JYU DISSERTATIONS 224

Tiina Vestman

Kriittinen analyysi neutralisoimisteorian soveltamisesta tietojärjestelmätieteessä

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION TECHNOLOGY

JYU DISSERTATIONS 224

Tiina Vestman

Kriittinen analyysi neutralisoimisteorian soveltamisesta tietojärjestelmätieteessä

Esitetään Jyväskylän yliopiston informaatioteknologian tiedekunnan suostumuksella
julkisesti tarkastettavaksi kesäkuun 5. päivänä 2020 kello 12.

Academic dissertation to be publicly discussed, by permission of
the Faculty of Information Technology of the University of Jyväskylä,
on June 5, 2020 at 12 o'clock noon.

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2020

Editors
Marja-Leena Rantalainen
Faculty of Information Technology, University of Jyväskylä
Ville Korkiakangas
Open Science Centre, University of Jyväskylä

Permanent link to this publication: http://urn.fi/URN:ISBN:978-951-39-8174-7

ISBN 978-951-39-8174-7 (PDF)
URN:ISBN:978-951-39-8174-7
ISSN 2489-9003

ABSTRACT

Vestman, Tiina
A Critical Analysis of the Application of Neutralization Theory in Information Systems Science
Jyväskylä: University of Jyväskylä, 2020, 170 p.
(JYU Dissertations,
ISSN 2489-9003; 224)
ISBN 978-951-39-8174-7 (PDF)

Technology development, the internet and digitalization have changed all of our lives during the last few decades. Information security is often seen as a purely technology-driven issue. However, technology alone cannot provide the perfect solution for securing and protecting critical information in an organization. Often the biggest security trouble sits between the keyboard and the chair. This thesis exams information security from an employees' viewpoint. It focuses on non-compliance with employee security policies and security breaches. The thesis explores factors that affect an individual's security behavior and discusses the underlying conditions that lead to an employee's security policy non-compliance and security breaches. The main task of this thesis is to present the revised neutralization theory in the security context and to examine how employees explain their non-compliance with the security policy. The theory of neutralization, published by Sykes and Matza in 1957 has given the theoretical basis for this thesis. The theory has driven the development of the interviews and provided a baseline for the analysis of research data. The central argument of the Neutralization Theory is that man justifies his deviant behavior by means of neutralization techniques and thus avoids feelings of guilt and shame. Previous researches have suggested that the Neutralization Theory can explain intentions of information security violations or breaches. However, the researches have not applied the central assumptions of Neutralization Theory, and so it cannot be clear whether it can explain security behavior. The theoretical contribution of this thesis is to introduce new information from employees' accounts and how they explain their non-compliance with information security policies. Scott and Lyman's (1968) Accounts-article has been applied in this thesis, which has been influenced by the theory of neutralization. A practical contribution of this thesis is to look at what everyday situations can be risky from the security perspective and provide solutions that can be utilized in the security management. The result of this thesis supports the claim that employees do not necessarily utilize the neutralization techniques to justify their security breaches.

Keywords: neutralization theory, techniques of neutralization, information security, information security policy, information security violation, social norms, social control

TIIVISTELMÄ

Vestman, Tiina
Kriittinen analyysi neutralisoimisteorian soveltamisesta tietojärjestelmätieteessä
Jyväskylä: University of Jyväskylä, 2020, 170 p.
(JYU Dissertations,
ISSN 2489-9003; 224)
ISBN 978-951-39-8174-7 (PDF)

Teknologian kehitys, internet ja digitalisaatio ovat viime vuosikymmeninä muuttaneet meidän jokaisen elämää. Vaikka tietoturvaa usein pidetään vain teknisenä asiana, ei pelkkä teknologia yksin pysty turvaamaan ja suojaamaan organisaation kriittisiä tietoja. Usein suurin tietoturvaongelma istuukin näppäimistön ja tuolin välissä. Tässä tutkimuksessa tietoturvaa tarkastellaan työntekijöiden näkökulmasta, keskittyen työntekijöiden tietoturvapolitiikan noudattamattomuuteen sekä tietoturvarikkomuksiin.

Tutkimus keskittyy tietoturvakäyttäytymiseen ja pyrkii ymmärtämään lähtökohtia, jotka johtavat työntekijän tietoturvapolitiikan noudattamattomuuteen ja tietoturvarikkomuksiin. Tutkimusaineiston keräystapana on käytetty teemahaastatteluita. Tutkimuksen päätehtävänä on esittää revisioitu neutralisoimisteoria tietoturvakontekstiin ja tarkastella, miten työntekijät selittävät ja perustelevat tietoturvapolitiikan noudattamattomuutta. Tutkimuksen teoreettisena lähtökohtana toiminutta Sykes ja Matzan vuonna 1957 julkaisemaa neutralisoimisteoriaa on käytetty ohjaamaan aiempien, saman aihepiirin tutkimusten tarkastelua, haastatteluiden teemoja ja tutkimusaineiston analyysiä. Neutralisoimisteorian keskeinen väittämä on, että ihminen oikeuttaa normeista poikkeavan käyttäytymisensä neutralisoimistekniikoiden avulla ja välttyy näin syyllisyydeltä ja häpeältä. Aiemmat tutkimukset ovat esittäneet neutralisoimisteorian selittävän tietoturvarikkomuksia, mutta eivät ole huomioineet neutralisoimisteorian keskeisiä olettamuksia eikä siten voi olla selvää, pystyykö neutralisoimisteoria selittämään tietoturvakäyttäytymistä.

