavilla. Tiedon pitäisi kuitenkin olla yksiselitteisesti saatavilla, kunhan uudet lakiesitykset julkaistaan. Vaikka direktiivi suoraan koskee vain näitä kahta ryhmää, voidaan sen piiriin katsoa kuuluvan myös kolmansia osapuolia. Tällaisia ovat esimerkiksi järjestelmä-, palvelu- ja laitevalmistajat, -toimittajat ja -myyjät, jotka toimivat verkko- ja tietojärjestelmäalueella, sillä jotta direktiivin alaiset toimijat voisivat noudattaa direktiivin määräyksiä, tulee niiden käyttämien ratkaisuiden tukea direktiivin vaatimuksia esimerkiksi turvallisuustasosta ja ilmoitusvelvollisuuden tukemisesta. Mikäli direktiivin alaiset toimijat parantavat verkko- ja tietojärjestelmäturvallisuuttaan, vaikuttaa se myös direktiivin ulkopuolisten toimijoiden turvallisuuden nykytilaan ja voi vaatia näiltä toimenpiteitä turvallisuustilansa ylläpitämiseksi.

Kuten tutkimustuloksista nähdään, direktiivi tuo yrityksille niin uusia riskejä, kuin riskienhallintaa tukeviakin keinoja. Se, ketkä direktiivin vaikutusten piiriin kuuluvat, on vaikeaa rajata, ennen kansallisten lakien täytäntöönpanoa, mutta jo nyt tiedetään, että joukko tulee olemaan laajempi, kuin vain suoraan direktiivin alaisiksi määritellyt toimijat. Epäonnistuessaan direktiivi tuo yrityksille useita taloudellisia ja toiminnallisia riskejä, jotka haittaavat yritysten toimintaa, mutta onnistuessaan se voi merkittävästi parantaa verkko- ja tietoturvallisuutta EU:n jäsenmaissa.

6.2 Tutkimuksen rajoitukset, arviointi ja luotettavuus

Yksi tutkimuksen lähtökohdista ja ennakko olettamista oli, että NIS-direktiivi, jonka päätehtävänä on auttaa yrityksiä hallitsemaan verkko- ja tietojärjestelmien turvallisuuteen liittyviä uhkia, luo ohessa myös liiketoiminnalle uhkia. Eli samalla kun direktiivi tarjoaa riskienhallinnan työkaluja, se myös luo yrityksille riskejä. Tutkimuskysymyksistä ensimmäinen olikin, millaisia vaikutuksia direktiivillä on yrityksille. Jotta vaikutukset pystytään

laittamaan kontekstiin, haluttiin myös selvittää, ketkä direktiivin vaikutuksen piiriin kuuluu, sillä direktiivillä oletettiin olevan myös välillisiä vaikutuksia yrityksiin ja toimialoihin, joita ei suoraan oltu määritelty itse direktiivissä. Viimeisenä, jotta tutkimus ei keskittyisi liikaa vaikutusten riskinäkökulmaan, painotettiin vielä niitä riskienhallinnan työkaluja, joita direktiivi tuo mukanaan yrityksille. Jokaiseen tutkimuskysymykseen löydettiin tutkimuksessa vastaus.

Vaikka tutkimuksessa pyritään välttämään virheitä, tulosten luotettavuus ja pätevyys ovat vaihtelevia. (Hirsjärvi ym. 1997, 231) Laadullisessa tutkimuksessa ei ole yksiselitteisiä vakiintuneita luotettavuuden arviointimenetelmiä.(Tuomi & Sarajärvi 2009, 140) Määrällisessä tutkimuksessa käytetään luotettavuutta (validius) ja toistettavuutta (reliaabelius), mutta nämä sopivat heikosti laadullisen tutkimuksen tulosten arviointiin.(Hirsjärvi ym. 1997, 231-233) Sen sijaan Tuomi ja Sarajärvi (2009, 140-141) ehdottavat muun muassa seuraavien arviointia: tutkimuksen kohde ja tarkoitus, tutkijan oma sitoumus, aineiston keruu, tutkimuksen kesto, aineistoanalyysi ja tutkimuksen luotettavuus/eettisyys.

Erityisesti kun kyse on riskiarvioista, tutkimustuloksia tarkasteltaessa tulee huomioida, että riskit ja niiden kokeminen on hyvin yksilöllistä (Yates 1992), joten on oletettavaa, että tutkimustulokset eivät ole täysin identtisiä, jos sama tutkimus suoritetaan kahden eri tutkijan toimesta. Koska tutkimustulokset perustuvat kuvattuun teoreettiseen viitekehykseen, voidaan tulosten kuitenkin olettaa olevan samansuuntaisia. Jotta tutkimustulosten luotettavuuden arviointi olisi mahdollista, on tutkimuksen etenemistä kuvattu liitteissä. Liitteessä A kuvataan vaikutusten tunnistamista ja direktiiviin liittyvät riskit on kirjattu artikloittain liitteessä E.

Aineiston kerääminen tutkimuksen alkuvaiheessa oli kattavaa ja sitä tehtiin useamman kuukauden ajalta. Ajankohdasta johtuen analyysiin ei kuitenkaan päästy sisällyttämään itse lakiehdotuksia, joten tutkimuksen tuloksia tulisi uudelleen arvioida lain voimaantulon jälkeen, jotta voidaan varmistua siitä, että ne eivät ole ristiriidassa lain sisällön kanssa. Myös mahdolliset oikeuskäsittelyt tai valtionviraston tekemät huomautukset yrityksille voivat joko vahvistaa tai heikentää tutkimuksen tuloksia. Tutkimuksessa ei ole otettu huomioon kesäkuun 2017 jälkeen julkaistua NIS-direktiiviä käsittelevää aineistoa. Tällaista on esi-

merkiksi elokuussa 2017 Iso-Britannian julkista konsultaatiota varten julkaisema NIS-direktiiviin vastaavan lakiehdotuksen sisältö (UK Department for Digital, Culture 2017). Tutkimuksen rajoitukseksi täytyy huomioida myös se, että se perustuu direktiiviin. Direktiivit ovat ohjeistuksia jäsenmaille, eivät suoria määräyksiä, jotka jäsenmaiden tulisi implementoida sellaisinaan lakeihinsa. Tästä johtuen lopullinen lakiesitys ei välttämättä täysin vastaa direktiivissä mainittuja kohtia.

6.3 Tutkimuksen merkittävyys ja jatkotutkimusaiheet

Tutkimukseen liittyi rajoitteita niin laajuuden kuin ajankohdankin kautta. Koska kyseessä on pro gradu -tutkielma, on sen laajuus rajallinen eikä siinä ole tarkoituksen mukaista lähteä selvittämään yksittäisiä tutkimuksen aikana ilmenneitä seikkoja. Tässä luvussa käsitellään mahdollisia jatkotutkimusaiheita sekä tutkimuksen merkittävyyttä sen julkaisuhetkellä.

NIS-direktiivistä on julkaistu vain vähän aikaisempia tutkimuksia. Koska direktiivi on jäänyt tietosuoja-asetuksen varjoon, voi direktiivin asettamat vaatimukset tulla yrityksille yllättäen. Tällöin riskinäkökulmasta tehty tutkimus voi auttaa yritystä päättämään direktiivin mukaisten toimenpiteiden tärkeysjärjestyksen. Tutkimus on hyödyksi myös tilanteissa, joissa yritys ei ennestään tunne direktiivin sisältöä ja haluaa perehtyä siihen tarkemmin. Tutkimuksen tulokset auttavat yrityksiä ymmärtämään, millaisia riskejä ja riskienhallinnan keinoja direktiivi tuo sen alaisille toimijoille. Rajoituksena täytyy muistaa, että kuten yksilöt, myös yritykset kokevat riskit eri tavoin ja heidän riskinottokykynsä ja -halunsa vaihtelee, joten jokaisen yrityksen tulisi arvioida mahdollisia riskejä omasta näkökulmastaan.

Koska tutkimuksen tekohetkellä kansallista lakia ei ollut julkaistu tutkimuksen voisi uusia siinä vaiheessa, kun kansallinen laki astuu voimaan. Tällöin tutkimustuloksia voisi täydentää mahdollisilla lakiin kirjattujen pykälien sisällöllä. Vaihtoehtoisesti tutkimuksen tuloksia voisi vertailla eri maiden lakien välillä.

Tutkimuksen tuloksia voisi tarkastella lain julkaisun jälkeen määrällisen tutkimuksen tai laadullisen haastattelu tutkimuksen avulla, jossa selvitettäisiin yritysten näkökulmia aiheeseen. Alkuperäisen tutkimuksen aikana oli vielä liian aikaista tehdä yrityshaastatteluita,

sillä ei ollut esimerkiksi yksiselitteistä määritelmää siitä, ketkä kuuluvat direktiivin vaikutuksen piiriin ja useilla yrityksillä ei ollut ymmärrystä siitä, mitä laki tulee sisältämään tai kuinka se vaikuttaa heihin. Myös direktiivin vaikutus kolmansiin osapuoliin ja muita välillisiä vaikutuksia voisi tutkia tätä tutkimusta laajemmin lain sisällön julkistamisen jälkeen.

Lähteet

Alasuutari, P., 2011. Laadullinen tutkimus 2.0 Neljäs uudistettu painos, Tampere: Osuuskunta vastapaino.

Anon, 2015. Belgia : Commission welcomes agreement to make EU online environment more secure. MENA Report. Saatavilla: https://search.proquest.com/docview/1747156868/abstract/18B60FA719B2445EPQ/1?accountid=11774 [Luettu 27.5.2017].

Anon, 2016a. Belgia : EU-wide cybersecurity rules adopted by the Council. MENA Report. Saatavilla: http://search.proquest.com/docview/1789665415/6E7F1812DF014B56PQ/47?accountid=11774 [Luettu 27.5.2017].

Anon, 2016b. European Union: Directive on Security of Network and Information Systems. Asia News Monitor. Saatavilla: http://search.proquest.com/docview/1802496770/6E7F1812DF014B56PQ/12?accountid=11774 [Luettu 27.5.2017].

Anon, 2017a. The Directive on security of network and information systems (NIS Directive) | Digital Single Market. Saatavilla: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive [Luettu 30.4.2017].

Anon, 2017b. The Network and Information Security Directive implications for the energy sector. Energy Monitor Worldwide. Saatavilla: http://search.proquest.com/docview/1865338681/citation/19406FFDBE7E431APQ/1?accountid=11774 [Luettu 27.5.2017].

Attila, M. ym., 2012. Teollisuuspäästödirektiivin toimeenpanon vaikutukset Suomessa, Saatavilla: https://helda.helsinki.fi/bitstream/handle/10138/39765/SYKEra_19_2012.pdf?sequence=1 [Luettu 17.7.2017].