Tutkimuksen teoreettisena kontribuutiona on tuoda uutta tietoa työntekijöiden tietoturvarikkomusten selonteoista. Näiden selontekojen tarkastelussa on sovellettu Scottin ja Lymanin (1968) neutralisoimisteoriasta vaikutteita saanutta Accounts-nimistä artikkelia. Tutkimuksen käytännön kontribuutiona on tarkastella, millaiset arkipäiväiset tilanteet voivat olla tietoturvan näkökulmasta riskialttiita sekä tarjota ratkaisuja, joita voidaan hyödyntää tietoturvajohtamisessa. Tutkimustulos tukee väitettä, etteivät työntekijät välttämättä hyödynnä neutralisoimisteoriassa esitettyjä neutralisoimistekniikoita ja oikeuta niiden avulla tietoturvarikkomuksiaan.

Asiasanat: neutralisoimisteoria, tietoturvallisuus, tietoturvarikkomus, sosiaalinen normi, normista poikkeaminen, sosiaalinen kontrolli

Author

Tiina Vestman
Faculty of Information Technology
University of Jyväskylä
Finland

Supervisor

Professor Mikko Siponen
Faculty of Information Technology
University of Jyväskylä
Finland

Reviewers

Professor Rauno Kuusisto
Finnish Defence Research Agency
Finland

Docent Teemupekka Virtanen
The Ministry of Social Affairs and Health
Finland

Opponent

Professor Netta Iivari
Faculty of Information Technology
and Electrical Engineering
University of Oulu
Finland

KIITOKSET

Sanotaan, ettei innostumiseen tarvita kuin uteliasta mieltä, uutteraa panostamista ja kykyä nauttia ja iloita pienistä saavutuksista. Jotain vastaavaa uteliaisuutta ja kiinnostusta tietoturvaa kohtaan on vaadittu tämänkin tutkimuksen tekemiseen. Väitöskirja on jatkoa pro gradu –tutkimukselleni. Pro gradu –tutkimus tuntui jääneen keskeneräiseksi, mutta nyt tutkimus on valmis ja on aika kiittää heitä, jotka edesauttoivat työn valmistumisessa.

Erityiskiitokseni kuuluvat väitöskirjani ohjaajalle, professori Mikko Siposelle. Hänen vankka asiantuntijuutensa tieteellisen tutkimuksen tekemiseen sekä kannustava ja eteenpäin vievä tapansa ohjata varmistivat työn valmistumisen. Olen kiitollinen, että sain aina ohjausta, kun sitä tarvitsin, ja sain oppia tarkastelemaan asioita kriittisesti. Professori Siposelle kuuluu myös kiitos kontaktista professori Volkan Topalliin, joka avasi näkemään tutkimuksen keskeisestä teoriasta erilaisia näkökulmia. Kiitän väitöskirjani esitarkastajia, professori Rauno Kuusistoa ja dosentti Teemupekka Virtasta heidän arvokkaista huomioistaan ja näkemyksistään, rakentavasta kritiikistään ja havainnollistavista kommenteistaan.

Kiitän Jyväskylän yliopiston informaatioteknologian tiedekunnan tohtorikoulua siitä taloudellisesta tuesta, joka mahdollisti lähes vuoden yhtäjaksoisen keskittymisen vain tutkimustyöhön.

Jatko-opintoihin liittyvästä vertaistuesta haluan kiittää Martti Karia. Kiitos Martti kaikista keskusteluista ja neuvoista sekä hyvistä tarinoista.

Jukka Mäki-Kuhnaa haluan kiittää hänen opastuksestaan ja neuvostaan kilpailevien hypoteesien analyysimenetelmää koskien. Englanninkieliseen tiivistelmään sain tukea Kyle Thompsonilta. Thanks a lot Kyle somewhere out there in the United States! Saana Näreahoa haluan kiittää avusta englanninkielisen yhteenvedon oikoluvussa.

Kiitos nykyiselle työyhteisölleni kiinnostuksesta tutkimustani kohtaan sekä myönteisestä ja kannustavasta suhtautumisesta työn ohella opiskeluun. Keskustelut työkavereiden kanssa ovat rikastuttaneet elämääni monella tavoin.