Bartholomew, J., 2016. The EU has destroyed some of our most prosperous industries - and will continue to do so. The Telegraph. Saatavilla: http://www.telegraph.co.uk/news/2016/05/21/the-eu-has-destroyed-some-of-our-most-prosperous-industries---an/ [Luettu 19.7.2017].

Bebbington, J., Larrinaga, C. & Moneva, J.M., 2008. Corporate social reporting and reputation risk management. Accounting, Auditing & Accountability Journal, 21(3), pp.337–361. Saatavilla: http://www.emeraldinsight.com/doi/10.1108/09513570810863932 [Luettu 21.9.2017].

Benedek, P., 2012. Compliance Management – a New Response to Legal and Business Challenges. Acta Polytechnica Hungarica, 9(3), pp.135–148. Saatavilla: https://www.uni-obuda.hu/journal/Benedek_35.pdf [Luettu 20.7.2017].

Brown, C.S.D., 2015. Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. International Journal of Cyber Criminology, 9(1), pp.55–119. Saatavilla: http://media.proquest.com/media/pq/classic/doc/3790832691/fmt/pi/rep/NONE?cit%3Aauth=Brown%2C+Cameron+S+D&cit%3Atitle=Investigating+and+Prosecuting+Cyber+Crime%3A+Forensic+Dependencies+and+Barriers+to+Justice&cit%3Apub=Inte

rnational+Journal+of+Cyber+Crimi [Luettu 8.6.2017].
Byström, N., 2016. First EU-wide cybersecurity rules: the NIS Directive. Disruption Brief, 7, pp.1–5. Saatavilla: http://ddi.aalto.fi/en/publications/disruption_briefs/ [Luettu 30.4.2017].
Center for Strategic and International Studies, 2016. Hacking the Skills Shortage. Saatavilla: https://www.csis.org/events/hacking-skills-shortage [Luettu 28.7.2017].
Chavas, J.-P., 2004. Risk analysis in theory and practice, San Diego: Elsevier Academic Press.
Deloitte, 2014. 2014 global survey on reputation risk, Saatavilla: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/gx_grc_Reputation@Risk survey report_FINAL.pdf [Luettu 21.9.2017].
Deloitte Touche Tohmatsu Limited, 2017. Overcoming the threats and uncertainty Third-party governance and risk management (TPGRM).
Van Dijk Management Consultants & Time.lex, 2012. EUROPEAN COMMISSION Impact assessment of possible measures to enhance cooperation, coordination and information exchange in the area of Internet Security between Member States and stakeholders, including across sectors, in the EU, Brussels.
ENISA, 2016. Gaps in NIS standardisation. Recommendations for improving NIS in EU standardisation policy,
ENISA, 2017. Incident notification for DSPs in the context of the NIS Directive,
EU, 2013. Euroopan parlamentin ja neuvoston direktiivi 2013/11/EU kuluttajariitojen vaihtoehtoisesta riidanratkaisusta sekä asetuksen (EY) N:o 2006/2004 ja direktiivin 2009/22/EY muuttamisesta. Euroopan unionin virallinen lehti, p.L165/63. Saatavilla: http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX:32013L0011 [Luettu 13.5.2017].
Euroopan parlamentti ja euroopan unionin neuvosto, 2016. Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/ 1148. Euroopan unionin virallinen lehti, 19.7.2016. Saatavilla: http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016L1148&from=FI [Luettu 13.5.2017].
Europan neuvosto, 2017. Improving cyber security across the EU - Consilium. Saatavilla: http://www.consilium.europa.eu/en/policies/cyber-security/ [Luettu 20.7.2017].
European Commission, 2013. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. , p.20. Saatavilla: http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf [Luettu 12.7.2017].
Fortune, 2017. Petya Ransomware: Cyberattacks Hit Merck, Deutsche Post, WPP | Fortune.com. Fortune.com. Saatavilla: http://fortune.com/2017/06/27/petya-ransomware-cyber-attack-targets/ [Luettu 11.7.2017].
Gatlin, A., 2016. Amazon, Facebook, Google May Be Burdened Under New EU Security Law. Investor's Business Daily. Saatavilla: http://search.proquest.com/docview/1802326039/FC53A57119D743AEPQ/6?accountid=11774 [Luettu 27.5.2017].
Graham, C., 2017. NHS cyber attack: Everything you need to know about "biggest ransomware" offensive in history. Saatavilla: http://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/ [Luettu 11.7.2017].

Guibourg, C., 2015. EU to force firms to report cyber attacks. City A.M. Saatavilla: http://search.proquest.com/docview/1746738411/FC53A57119D743AEPQ/4?accountid=11774 [Luettu 27.5.2017].
Haines, F., 2017. Regulation and Risk Analysis. Methodological Regulatory theory. Foundations and applications. Collected and edited by Drahos, Peter, pp.181–193.
Hammond, B., 2013. EU cybersecurity strategy to stress cooperation; directive planned on internal network security. Cybersecurity Policy Report. Saatavilla: http://search.proquest.com/docview/1315925530/6E7F1812DF014B56PQ/7?accountid=11774 [Luettu 27.5.2017].
Hansen, L. ym., 2009. Digital Disaster, Cyber Security, and the Copenhagen School. International Studies Quarterly, 53, pp.1155–1175. Saatavilla: https://www.nyu.edu/projects/nissenbaum/papers/digital disaster.pdf [Luettu 22.5.2017].
Härkönen, A., 2017. Sähköisen reseptipalvelun toistuvat häiriöt työllistävät apteekkeja – ”Pahimmillaan asiakkaan lääkitysturvallisuus voi vaarantua”. Helsingin sanomat. Saatavilla: http://www.hs.fi/kotimaa/art-2000005225435.html [Luettu 8.6.2017].
Hirsjärvi, S., Remes, P. & Sajavaara, P., 1997. Tutki ja kirjoita 15., uudis., Helsinki: Tammi.
Holder, C. ym., 2016. Robotics and law: Key legal and regulatory implications of the robotics age (part II of II). Saatavilla: http://ac.els-cdn.com/S0267364916300899/1-s2.0-S0267364916300899-main.pdf?_tid=2cfb26ae-42be-11e7-85f9-00000aacb362&acdnat=1495877202_ae61b37e17616aa8e469f32b9b649412 [Luettu 27.5.2017].
Holzleitner, M.-T. & Reichl, J., 2017. European provisions for cyber security in the smart grid – an overview of the NIS-directive. Elektrotech. Inftech., 134/1, pp.14–18. Saatavilla: http://download.springer.com/static/pdf/81/art%253A10.1007%252Fs00502-017-0473-7.pdf?originUrl=http%3A%2F%2Flink.springer.com%2Farticle%2F10.1007%2Fs00502-017-0473-7&token2=exp=1495876869~acl=%2Fstatic%2Fpdf%2F81%2Fart%25253A10.1007%25252Fs00502-017-0473- [Luettu 27.5.2017].
Hopkin, P., 2017. Fundamentals of Risk Management: Undestanding, Evaluating and Implementing Effective Risk Management, Fourth Edition 4th ed., Kogan Page.
Hurtaud, S. ym., 2016. Agreement reached on EU Network and Information Security (NIS) Directive - A first analysis of the security and incident notification requirements for Operators of Essential Services and Digital Service Providers,
Hutter, B. & Power, M., 2000. RISK MANAGEMENT AND BUSINESS REGULATION, London. Saatavilla: https://core.ac.uk/download/pdf/219179.pdf [Luettu 19.7.2017].
IDG Connect & FireEye, 2015. Mixed state of readiness for new cybersecurity regulations in Europe, Saatavilla: https://www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/rpt-mixed-state-of-readiness-for-new-cybersecurity-regulations-in-europe.pdf [Luettu 27.5.2017].
Ilmonen, I. ym., 2010. Johda riskejä, Rössneck: Tammi.
Ilvonen, I., 2013. Knowledge Security - A Conceptual Analysis. Tampereen teknillinen yliopisto.
ITIL, 2011. ITIL-sanasto ja lyhenteet Suomenkielinen. Saatavilla: http://itsmf.fi/wp-

content/uploads/2014/03/ITIL_2011_Finnish_Glossary_v1.0.pdf [Luettu 17.5.2017].
Jurvelin, M., 2014. Rikkidirektiivin vaikutukset suomalaisiin varustamoihin. Novia Yrkeshögskolan. Saatavilla: https://www.theseus.fi/bitstream/handle/10024/84235/Jurvelin_Miika.pdf?sequence=1 [Luettu 17.7.2017].
Koski, H., Kotiranta, A. & Mattila, J., 2015. Maarajoitusten taloudelliset vaikutukset suomalaisissa yrityksissä ja kotitalouksissa. Saatavilla: https://www.etla.fi/wp-content/uploads/VNK-raportti-2015-19.pdf [Luettu 17.7.2017].
Laube, S. & Böhme, R., 2016. The economics of mandatory security breach reporting to authorities. Journal of Cybersecurity, 2(1), pp.29–41. Saatavilla: https://academic.oup.com/cybersecurity/article-lookup/doi/10.1093/cybsec/tyw002 [Luettu 30.4.2017].
Lehto, M. & Limnéll, J., 2016. Cyber Security Capability and the Case of Finland. In European Conference on Cyber Warefare and Security. Reading: Academic Conferences International Limited, pp. 182–190. Saatavilla: http://media.proquest.com/media/pq/classic/doc/4116798341/fmt/pi/rep/NONE?cit%3Aauth=Lehto%2C+Martti%3BLimnéll%2C+Jarno&cit%3Atitle=Cyber+Security+Capability+and+the+Case+of+Finland&cit%3Apub=European+Conference+on+Cyber+Warfare+and+Security&cit%3Avo [Luettu 12.3.2017].
Liikenne- ja viestintäministeriö, 2017. Verkko- ja tietoturvadirektiivi. Kansallista täytäntöönpanoa tukevan työryhmän loppuraportti, Saatavilla: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79770/LVM_09_2017_Verkko_ ja_tietoturvadirektiivi.pdf?sequence=1 [Luettu 29.4.2017].
Liikenne- ja viestintäministeriö & Tietoturvallisen liiketoiminnan kehittämisryhmä, 2016. Maailman luetetuinta digitaalista liiketoimintaa. Suomen tietoturvallisuusstrategia. Liikenne- ja viestintäministeriön julkaisuja, (7/2016). Saatavilla: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/78106/Julkaisuja_7-2016.pdf?sequence=1 [Luettu 31.5.2017].
Mäkelä, K., 1990. Kvalitatiivisen analyysin arviointiperusteet. Teoksessa Kvalitatiivisen aineiston analyysi ja tulkinta. K. Mäkelä, ed., Helsinki: Painokaari Oy.
NCA Strategic Cyber Industry Group, 2016. Cyber Crime Assessment 2016, Saatavilla: http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file [Luettu 15.8.2017].
O'Callaghan, T., 2007. Disciplining Multinational Enterprises: The Regulatory Power of Reputation Risk. Global Society, 21(1), pp.95–117. Saatavilla: http://www.tandfonline.com/doi/pdf/10.1080/13600820601116583?needAccess=true [Luettu 16.9.2017].
Oikeusministeriö, 1999. Henkilötietolaki 523/1999. Saatavilla: http://www.finlex.fi/fi/laki/ajantasa/1999/19990523 [Luettu 13.7.2017].
Oikeusministeriö, 2014. Tietoyhteiskuntakaari 917/2014. Saatavilla: http://www.finlex.fi/fi/laki/ajantasa/2014/20140917 [Luettu 13.7.2017].
Paakkanen, M. & Räisänen, K., 2017. OP:lla pahoja teknisiä ongelmia: konttoreita kiinni, verkkopalveluissa ja maksukorteissa häiriöitä. Helsingin sanomat. Saatavilla: http://www.hs.fi/talous/art-2000005244914.html [Luettu 8.6.2017].
Pitkänen, O., 2005. Legal challenges to future information businesses. Helsinki Institute

for Information Technology HIIT,Helsinki University of Technology. Saatavilla: https://aaltodoc.aalto.fi/bitstream/handle/123456789/2666/isbn9512279983.pdf?sequence=1&isAllowed=y [Luettu 19.7.2017].
Pultarova, T., 2016. Cyber Security Ukraine Grid Hack Is Wake-Up Call for Network Operators Embedded Mcu Software. Engineering & Technology, (February), pp.12–13.
Saarelainen, A., 2016. It-ala löysi tietoturvavakuutukset – "tarpeettomasta turvasta ei kannata maksaa" - Tivi. TIVI. Saatavilla: http://www.tivi.fi/Kaikki_uutiset/it-ala-loysi-tietoturvavakuutukset-tarpeettomasta-turvasta-ei-kannata-maksaa-6590628 [Luettu 11.7.2017].
Sampo Group, 2017. Sanasto | Sampo.com. Saatavilla: http://www.sampo.com/fi/tietoameista/sanasto/ [Luettu 10.7.2017].
Shameli-Sendi, A., Aghababaei-Barzegar, R. & Cheriet, M., Taxonomy of Information Security Risk Assessment (ISRA). Saatavilla: https://www.researchgate.net/profile/Alireza_Shameli-Sendi/publication/284031735_Taxonomy_of_Information_Security_Risk_Assessment_ISRA/links/564b5bec08ae3374e5dd962b.pdf [Luettu 27.5.2017].
Sisäministeriö, 2013. Ministeri Räsänen: Kyberuhkien torjunta vaatii kaikkien yhteiskunnan toimijoiden huomion - Artikkeli - Sisäministeriö. Saatavilla: http://intermin.fi/artikkeli/-/asset_publisher/ministeri-rasanen-kyberuhkien-torjunta-vaatii-kaikkien-yhteiskunnan-toimijoiden-huomion?_101_INSTANCE_jyFHKc3on2XC_languageId=fi_FI [Luettu 28.5.2017].
Von Solms, B. & Von Solms, R., 2004. The 10 deadly sins of information security management. Computers & security, 23, pp.371–376. Saatavilla: http://ac.els-cdn.com/S0167404804001221/1-s2.0-S0167404804001221-main.pdf?_tid=fdecb754-7901-11e7-8384-00000aacb35e&acdnat=1501843694_1116692caadbcc7e46eac05033e81be1 [Luettu 4.8.2017].
Suominen, A., 2003. Riskienhallinta 3., Porvoo: WSOY.
Talus, A. ym., 2017. Miten valmistautua EU:n tietosuoja-asetukseen? Oikeusministeriön julkaisu 4/2017. Saatavilla: http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79316/OMSO_04_2017_OM_TSV_EU_tietosuoja.pdf?sequence=1 [Luettu 8.6.2017].
Tuomi, J. & Sarajärvi, A., 2009. Laadullinen tutkimus ja sisällönanalyysi 5. uudistettu painos, Helsinki: Kustannusosakeyhtiö Tammi.
UK Department for Digital, Culture, M. and S., 2017. Security of Network and Information Systems. Public consultation. (8). Saatavilla: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/636207/NIS_Directive_-_Public_Consultation__1_.pdf [Luettu 19.8.2017].
Weber, R.H. & Studer, E., 2016. Cybersecurity in the Internet of Things: Legal aspects. Computer Law and Security Review, 32(5), pp.715–728. Saatavilla: http://dx.doi.org/10.1016/j.clsr.2016.07.002 [Luettu 27.5.2017].
Yates, F., 1992. Risk-taking behavior, Chichester: Wiley.

Liitteet

A NIS-direktiivin sisältö (Euroopan parlamentti ja euroopan unionin neuvosto 2016)

NIS-direktiivin sisältö ja lukuihin liittyvä koodaus, joka ilmaisee, sisältyykö lukuun palvelun tarjoajiin kohdistuvaa sisältöä:

x keskeinen palvelun tarjoaja
o digitaalisen palvelun tarjoaja

I LUKU YLEISET SÄÄNNÖKSET

x	o	1 artikla	Kohde ja soveltamisala
		2 artikla	Henkilötietojen käsittely
		3 artikla	Vähimmäistason yhdenmukaistaminen
x	o	4 artikla	Määritelmät
x		5 artikla	Keskeisten palvelujen tarjoajien määrittäminen
x		6 artikla	Merkittävä haitallinen vaikutus

II LUKU VERKKO- JA TIETOJÄRJESTELMIEN TAURVALLISUUTTA KOSKEVAT KANSALLISET KEHYKSET

x	o	7 artikla	Verkko- ja tietojärjestelmien turvallisuutta koskeva kansallinen strategia
		8 artikla	Kansalliset toimivaltaiset viranomaiset ja keskitetty yhteyspiste
		9 artikla	Tietoturvaloukkauksiin reagoivat ja niitä tutkivat yksiköt (CSIRT-toimijat)
		10 artikla	Yhteistyö kansallisella tasolla

III LUKU YHTEISTYÖ

	11 artikla	Yhteistyöryhmä
	12 artikla	CSIRT-verkosto
	13 artikla	Kansainvälinen yhteistyö

IV LUKU KESKEISTEN PALVELUJEN TARJOAJIEN VERKKO- JA TIETOJÄRJESTELMIEN TURVALLISUUS

x		14 artikla	Turvallisuusvaatimukset ja poikkeamien ilmoittaminen
x		15 artikla	Täytäntöönpano ja sen valvonta

V LUKU DIGITAALISEN PALVELUN TARJOAJIEN VERKKO- JA TIETOJÄRJESTELMIEN TURVALLISUUS

x	o	16 artikla	Turvallisuusvaatimukset ja poikkeamien ilmoittaminen
	o	17 artikla	Täytäntöönpano ja sen valvonta
	o	18 artikla	Lainkäyttövalta ja alueperiaate

VI LUKU STANDARDOINTI JA VAPAAHETOINEN ILMOITTAMINEN

- [x] [o] 19 artikla Standardointi
- 20 artikla Vapaaehtoinen ilmoittaminen

VII LUKU LOPPUSÄÄNNÖKSET

- [x] [o] 21 artikla Seuraamukset
- 22 artikla Komiteamenettely
- 23 artikla Uudelleen tarkastelu
- 24 artikla Siirtymätoimenpiteet
- 25 artikla Saattaminen osaksi kansallista lainsäädäntöä
- [x] [o] 26 artikla Voimaantulo
- 27 artikla Osoitus

B NIS-direktiivin keskeisten toimijoiden tyypit (direktiivin liite II)

NIS-direktiivin mukaiset keskeisten toimijoiden tyypit. Tämän osion sisältö on kohtien ”Toimiala”, ”Osa-alue” ja ”Toimijan tyyppi” suoraan NIS-direktiivistä ja määritelmät ovat suoraan niiden kohdalla mainituista lähteistä.

Toimiala	Osa-alue	Toimijan tyyppi
1. Energia	a) Sähkö	Sähköalan yritykset, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston direktiivin 2009/72/EY (1) 2 artiklan 35 kohdassa, jotka harjoittavat kyseisen direktiivin 2 artiklan 19 kohdassa määriteltyä toimitusta
		Jakeluverkonhaltijat, sellaisina kuin ne määritellään direktiivin 2009/72/EY 2 artiklan 6 kohdassa
		Siirtoverkonhaltijat, sellaisina kuin ne määritellään direktiivin 2009/72/EY 2 artiklan 4 kohdassa
	b) Öljy	Öljynsiirtoputkistojen haltijat
		Öljyn tuotanto-, jalostus- ja käsittelylaitteistojen haltijat sekä öljyn varastointia ja siirtoa hoitavat operaattorit
	c) Kaasu	Maakaasun toimittajat, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston direktiivin 2009/73/EY (2) 2 artiklan 8 kohdassa
		Jakeluverkonhaltijat, sellaisina kuin ne määritellään direktiivin 2009/73/EY 2 artiklan 6 kohdassa
		Siirtoverkonhaltijat, sellaisina kuin ne määritellään direktiivin 2009/73/EY 2 artiklan 4 kohdassa
		Varastointilaitteiston haltijat, sellaisina kuin ne määritellään direktiivin 2009/73/EY 2 artiklan 10 kohdassa
		Nesteytetyn maakaasun käsittelylaitteiston haltijat, sellaisina kuin ne määritellään direktiivin 2009/73/EY 2 artiklan 12 kohdassa

		Maakaasualan yritykset, sellaisina kuin ne määritellään direktiivin 2009/73/EY 2 artiklan 1 kohdassa
		Maakaasun jalostus- ja käsittelylaitteistojen haltijat
2. Liikenne	a) Lentoliikenne	Lentoliikenteen harjoittajat, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 300/2008 (3) 3 artiklan 4 kohdassa
		Lentoaseman pitäjät, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston direktiivin 2009/12/EY (4) 2 artiklan 2 kohdassa, lentoasemat, sellaisina kuin ne määritellään kyseisen direktiivin 2 artiklan 1 kohdassa, mukaan lukien Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 1315/2013 (5) liitteessä II olevassa 2 jaksossa luetellut ydinlentoasemat, sekä lentoasemilla sijaitsevia lisärakennelmia ja -laitteita hoitavat toimijat
		Liikenteenhallinnan ylläpitäjät, jotka tarjoavat lennonjohtopalvelua, sellaisena kuin se määritellään Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 549/2004 (6) 2 artiklan 1 kohdassa
	b) Rautatieliikenne	Rataverkon haltijat, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston direktiivin 2012/34/EU (7) 3 artiklan 2 kohdassa
		Rautatieyritykset, sellaisina kuin ne määritellään direktiivin 2012/34/EU 3 artiklan 1 kohdassa, mukaan lukien palvelupaikan ylläpitäjät, sellaisina kuin ne määritellään direktiivin 2012/34/EU 3 artiklan 12 kohdassa
	c) Vesiliikenne	Sisävesillä, merillä ja rannikoilla matkustaja- ja rahtiliikennettä hoitavat yhtiöt, sellaisina kuin ne määritellään meriliikennettä varten Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 725/2004 (8) liitteessä I, lukuun ottamatta noiden yhtiöiden liikennöimiä yksittäisiä aluksia

		Euroopan parlamentin ja neuvoston direktiivin 2005/65/EY (9) 3 artiklan 1 kohdassa määriteltyjen satamien hallinnointielimet, mukaan lukien niiden satamarakenteet, sellaisina kuin ne määritellään asetuksen (EY) N:o 725/2004 2 artiklan 11 kohdassa, sekä toimijat, jotka huolehtivat tuotantolaitoksista ja laitteista satamien alueella
		Euroopan parlamentin ja neuvoston direktiivin 2002/59/EY (10) 3 artiklan o alakohdassa määriteltyjen alusliikennepalvelujen tarjoajat
	d) Tieliikenne	Tieviranomaiset, sellaisina kuin ne määritellään komission delegoidun asetuksen (EU) 2015/962 (11) 2 artiklan 12 kohdassa, jotka vastaavat liikenteenhallinnasta
		Euroopan parlamentin ja neuvoston direktiivin 2010/40/EU (12) 4 artiklan 1 kohdassa määriteltyjen älykkäiden liikennejärjestelmien ylläpitäjät
3. Pankkiala		Luottolaitokset, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 575/2013 (13) 4 artiklan 1 kohdassa
4. Finanssimarkkinoiden infrastruktuurit		Euroopan parlamentin ja neuvoston direktiivin 2014/65/EU (14) 4 artiklan 24 kohdassa määriteltyjen kauppapaikkojen ylläpitäjät
		Keskusvastapuolet, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 648/2012 (15) 2 artiklan 1 kohdassa
5. Terveydenhuoltoala	Terveydenhuoltolaitokset (mukaan lukien sairaalat ja yksityisklinikat)	Terveydenhuollon tarjoajat, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston direktiivin 2011/24/EU (16) 3 artiklan g alakohdassa

6. Juomaveden toimittaminen ja jakelu		Neuvoston direktiivin 98/83/EY (17) 2 artiklan 1 kohdan a alakohdassa määritellyn ihmisten käyttöön tarkoitetun veden toimittajat ja jakelijat, lukuun ottamatta jakelijoita, joille ihmisten käyttöön tarkoitetun veden jakelu on ainoastaan osa niiden yleistä toimintaa, joka muodostuu sellaisten muiden hyödykkeiden ja tavaroiden jakelusta, joita ei katsota keskeisiksi palveluiksi.
7. Digitaalinen infrastruktuuri		IXP:t
		Nimipalvelujen tarjoajat
		Aluetunnusrekisterit

C Digitaalisen palvelun tarjoajat (direktiivin liite III)

Digitaaliset palvelun tarjoajat, kuten ne on lueteltu direktiivin liitteessä III ja määritelty 4 artiklassa sekä se, mitä viittauksen takana sanotaan, mikäli viittausta käytetty määritelmässä.

1. Verkossa toimiva markkinapaikka.

4 artiklan 17 kohdan määritelmä	**Määritelmä viittauksen takana**
Tarkoitetaan digitaalista palveluja, joka antaa Euroopan direktiivin 2013/11/EU 4 artiklan 1 kohdan a alakohdassa määritellylle kuluttajille ja tai kyseisen direktiivin 4 artiklan 1 kohdassa b alakohdassa määritellylle elinkeinonharjoittajille mahdollisuuden tehdä verkossa kauppa- tai palvelusopimuksia elinkeinonharjoittajien kanssa joko verkossa toimivan markkinapaikan verkkosivustoilla tai elinkeinonharjoittajan verkkosivustolla, joka käyttää verkossa toimivan markkinapaikan tarjoamia tietojenkäsittelypalveluja.(Euroopan parlamentti ja euroopan unionin neuvosto 2016)	2013/11/EU 4.1.a (EU 2013) ’kuluttajalla’ tarkoitetaan luonnollista henkilöä, joka toimii tarkoituksessa, joka ei kuulu hänen elinkeino- tai ammattitoimintaansa. 2013/11/EU 4.1.b (EU 2013) ’elinkeinonharjoittajalla’ tarkoitetaan luonnollista henkilöä tai yksityisessä tai julkisessa omistuksessa olevaa oikeushenkilöä, joka toimii tarkoituksessa, joka kuuluu hänen elinkeino- tai ammattitoimintaansa, mukaan luettuna elinkeinonharjoittajan nimissä tai puolesta toimivat henkilöt

2. Verkossa toimiva hakukone.

4 artiklan 18 kohdan määritelmä	Määritelmä viittauksen takana
Tarkoitetaan digitaalista palvelua, joka antaa käyttäjille mahdollisuuden tehdä hakuja periaatteessa kaikilta verkkosivustoilta tai tietynkielisiltä verkkosivustoilta mitä tahansa aihetta koskevan hakusanan, lausekkeen tai muun tiedon muodossa tehdyn kyselyn perusteella ja joka antaa tulokseksi linkkejä, joista voi saada pyydettyyn sisältöön liittyvää tietoa.(Euroopan parlamentti ja euroopan unionin neuvosto 2016)	-

3. Pilvipalvelu.

4 artiklan 19 kohdan määritelmä	Määritelmä viittauksen takana
Tarkoitetaan digitaalista palvelua, joka mahdollistaa pääsyn skaalautuvaan ja mukautuvaan joukkoon jaettavissa olevia tietoteknisiä resursseja.(Euroopan parlamentti ja euroopan unionin neuvosto 2016)	-

D Selitykset (4 artikla)

NIS-direktiivin 4 artiklassa annetut määritelmät, joita käytetään myös tässä paperissa direktiivistä puhuttaessa.

Tässä direktiivissä tarkoitetaan

1) ’verkko- ja tietojärjestelmällä’
    a) direktiivin 2002/21/EY 2 artiklan a alakohdassa tarkoitettua sähköistä viestintäverkkoa;
    b) laitetta taikka yhteen kytkettyjen tai toisiinsa yhteydessä olevien laitteiden ryhmää, joista yksi tai useampi suorittaa ohjelman avulla digitaalisten tietojen automaattista käsittelyä; tai
    c) digitaalisia tietoja, joita a ja b alakohdassa tarkoitetuissa järjestelmissä säilytetään, käsitellään, haetaan tai siirretään niiden toimintaa, käyttöä, suojausta tai ylläpitoa varten;
2) ’verkko- ja tietojärjestelmien turvallisuudella’ verkko- ja tietojärjestelmien kykyä suojautua tietyllä varmuudella toimilta, jotka vaarantavat tallennettujen tai siirrettyjen tai käsiteltyjen tietojen taikka muiden kyseisissä verkko- ja tietojärjestelmissä

tarjottujen tai niiden välityksellä saatavilla olevien palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden;

3) ’verkko- ja tietojärjestelmien turvallisuutta koskevalla kansallisella strategialla’ kehystä, jossa esitetään verkko- ja tietojärjestelmien turvallisuutta koskevat kansallisen tason strategiset tavoitteet ja painopisteet;
4) ’keskeisten palvelujen tarjoajalla’ julkista tai yksityistä toimijaa, joka on liitteessä II tarkoitettua tyyppiä ja täyttää 5 artiklan 2 kohdassa säädetyt kriteerit;
5) ’digitaalisella palvelulla’ Euroopan parlamentin ja neuvoston direktiivin (EU) 2015/1535 1 artiklan 1 kohdan b alakohdassa tarkoitettua palvelua, joka on liitteessä III lueteltua tyyppiä;
6) ’digitaalisen palvelun tarjoajalla’ oikeushenkilöä, joka tarjoaa digitaalista palvelua;
7) ’poikkeamalla’ mitä tahansa tapahtumaa, joka tosiasiassa vaikuttaa haitallisesti verkko- ja tietojärjestelmien turvallisuuteen;
8) ’poikkeamien käsittelyllä’ kaikkia menettelyjä, jotka tukevat poikkeaman havaitsemista, analyysia ja sen vaikutusten rajoittamista sekä siihen reagointia;
9) ’riskillä’ mitä tahansa kohtuullisesti tunnistettavissa olevaa tilannetta tai tapahtumaa, joka saattaa vaikuttaa haitallisesti verkko- ja tietojärjestelmien turvallisuuteen;
10) ’edustajalla’ unioniin sijoittautunutta luonnollista henkilöä tai oikeushenkilöä, joka on nimenomaisesti nimetty toimimaan sellaisen digitaalisen palvelun tarjoajan puolesta, joka ei ole sijoittautunut unioniin; kansallinen toimivaltainen viranomainen tai CSIRT-toimija voi ottaa yhteyttä tällaiseen edustajaan digitaalisen palvelun tarjoajan sijasta kyseisen digitaalisen palvelun tarjoajan tämän direktiivin mukaisten velvollisuuksien osalta;
11) ’standardilla’ asetuksen (EU) N:o 1025/2012 2 artiklan 1 kohdassa tarkoitettua standardia; 12) ’eritelmällä’ asetuksen (EU) N:o 1025/2012 2 artiklan 4 kohdassa tarkoitettua teknistä eritelmää;
12) ’internetin yhdysliikennepisteellä (IXP)’ verkkoinfrastruktuurin osaa, joka mahdollistaa useamman kuin kahden riippumattoman autonomisen järjestelmän yhdistämisen pääasiassa internetliikenteen välittämisen helpottamiseksi; IXP tarjoaa yhteenliittämistä ainoastaan autonomisille järjestelmille; IXP ei edellytä minkään yhteenliittämänsä kahden autonomisen järjestelmän väliseltä internetliikenteeltä kulkemis-

ta minkään kolmannen autonomisen järjestelmän kautta, eikä se muuta tällaista liikennettä tai muutoin puutu siihen;

13) ’nimipalvelulla’ hajautettua hierarkkista verkon nimijärjestelmää, joka käsittelee nimipalvelukyselyjä;
14) ’nimipalvelujen tarjoajalla’ toimijaa, joka tarjoaa nimipalveluja internetissä;
15) ’aluetunnusrekisterillä’ toimijaa, joka hallinnoi ja hoitaa internetin verkkotunnusten rekisteröintiä tietyn aluetunnuksen puitteissa;
16) ’verkossa toimivalla markkinapaikalla’ digitaalista palvelua, joka antaa Euroopan parlamentin ja neuvoston direktiivin 2013/11/EU 4 artiklan 1 kohdan a alakohdassa määritellyille kuluttajille ja/tai kyseisen direktiivin 4 artiklan 1 kohdan b alakohdassa määritellyille elinkeinonharjoittajille mahdollisuuden tehdä verkossa kauppa- tai palvelusopimuksia elinkeinonharjoittajien kanssa joko verkossa toimivan markkinapaikan verkkosivustolla tai elinkeinonharjoittajan verkkosivustolla, joka käyttää verkossa toimivan markkinapaikan tarjoamia tietojenkäsittelypalveluja;
17) ’verkossa toimivalla hakukoneella’ digitaalista palvelua, joka antaa käyttäjille mahdollisuuden tehdä hakuja periaatteessa kaikilta verkkosivustoilta tai tietynkielisiltä verkkosivustoilta mitä tahansa aihetta koskevan hakusanan, lausekkeen tai muun tiedon muodossa tehdyn kyselyn perusteella ja joka antaa tulokseksi linkkejä, joista voi saada pyydettyyn sisältöön liittyvää tietoa;
18) ’pilvipalvelulla’ digitaalista palvelua, joka mahdollistaa pääsyn skaalautuvaan ja mukautuvaan joukkoon jaettavissa olevia tietoteknisiä resursseja

E Direktiivin riskit kohdittain

Tässä liitteessä läpikäydään direktiivistä ne osa-alueet, joihin liittyen on tunnistettu liiketoimintariskejä sekä avataan, mitä nämä riskit ovat. Riskien kannalta oleelliset resitaalit on liitetty direktiivin niihin artiklan kohtiin, johon ne liittyvät, jotta saadaan kokonaisvaltaisempi kuva direktiivin sisällöstä ja sitä kautta riskeistä. Koska yksittäisen artiklan kohdasta ei voida aina suoraan päätellä, mihin toimijaan se viittaa, on vaikutuksen alaiset toimijat myös listattu jokaisessa kohdassa.

Riskeille on annettu tunnisteet niiden käsittelyn helpottamiseksi. Esimerkiksi 1 artiklan 5 kohtaan liittyvän riskin tunniste on 1.5. Mikäli samaan kohtaan liittyy useampi riski, on ne lisäksi merkitty kirjaimin a, b, c, esimerkiksi 1.5.a.

1 artiklan 5 kohta Resitaali 41 Resitaali 59		Vaikuttaa: Keskeiset toimijat Digitaaliset toimijat
Tietoja, jotka katsotaan luottamuksellisiksi unionin ja kansallisten sääntöjen, kuten liikesalaisuuksia koskevien sääntöjen mukaisesti, vaihdetaan komission ja muiden asianomaisten viranomaisten kanssa vain silloin, kun tällainen vaihtaminen on välttämätöntä tämän direktiivin soveltamiseksi, sanotun kuitenkaan rajoittamatta Euroopan unionin toiminnasta tehdyn sopimuksen 346 artiklan soveltamista. Tällöin on vaihdettava ainoastaan sellaisia tietoja, jotka ovat merkityksellisiä ja oikeasuhteisia tällaisen vaihdon tarkoituksen kannalta. Tällaisessa tiedonvaihdossa on säilytettävä kyseisten tietojen luottamuksellisuus sekä suojeltava keskeisten palvelujen tarjoajien ja digitalisen palvelun tarjoajien turvallisuusetuja ja kaupallisia etuja. *Jos tietoja pidetään luottamuksellisina liikesalaisuuksia koskevien unionin ja kansallisten sääntöjen mukaisesti, tällainen luottamuksellisuus olisi varmistettava tässä direktiivissä säädettyjen toimien ja tavoitteiden toteuttamisen yhteydessä.* *Toimivaltaisten viranomaisten olisi kiinnitettävä asianmukaista huomiota epävirallisten ja luotettavien tiedonjakokanavien säilyttämiseen. Toimivaltaisille viranomaisille raportoitujen poikkeamien julkistamisessa olisi otettava asianmukaisesti ja tasapainoisesti huomioon yleisön yleinen etu saada tietoa uhista sekä toisaalta poikkeamista raportoivien keskeisten palvelujen tarjoajien ja digitaalisen palvelun tarjoajien mahdollinen maineen vahingoittuminen ja niille mahdollisesti koituva taloudellinen vahinko. Ilmoitusvelvollisuuksien täytäntöönpanossa toimivaltaisten viranomaisten ja CSIRT-toimijoiden olisi kiinnitettävä erityistä huomiota tarpeeseen pitää tuotteiden haavoittuvuutta koskevat tiedot tiukasti luottamuksellisina ennen asiaankuuluvien turvallisuuspäivitysten julkistamista.*		
Havaitut riskit	(1.5.a) Riski, että yrityksen liikesalaisuuksia pääsee vääriin käsiin, sillä direktiivin nojalla myös liikesalaisuuksien alainen tieto voidaan jakaa muille jäsenmaille, mikäli sen katsotaan olevan direktiivin nojalla tarpeellista. (1.5.b) Vaikka tiedonjaossa painotetaan luottamuksellisen tiedon jakamisen haitan arviointia yritykselle, on riski, että viranomainen ei tunnista eri alojen keskeisiä liikesalaisuuksien alaisia toimintoja ja tietoja sekä niiden kriittisyyttä, ja näin ollen aliarvioi tietojen jakamisesta yrityksille aiheutuvan haitan. (1.5.c) Riski, että luottamuksellista tietoa esim. liikesalaisuuksia päätyy vääriin käsiin.	

1 artiklan 7 kohta		Vaikuttaa: Keskeiset toimijat Digitaaliset toimijat
Kun alakohtaisessa unionin säädöksessä edellytetään keskeisten palvelujen tarjoajien tai digitaalisen palvelun tarjoajien joko varmistavan verkko- ja tietojärjestelmiensä turvallisuuden tai ilmoittavan poikkeamista, sovelletaan kyseisen alakohtaisen unionin säädöksen säännöksiä edellyttäen, että siinä säädetyt vaatimukset ovat vaikutukseltaan vähintään vastaavia kuin tässä direktiivissä säädetyt velvollisuudet.		

Havaitut riskit	(1.7) Direktiivin noudattaminen ei ole yksiselitteistä vaan toimijan tulee varmistaa, tuleeko sen seurata NIS-direktiivin mukaisia vaatimuksia vai onko sille määritetty toimialakohtaisia vaatimuksia. Tämän jälkeen pitää vielä tunnistaa kummat vaatimuksista ovat tiukempia verkko- ja tietojärjestelmäturvallisuuden osalta. Riski, että yritys ymmärtää lain eri tavalla kuin lainsäätäjä eikä näin noudata sen vaatimuksia. Riskin realisoitumiseen vaikuttaa myös direktiivien kansallinen toteutus ja sen yksiselitteisyys.

5 artiklan 2 kohta		Vaikuttaa: Keskeiset toimijat
Edellä 4 artiklan 4 kohdassa tarkoitetut kriteerit keskeisten palvelujen tarjoajien määrittämiseksi ovat seuraavat: *a) toimija tarjoaa palvelua, joka on keskeinen yhteiskunnan ja/tai talouden kriittisten toimintojen ylläpitämiseksi; b) kyseisen palvelun tarjoaminen on riippuvainen verkko- ja tietojärjestelmistä; ja c) poikkeamalla olisi merkittäviä haitallisia vaikutuksia kyseisen palvelun tarjoamiseen.*		
Havaitut riksit	(5.2) Direktiivissä annetut määritelmät ovat laajoja ja tulkinnanvaraisia, mikä vaikeuttaa niiden tulkintaa ja kasvattaa compliance-riskiä. Kansallisella täytäntöönpanolla ja sen yksiselitteisyydellä on suuri merkitys riskin realisoitumiselle.	

6 artiklan 1 kohta Resitaali 27 Resitaali 28		Vaikuttaa: Keskeiset toimijat
Määrittäessään 5 artiklan 2 kohdan c alakohdassa tarkoitetun haitallisen vaikutuksen merkitystä jäsenvaltioiden on otettavan huomioon vähintään seuraavat toimialojen väliset tekijät: a) asianomaisen toimijan tarjoamasta palvelusta riippuvaisten käyttäjien lukumäärä; b)muiden liitteessä II tarkoitettujen toimialojen riippuvaisuus kyseisen toimija tarjoamasta palvelusta; c) vaikutus, joka poikkeamilla voisi olla vakavuutensa ja kestonsa perusteella talouden ja yhteiskunnan toimintoihin tai yleiseen turvallisuuteen; d) kyseisen toimijan markkinaosuus; e) maatieteellinen levinneisyys alueella, johon poikkeama saattaa vaikuttaa; f) toimijan merkitys palvelun riittävän tason ylläpitämisessä ottaen huomioon kyseisen palvelun tarjoamista koskevien vaihtoehtoisten keinojen saatavuus. *Sen määrittämiseksi, olisiko poikkeamalla merkittävä haitallinen vaikutus keskeisen palvelun tarjoamiseen, jäsenvaltioiden olisi otettava huomioon useita eri tekijöitä, kuten niiden käyttäjien lukumäärä, jotka ovat riippuvaisia kyseisestä palvelusta henkilökohtaisten tai ammatillisten tarkoitusten vuoksi. Kyseisen palvelun käyttö voi olla suoraa, epäsuoraa tai välityksen kautta tapahtuvaa. Arvioidessaan vaikutusta, joka poikkeamalla voisi vakavuutensa ja kestonsa perusteella olla talouden ja yhteiskunnan toimintoihin tai yleiseen turvallisuuteen, jäsenvaltioiden olisi arvioitava myös aika, joka todennäköisesti kuluu, ennen kuin palvelun keskeytymisellä alkaisi olla kielteinen vaikutus* *Toimialojen välisten tekijöiden lisäksi olisi otettava huomioon myös toimialakohtaisia tekijöitä määritettäessä sitä, olisiko poikkeamalla merkittävä haitallinen vaikutus keskeisen palvelun tarjoamiseen. Energiantoimittajien osalta tällaisiin tekijöihin voisi sisältyä tuotetun kansallisen energian määrä tai osuus siitä; öljyntoimittajien osalta päiväkohtainen määrä; lentoliikenteen, mukaan lukien lentoasemat ja lentoliikenteen harjoittajat, sekä rautatieliikenteen ja merisatamien osalta osuus kansallisesta liikennemäärästä ja matkustajien tai rahtikuljetusten lukumäärä vuodessa; pankkialan tai finanssimarkkinoiden infrastruktuurien osalta niiden järjestelmäkohtainen merkitys perustuen kokonaisvaroihin tai näiden kokonaisvarojen ja bruttokansantuotteen suhteeseen; terveydenhuoltoalan osalta palvelun tarjoajan hoidossa olevien potilaiden lukumäärä vuo-*		

dessa; veden tuotannon, käsittelyn ja toimittamisen osalta vesimäärä sekä käyttäjien lukumäärä ja tyypit, mukaan lukien esimerkiksi sairaalat, julkiset palveluorganisaatiot tai henkilöt, sekä vaihtoehtoisten veden lähteiden olemassaolo saman maantieteellisen alueen kattamiseksi.	
Havaitut riskit	(6.1.a) Direktiivin antamat määritelmät ovat summittaisia eivätkä anna yksiselitteistä määritystä sille, miten merkittävä haitallinen poikkeama tunnistetaan. Tämä kasvattaa compliance-riskiä. Kansallisella toteutuksella on suuri merkitys siihen, miten riski realisoituu. (6.1.b) Mikäli yritys kasvaa nopeasti saattaa se täyttää nämä asiat, vaikka muuten ei kuuluisikaan direktiivin piriin. Sama saattaa tapahtua, mikäli ala on kausiluontoista tai muuten voimakkaasti vaihtelevaa. Riski, että yritykset eivät tunnista kuuluvansa direktiivin piiriin. (6.1.c) Mikäli määritys tulee voimassaolevien lakien alakohdaksi ja virastojen päätettäväksi (työryhmän ehdotus), voi olla edelleen vaikea arvioida onko yritys lain piirissä, ellei sitä selkeästi määritellä laissa. Eli jos osa lain tai viraston valvonnan alle kuuluvista on direktiivin piirissä ja osa ei.

14 artiklan 1 kohta		Vaikuttaa: Keskeiset toimijat
Jäsenvaltioiden on varmistettava, että keksisten palvelujen tarjoajat toteuttavat asianmukaiset ja oikeasuhteiset tekniset ja organisatoriset toimenpiteet hallitakseen riskejä, joita kohdistuu niiden verkko- ja tietojärjestelmien turvallisuuteen, joita nämä keskeisten palvelujen tarjoajat käyttävät toiminoissaan. Näillä toimenpiteillä on varmistettava riskiin suhteutettu verkko- ja tietojärjestelmien turvallisuuden taso uusin tekniikka huomioon ottaen.		
Havaitut riskit	(14.1.a) ’Asianmukaiset ja oikeasuhtaiset riskienhallinta toimenpiteet’ on laaja käsite ja sisältää riskin, että yritys ei tunnista viranomaisen vaatimaa tasoa ja joko yli-investoija tai ali-investoida. (14.1.b) Riski, että viranomaisella ja elinkeinonharjoittajalla on eri näkemys siitä, mikä on uusimman tekniikan taso. Tämä voi vaihdella suuresti, sillä kaikki kaupalliset ohjelmistot tai laitteistot eivät ole sopivia jokaiselle toimialalle käytettäviksi tai eivät kustannuksiltaan ole mahdollisia hankkia. (14.1.c) Mikäli organisatoriset toimenpiteet edellyttävät esimerkiksi verkko- ja tietojärjestelmäturvallisuuden osaajaa yritykseen, tulee osaajista olemaan pulaa, sillä jo nyt kysyntää on enemmän kuin tarjontaa kyberturvallisuuden osaajista. (Center for Strategic and International Studies 2016)	

14 artiklan 2 kohta		Vaikuttaa: Keskeiset toimijat

Jäsenvaltioiden on varmistettava, että keskeisten palvelujen tarjoajat toteuttavat asianmukaiset toimenpiteet, joilla ehkäistään ja minimoidaan tällaisten keskeisten palvelujen tarjoamisessa käytettyjen verkko- ja tietojärjestelmien turvallisuuteen vaikuttavien poikkeamien vaikutus näiden palvelujen jatkuvuuden takaamiseksi.	
Havaitut riskit	(14.2) Jotta poikkeamien vaikutuksia kyetään minimoimaan, on mahdolliset poikkeamat ja niiden mahdolliset vaikutukset ensin tunnistettava. Riski, että yritykset eivät tunnista poikkeamia ja yli- tai aliinvestoivat niiden ehkäisemiseen.

14 artiklan 3 kohta		Vaikuttaa: Keskeiset toimijat
Jäsenvaltion on varmistettava, että keskeisten palvelujen tarjoajat ilmoittavat ilman aiheetonta viivytystä toimivaltaiselle viranomaiselle tai CSIRT-toimijalle poikkeamista, joilla on merkittävä vaikutus niiden tarjoamien keskeisten palvelujen jatkuvuuteen. Ilmoituksiin on sisällytettävä tiedot, joiden perusteella toimivaltainen viranomainen tai CSIRT toimija voi määrittää poikkeaman mahdollisen rajat ylittävän vaikutuksen. Ilmoittaminen ei lisää ilmoituksen tekevän osapuolen vastuuta.		
Havaitut riskit	(14.3) Riski, että yritykset käyttävät enemmän aikaa ilmoituksen tekemiseen ja sitä kautta itse poikkeaman korjaaminen viivästyy. Pelkästään poikkeaman laajuuden analysointiin ja ilmoitusvelvollisuuden täyttymisen arviointiin voi kulua tarpeettoman paljon aikaa, mikäli ongelma ei ole etukäteen tunnettu. Aiheettoman viivytyksen määritelmä on epätarkka ja monitulkintainen, mikä kasvattaa compliance-riskiä.	

14 artiklan 4 kohta		Vaikuttaa: Keskeiset toimijat
Poikkeaman vaikutuksen merkittävyyden määrittämiseksi on otettava huomioon erityisesti seuraavat parametrit: a) niiden käyttäjien lukumäärä, joihin keskeisen palvelun häiriö vaikuttaa; b) poikkeaman kesto; c) maantieteellinen levinneisyys alueella, johon poikkeama vaikuttaa.		
Havaitut riskit	(14.4) Ilmoitusvelvollisuuden määritelmä on direktiivissä hyvin häilyvä ja vaikeasti tulkittava. Riski, että yritys jättää ilmoituksen tekemättä, koska se tulkitsee määritelmää eri tavalla kuin lain laatija.	

14 artiklan 6 kohta Resitaali 59		Vaikuttaa: Keskeiset toimijat

Kuultuaan ilmoituksen tehnyttä keskeisten palvelujen tarjoajaa toimivaltainen viranomainen tai CSIRT-toimija voi tiedottaa yleisölle yksittäisistä poikkeamista, jos yleinen tietoisuus on tarpeen poikkeaman estämiseksi tai käynnissä olevan poikkeaman käsittelemiseksi. *Toimivaltaisten viranomaisten olisi kiinnitettävä asianmukaista huomiota epävirallisten ja luotettavien tiedonjakokanavien säilyttämiseen. Toimivaltaisille viranomaisille raportoitujen poikkeamien julkistamisessa olisi otettava asianmukaisesti ja tasapainoisesti huomioon yleisön yleinen etu saada tietoa uhista sekä toisaalta poikkeamista raportoivien keskeisten palvelujen tarjoajien ja digitaalisen palvelun tarjoajien mahdollinen maineen vahingoittuminen ja niille mahdollisesti koituva taloudellinen vahinko. Ilmoitusvelvollisuuksien täytäntöönpanossa toimivaltaisten viranomaisten ja CSIRT-toimijoiden olisi kiinnitettävä erityistä huomiota tarpeeseen pitää tuotteiden haavoittuvuutta koskevat tiedot tiukasti luottamuksellisina ennen asiaankuuluvien turvallisuuspäivitysten julkistamista.*		
Havaitut riskit	(14.6) Tiedottamisvelvollisuus luo yritykselle maineriskin. Riski, on myös niissä tilanteissa, jolloin poikkeama ei kohdistu yritykseen itseensä, vaan johonkin toiseen saman alan toimijaan, mutta julkisuuteen kerrotaan vain toimiala, ei toimijaa.	

15 artiklan 2 kohta		Vaikuttaa: Keskeiset toimijat
Jäsenvaltioiden on varmistettava, että toimivaltaisilla viranomaisilla on valtuudet ja keinot pyytää keskeisten palvelujen tarjoajia a) antamaan tiedot, jotka tarvitaan niiden verkko- ja tietojärjestelmien turvallisuuden arvioimiseksi, mukaan lukien todennettavassa muodossa olevat turvallisuusohjeet; b) esittämään näyttöä turvallisuusohjeiden tosiasiallisesta täytäntöönpanosta, kuten toimivaltaisen viranomaisen tai pätevän tarkastajan suorittaman turvallisuustarkastuksen tulokset, ja viimeksi mainitussa tapauksessa antamaan turvallisuustarkastuksen tulokset, mukaan lukien niitä tukeva näyttö, toimivaltaisen viranomaisen käyttöön. Toimivaltaisen viranomaisen on tällaisia tietoja tai näyttöä pyytäessään ilmoitettava pyynnön tarkoitus ja täsmennettävä, mitä tietoja pyydetään.		
Havaitut riskit	(15.2) Riski, että turvallisuusohjeet luodaan ainoastaan sen takia, että direktiivi vaatii, eivätkä ne näin vastaa yrityksen todellisia tarpeita.	

15 artiklan 3 kohta		Vaikuttaa: Keskeiset toimijat
Toimivaltainen viranomainen voi 2 kohdassa tarkoitettujen tietojen tai turvallisuustarkastusten tulosten arvioinnin jälkeen antaa keskeisten palvelujen tarjoajille sitovia ohjeita havaittujen puutteiden korjaamiseksi.		

Havaitut riskit	(15.3) Sitovat ohjeet voivat luoda riskin yrityksen liiketoiminnalle, mikäli ne vaativat suuria muutoksia sen keskeisiin toimintoihin tai nykyiseen toimintamalliin. Lisäksi tällaiset määräykset tulevat usein julkisuuteen ja sitä kautta aiheuttavat maineriskin.

15 artiklan 4 kohta		Vaikuttaa: Keskeiset toimijat
Toimivaltaisen viranomaisen on toimittava tiiviisti yhteistyössä tietosuojaviranomaisten kanssa käsitellessään henkilötietojen tietoturvaloukkauksiin johtaneita poikkeamia.		
Havaitut riskit	(15.4) Mikäli NIS-direktiivin toimivaltaisen viranomaisen ja tietosuojaviranomaisen yhteistyö ei toimi, aiheutuu yritykselle tuplatyö ilmoittamisvelvollisuuden osalta, mikäli poikkeama vaarantaa henkilötietoja.	

16 artiklan 1 kohta Resitaali 49 Resitaali 60		Vaikuttaa: Digitaaliset toimijat
Jäsenvaltioiden on varmistettava, että digitaalisen palvelun tarjoajat määrittävät ja toteuttavat asianmukaiset ja oikeasuhteiset tekniset ja organisatoriset toimenpiteet hallitakseen riskejä, joita kohdistuu niiden verkko- ja tietojärjestelmien turvallisuuteen, joita nämä digitaalisen palvelun tarjoajat käyttävät tarjotessaan liitteessä III tarkoitettuja palveluja unionissa. Näillä toimenpiteillä on varmistettava riskiin suhteutettu verkko- ja tietojärjestelmien turvallisuuden taso uusin tekniikka huomioon ottaen, ja niissä on otettava huomioon seuraavat seikat: a) järjestelmien ja tilojen turvallisuus; b) poikkeamien käsittely; c) liiketoiminnan jatkuvuuden hallinta; d) seuranta, tarkastukset ja testaukset; e) kansainvälisten standardien noudattaminen. *Digitaalisen palvelun tarjoajien olisi varmistettava turvallisuuden taso, joka on oikeassa suhteessa niiden tarjoamien digitaalisten palvelujen turvallisuuteen kohdistuvan riskin suuruuteen, ottaen huomioon niiden palvelujen merkitys muiden yritysten toiminnalle unionissa. Käytännössä riskin suuruus on keskeisten palvelujen tarjoajille korkeampi kuin digitaalisen palvelun tarjoajille, koska keskeiset palvelut ovat usein olennaisia yhteiskunnan ja talouden kriittisten toimintojen ylläpitämiseksi. Näin ollen digitaalisen palvelun tarjoajia koskevien turvallisuusvaatimusten olisi oltava löyhempiä. Digitaalisen palvelun tarjoajilla olisi oltava vapaus toteuttaa toimenpiteet, jotka ne katsovat aiheellisiksi verkko- ja tietojärjestelmiensä turvallisuuteen kohdistuvien riskien hallitsemiseksi. Rajat ylittävän luonteensa vuoksi digitaalisen palvelun tarjoajiin olisi sovellettava yhdenmukaistetumpaa lähestymistapaa unionin tasolla. Tällaisten toimenpiteiden määrittämistä ja täytäntöönpanoa olisi helpotettava täytäntöönpanosäädöksillä.* *Digitaalisen palvelun tarjoajiin olisi sovellettava kevyitä ja reaktiivisia jälkikäteen toteutettavia valvontatoimia, jotka ovat perusteltavissa niiden palvelujen ja toiminnan luonteella. Asianomaisen toimivaltaisen viranomaisen olisi näin ollen ryhdyttävä toimiin ainoastaan silloin, kun sille esitetään näyttöä esimerkiksi digitaalisen palvelun tarjoajan itsensä, toisen toimivaltaisen viranomaisen, mukaan lukien toisen jäsenvaltion toimivaltainen viranomainen, tai palvelun käyttäjän toimesta siitä, että digitaalisen palvelun tarjoaja ei noudata tämän direktiivin vaatimuksia, etenkin poikkeaman jo tapahduttua. Toimivaltaisella viranomaisella ei siis pitäisi olla yleistä velvoitetta valvoa digitaalisen palvelun tarjoajia.*		

Havaitut riskit	(16.1) Direktiivi asettaa vaatimuksia digitaalisen palvelun tarjoajien toiminnalle, mutta koska vaatimukset eivät ole selkeästi määriteltyjä (”oikeasuhtaiset tekniset ja organisatoriset toimenpiteet”) niitä on vaikea noudattaa, mikä kasvattaa compliance-riskiä.

16 artiklan 2 kohta Resitaali 60 Resitaali 69		Vaikuttaa: Digitaaliset toimijat
Jäsenvaltioiden on varmistettava, että digitaalisen palvelun tarjoajat toteuttavat toimenpiteitä, joilla ehkäistään ja minimoidaan niiden verkko- ja tietojärjestelmien turvallisuuteen vaikuttavien poikkeamien vaikutus liitteessä III tarkoitettuihin unionissa tarjottuihin palveluihin, jotta voidaan taata näiden palvelujen jatkuvuus. *Digitaalisen palvelun tarjoajiin olisi sovellettava kevyitä ja reaktiivisia jälkikäteen toteutettavia valvontatoimia, jotka ovat perusteltavissa niiden palvelujen ja toiminnan luonteella. Asianomaisen toimivaltaisen viranomaisen olisi näin ollen ryhdyttävä toimiin ainoastaan silloin, kun sille esitetään näyttöä esimerkiksi digitaalisen palvelun tarjoajan itsensä, toisen toimivaltaisen viranomaisen, mukaan lukien toisen jäsenvaltion toimivaltainen viranomainen, tai palvelun käyttäjän toimesta siitä, että digitaalisen palvelun tarjoaja ei noudata tämän direktiivin vaatimuksia, etenkin poikkeaman jo tapahduttua. Toimivaltaisella viranomaisella ei siis pitäisi olla yleistä velvoitetta valvoa digitaalisen palvelun tarjoajia.* *Kun komissio hyväksyy täytäntöönpanosäädöksiä digitaalisen palvelun tarjoajia koskevista turvallisuusvaatimuksista, sen olisi otettava mahdollisimman tarkasti huomioon ENISAn lausunto sekä kuultava asianomaisia sidosryhmiä. Lisäksi komissiota kannustetaan ottamaan huomioon seuraavat esimerkit: järjestelmien ja tilojen turvallisuuden osalta: fyysinen turvallisuus ja ympäristön turvallisuus, toimitusvarmuus, verkko- ja tietojärjestelmiin pääsyn valvonta sekä verkko- ja tietojärjestelmien eheys; poikkeamien käsittelyn osalta: poikkeamien käsittelymenettelyt, poikkeamien havaitsemisvalmius, poikkeamista raportoiminen ja tiedottaminen; liiketoiminnan jatkuvuuden hallinnan osalta: palvelun jatkuvuutta koskeva strategia ja varautumissuunnitelmat, palautumisvalmiudet; ja seurannan, tarkastusten ja testausten osalta: seuranta- ja lokinpitomenettelyt, varautumissuunnitelmien läpiviennit, verkko- ja tietojärjestelmien testaus, turvallisuusarvioinnit ja vaatimustenmukaisuuden seuranta.*		
Havaitut riskit	(16.2) Jotta poikkeamien vaikutuksia kyetään minimoimaan, on mahdolliset poikkeamat ja niiden mahdolliset vaikutukset ensin tunnistettava. Riski, että yritykset eivät tunnista poikkeamia ja yli- tai ali-investoivat niiden ehkäisemiseen.	

16 artiklan 3 kohta		Vaikuttaa: Digitaaliset toimijat
Jäsenvaltioiden on varmistettava, että digitaalisen palvelun tarjoajat ilmoittavat toimivaltaiselle viranomaiselle tai CSIRT-toimijalle ilman aiheetonta viivytystä kaikista poikkeamista, joilla on merkittävä vaikutus sellaisen liitteessä III tarkoitetun palvelun tarjoamiseen, jota ne tarjoavat unionissa. Ilmoituksiin on sisällytettävä tiedot, joiden perusteella toimivaltainen viranomainen tai CSIRT-toimija voi määrittää mahdollisen rajat ylittävän vaikutuksen merkittävyyden. Ilmoittaminen ei lisää ilmoituksen tekevän osapuolen vastuuta.		

Havaitut riskit	(16.3) Riski, että yritykset käyttävät enemmän aikaa ilmoituksen tekemiseen ja sitä kautta itse poikkeaman korjaaminen viivästyy. Pelkästään poikkeaman laajuuden analysointiin ja ilmoitusvelvollisuuden täyttymisen arviointiin voi kulua tarpeettoman paljon aikaa, mikäli ongelma ei ole etukäteen tunnettu. Aiheettoman viivytyksen määritelmä on epätarkka ja monitulkintainen, mikä kasvattaa compliance-riskiä.

16 artiklan 4 kohta		Vaikuttaa: Digitaaliset toimijat
Sen määrittämiseksi, onko poikkeaman vaikutus merkittävä, on otettava huomioon erityisesti seuraavat parametrit: a) niiden käyttäjien lukumäärä, joihin poikkeama vaikuttaa, erityisesti niiden käyttäjien lukumäärä, jotka ovat riippuvaisia kyseessä olevasta palvelusta omien palvelujensa tarjoamiseksi; b) poikkeaman kesto; c) maantieteellinen levinneisyys alueella, johon poikkeama vaikuttaa; d) palvelun toiminnan häiriön laajuus; e) talouden ja yhteiskunnan toimintoihin kohdistuvan vaikutuksen laajuus. *Velvollisuutta ilmoittaa poikkeamasta sovelletaan ainoastaan, jos digitaalisen palvelun tarjoajalla on pääsy tietoihin, joita tarvitaan arvioitaessa poikkeaman vaikutusta suhteessa ensimmäisessä alakohdassa tarkoitettuihin parametreihin.*		
Havaitut riskit	(16.4) Ilmoitusvelvollisuuden määritelmä on direktiivissä hyvin häilyvä ja vaikeasti tulkittava. Riski, että yritys jättää ilmoituksen tekemättä, koska se tulkitsee määritelmää eri tavalla kuin lain laatija.	

16 artiklan 5 kohta		Vaikuttaa: Keskeiset toimijat Digitaaliset toimijat
Jos keskeisten palvelujen tarjoaja on riippuvainen kolmantena osapuolena olevasta digitaalisen palvelun tarjoajasta sellaisen palvelun tarjoamiseksi, joka on olennainen yhteiskunnan ja talouden kriittisten toimintojen ylläpitämiseksi, keskeisten palvelujen tarjoajan on ilmoitettava sellaisista merkittävistä vaikutuksista keskeisten palvelujen jatkuvuuteen, jotka johtuvat digitaalisen palvelun tarjoajaan vaikuttavasta poikkeamasta.		
Havaitut riskit	(16.5.a) Mahdollinen päällekkäinen ilmoitusvelvollisuus, sillä digitaalisen palvelun tarjoajalla on ilmoitusvelvollisuus samasta poikkeamasta, mikäli se on heidän kannaltaan merkittävä ja tämän mukaisesti myös keskeisten palvelujen tarjoajalle syntyy ilmoitusvelvollisuus samaisesta poikkeamasta. Riski, että aika menee ilmoitusvelvollisuuksien hoitamiseen poikkeaman korjaamisen sijaan. (16.5.b) Direktiivi ei itsessään velvoita digitaalisen palvelun tarjoajaa tiedottamaan poikkeamasta keskeisten palvelujen tarjoajalle, joten tästä täytyy erikseen sopimuksellisesti sopia.	

16 artiklan 6 kohta Resitaali 41		Vaikuttaa:

		Digitaaliset toimijat
Toimivaltaisen viranomaisen tai CSIRT-toimijan on tarvittaessa ja erityisesti silloin, kun 3 kohdassa tarkoitettu poikkeama koskee kahta tai useampaa jäsenvaltiota, tiedotettava asiasta muille asiaan liittyville jäsenvaltioille. Näin tehdessään toimivaltaisten viranomaisten, CSIRT-toimijoiden ja keskitettyjen yhteyspisteiden on unionin oikeuden tai unionin oikeuden mukaisen kansallisen lainsäädännön mukaisesti säilytettävä digitaalisen palvelun tarjoajan turvallisuusedut ja kaupalliset edut sekä annettujen tietojen luottamuksellisuus. *Jos tietoja pidetään luottamuksellisina liikesalaisuuksia koskevien unionin ja kansallisten sääntöjen mukaisesti, tällainen luottamuksellisuus olisi varmistettava tässä direktiivissä säädettyjen toimien ja tavoitteiden toteuttamisen yhteydessä.*		
Havaitut riskit	(16.6) Kun tietoja jaetaan uusille tahoille, lisää se riskiä tiedon joutumisesta vääriin käsiin tai julkisuuteen, joko tahallisesti tai vahingossa. Riippuen tiedon laadusta voi se aiheuttaa haittaa joko maineelle tai liiketoiminnalle.	

16 artiklan 7 kohta Resitaali 59		Vaikuttaa: Digitaaliset toimijat
Kuultuaan kyseessä olevaa digitaalisen palvelun tarjoajaa toimivaltainen viranomainen tai CSIRT-toimija ja tarvittaessa muiden asiaankuuluvien jäsenvaltioiden viranomaiset tai CSIRT-toimijat voivat tiedottaa yleisölle yksittäisistä poikkeamista tai vaatia digitaalisen palvelun tarjoajaa tekemään niin, jos yleinen tietoisuus on tarpeen poikkeaman estämiseksi tai käynnissä olevan poikkeaman käsittelemiseksi tai jos poikkeaman ilmaiseminen on muutoin yleisen edun mukaista. *Toimivaltaisten viranomaisten olisi kiinnitettävä asianmukaista huomiota epävirallisten ja luotettavien tiedonjakokanavien säilyttämiseen. Toimivaltaisille viranomaisille raportoitujen poikkeamien julkistamisessa olisi otettava asianmukaisesti ja tasapainoisesti huomioon yleisön yleinen etu saada tietoa uhista sekä toisaalta poikkeamista raportoivien keskeisten palvelujen tarjoajien ja digitaalisen palvelun tarjoajien mahdollinen maineen vahingoittuminen ja niille mahdollisesti koituva taloudellinen vahinko. Ilmoitusvelvollisuuksien täytäntöönpanossa toimivaltaisten viranomaisten ja CSIRT-toimijoiden olisi kiinnitettävä erityistä huomiota tarpeeseen pitää tuotteiden haavoittuvuutta koskevat tiedot tiukasti luottamuksellisina ennen asiaankuuluvien turvallisuuspäivitysten julkistamista.*		
Havaitut riskit	(16.7) Tiedottamisvelvollisuus luo yritykselle maineriskin. Riski, on myös niissä tilanteissa, jolloin poikkeama ei kohdistu yritykseen itseensä, vaan johonkin toiseen saman alan toimijaan, mutta julkisuuteen kerrotaan vain toimiala, ei toimijaa.	

17 artiklan 1 kohta		Vaikuttaa: Digitaaliset toimijat
Jäsenvaltioiden on varmistettava, että toimivaltaiset viranomaiset ryhtyvät tarvittaessa toimiin panemalla täytäntöön jälkikäteen toteutettavia valvontatoimenpiteitä, kun niille esitetään näyttöä siitä, että digitaalisen palvelun tarjoaja ei täytä 16 artiklassa säädettyjä vaatimuksia. Tällaisen näytön voi esittää sellaisen toisen jäsenvaltion toimivaltainen viranomainen, jossa palvelua tarjotaan.		
Havaitut riskit	(17.1) Compliance riski. Mikäli yrityksen toiminnot eivät vastaa viranomaisen tulkintaa kyseisestä pykälästä kohtaavat he kurinpitomenettelyn.	

17 artiklan 2 kohta		Vaikuttaa:

		Digitaaliset toimijat
Edellä olevaa 1 kohtaa sovellettaessa toimivaltaisilla viranomaisilla on oltava tarvittavat valtuudet ja keinot vaatia, että digitaalisen palvelun tarjoajat a) antavat niiden verkko- ja tietojärjestelmien turvallisuuden arvioimiseksi tarvittavat tiedot, mukaan lukien todennettavassa muodossa olevat turvallisuusohjeet; b) korjaavat mahdolliset puutteet 16 artiklassa säädettyjen vaatimusten täyttämisessä.		
Havaitut riskit	(17.2) Riski, että turvallisuusohjeet luodaan ainoastaan sen takia, että direktiivi vaatii, eivätkä ne näin vastaa yrityksen todellisia tarpeita.	

17 artiklan 3 kohta		Vaikuttaa: Digitaaliset toimijat
Jos digitaalisen palvelun tarjoajan pääasiallinen toimipaikka tai edustaja on jäsenvaltiossa mutta sen verkko- ja tietojärjestelmät sijaitsevat yhdessä tai useammassa muussa jäsenvaltiossa, pääasiallisen toimipaikan tai edustajan jäsenvaltion toimivaltaisen viranomaisen ja näiden muiden jäsenvaltioiden toimivaltaisten viranomaisten on tehtävä yhteistyötä ja avustettava toisiaan tarpeen mukaan. Tällaiseen avustamiseen ja yhteistyöhön voivat sisältyä tiedonvaihto asianomaisten toimivaltaisten viranomaisten välillä sekä pyynnöt 2 kohdassa tarkoitettujen valvontatoimenpiteiden toteuttamiseksi.		
Havaitut riskit	(17.3) Kun tietoja jaetaan uusille tahoille, lisää se riskiä tiedon joutumisesta vääriin käsiin tai julkisuuteen, joko tahallisesti tai vahingossa. Riippuen tiedon laadusta voi se aiheuttaa haittaa joko maineelle tai liiketoiminnalle.	

18 artiklan 2 kohta 18 artiklan 3 kohta Resitaali 65		Vaikuttaa: Digitaaliset toimijat
Digitaalisen palvelun tarjoajan, joka ei ole sijoittautunut unioniin mutta joka tarjoaa liitteessä III tarkoitettuja palveluja unionissa, on nimettävä edustaja unionin aluetta varten. Edustajan on oltava sijoittautunut johonkin niistä jäsenvaltioista, joissa palveluja tarjotaan. Digitaalisen palvelun tarjoajan katsotaan kuuluvan sen jäsenvaltion lainkäyttövallan piiriin, johon edustaja on sijoittautunut. *Se, että digitaalisen palvelun tarjoaja on nimennyt edustajan, ei rajoita oikeustoimia, joita voidaan panna vireille digitaalisen palvelun tarjoajaa itseään vastaan.* *Jos digitaalisen palvelun tarjoaja, joka ei ole sijoittautunut unioniin, tarjoaa palveluja unionissa, sen olisi nimettävä edustaja. Jotta voidaan määrittää, tarjoaako tällainen digitaalisen palvelun tarjoaja palveluja unionissa, olisi varmistettava, onko ilmeistä, että digitaalisen palvelun tarjoaja aikoo tarjota palveluja henkilöille yhdessä tai useammassa jäsenvaltiossa. Pelkkä digitaalisen palvelun tarjoajan tai välittäjän verkkosivuston tai sähköpostiosoitteen ja muiden yhteystietojen saatavuus unionissa taikka se, että käytetään siinä kolmannessa maassa, johon digitaalisen palvelun tarjoaja on sijoittautunut, yleisesti käytettävää kieltä, ei riitä tällaisen aikomuksen varmistamiseksi. Sellaiset seikat, kuten yhdessä tai useammassa jäsenvaltiossa yleisesti käytettävän kielen tai rahayksikön käyttö ja mahdollisuus tilata palveluja kyseisellä muulla kielellä tai maininta unionissa olevista asiakkaista tai käyttäjistä, voivat kuitenkin osoittaa olevan ilmeistä, että digitaalisen palvelun tarjoaja aikoo tarjota palveluja unionissa. Edustajan olisi toimittava digitaalisen palvelun tarjoajan puolesta, ja toimivaltaisten viranomaisten tai CSIRT-toimijoiden olisi voitava ottaa yhteyttä edustajaan. Edustaja olisi nimenomaisesti nimettävä digitaalisen palvelun tarjoajan antamalla kirjallisella valtuutuksella hoitamaan tämän puolesta tämän direktiivin mukaiset velvollisuudet, mukaan lukien poikkeamista raportointi.*		
Havaitut riskit	(18.2) Myös EU:n ulkopuolisten digitaalisten palvelun tarjoajien täytyy arvioida kuulumisensa direktiivin piiriin, mikäli heillä on asiakkaita EU:n alueella. Direktiivi luo heille compliance-riskin.	

21 artikla		Vaikuttaa: Keskeiset toimijat Digitaaliset toimijat
Jäsenvaltioiden on säädettävä tämän direktiivin nojalla annettujen kansallisten säännösten rikkomiseen sovellettavista seuraamuksista ja toteutettava kaikki tarvittavat toimenpiteet sen varmistamiseksi, että ne pannaan täytäntöön. Säädettyjen seuraamusten on oltava tehokkaita, oikeasuhteisia ja varoittavia. Jäsenvaltioiden on annettava komissiolle tiedoksi nämä säännökset ja toimenpiteet viimeistään 9 päivänä toukokuuta 2018 ja ilmoitettava sille niihin vaikuttavista myöhemmistä muutoksista viipymättä.		
Havaitut riskit	(21) Sanktiot ovat osa compliance-riskiä. Mikäli lain noudattamatta jättämisellä ei ole mitään seuraamuksia, siihen liittyvä riski on myöskin vähäinen.	