Kiitän tutkimukseen osallistuneita organisaatioita heidän myönteisestä suhtautumisestaan tutkimustani kohtaan. Kiitos Teille kaikille korvauksetta tutkimukseen osallistuneille haastateltaville. Teidän jokaisen kokemukset, ajatukset, tunteet ja uskomukset ovat arvokkaita ja tärkeitä.

Lämpimät kiitokseni kuuluvat myös teille, J ja A, jotka olitte tavalla tai toisella taustatukenani tutkimuksen alusta loppuun saakka. Ilman taustatukeanne olisi moni arvokas näkökulma jäänyt puuttumaan.

Kiitos ystäväni Päivi, Sari, Anne, Tarja ja Pia sekä sisarukseni Virpi ja Petrus, jotka jaksoitte ihmettelemättä vastailla välillä mitä kummallisimpiin kysymyksiini ja pohdintoihini, jotka eivät välttämättä liittyneet tutkimukseeni mitenkään. Välillä on ollut hyvä tuulettaa aivoja tutkimuksesta ja keskustella jostain ihan muusta.

Suurimmat kiitokseni kuuluvat Viljalle ja Juhalle. Kiitos Vilja kannustuksesta tutkimustyötäni kohtaan sekä avustasi englanninkielisen tiivistelmän oikoluvussa. Vilja, olet kasvanut itseohjautuvaksi nuoreksi ja toivon voivani olla sinulle esikuvana edes jossain määrin. Kiitos Juha kaikesta siitä, miten olet tukenut minua ja tekemiäni valintoja elämässä. Olemassa olonne muistuttaa siitä, mikä on elämässä tärkeintä. Kiitos teidän vankkumattomasta uskosta (joka ajoittain oli suurempi kuin itselläni), että tämä väitöskirja on jonain päivänä valmis.

Jyväskylässä 2.5.2020
Tiina Vestman

KUVIOT

KUVIO 1 Tutkimuksen kokonaisasetelma 15
KUVIO 2 Tietoturvallisuuden kulmakivet 38
KUVIO 3 Haastatteluiden keskeiset teemat 99

TAULUKOT

TAULUKKO 1 Aiempien tutkimusten kooste 56
TAULUKKO 2 Tutkimuksissa huomioidut alkuperäisen teorian neutralisoimistekniikat 63
TAULUKKO 3 Tutkimuksissa huomioidut muut neutralisoimistekniikat 64
TAULUKKO 4 Sykes ja Matzan alkuperäisen teorian keskeiset väittämät 65
TAULUKKO 5 Suorat lainaukset aiemmista tutkimuksista sanalle "neutralisointi" 67
TAULUKKO 6 Bauer & Bernroider (2017) artikkelin mittauskohteet 76
TAULUKKO 7 Cheng ym., (2014) artikkelin mittauskohteet 77
TAULUKKO 8 Haag & Eckhardt (2015) artikkelin mittauskohteet 79
TAULUKKO 9 Haag ym., artikkelin (2015) mittauskohteet 80
TAULUKKO 10 Khansa ym., (2017) artikkelin mittauskohde 80
TAULUKKO 11 Li ja Cheng (2013) artikkelin mittauskohteet 81
TAULUKKO 12 Silic ym., (2017) artikkelin mittauskohteet 83
TAULUKKO 13 Siponen & Vance (2010) artikkelin mittauskohteet 83
TAULUKKO 14 Siponen ym., (2020) artikkelin mittauskohteet 85
TAULUKKO 15 Eisenhardin teorianmuodostusprosessi 95
TAULUKKO 16 ACH analyysin kahdeksan vaihetta 168
TAULUKKO 17 Mallia analyysin ensimmäisestä vaiheesta 169

SISÄLLYS

ABSTRACT
TIIVISTELMÄ
KIITOKSET
KUVIOT JA TAULUKOT
SISÄLLYS

1 JOHDANTO ... 11
1.1 Tutkimuksen lähtökohdat ... 11
1.2 Tutkimuksen tarkoitus ... 14
1.3 Aiheen valinnan perustelu ... 16
1.4 Tutkimuksen keskeiset käsitteet ... 18
1.5 Tutkimuksen rakenne ... 19

2 TEOREETTISET LÄHTÖKOHDAT ... 20
2.1 Neutralisoimisteorian perusta ja väitteet ... 20
2.2 Poikkeavuuden oikeutus ... 23
2.2.1 Vastuun kieltäminen ... 25
2.2.2 Vahingon kieltäminen ... 27
2.2.3 Uhrin kieltäminen ... 28
2.2.4 Tuomitsijoiden tuomitseminen ... 29
2.2.5 Vetoaminen korkeampiin lojaliteetteihin ... 29
2.3 Neutralisoimisteorian soveltaminen ... 31
2.4 Neutralisoimisteoriaan liittyvää kritiikkiä ... 32
2.5 Tutkimusten haasteet ... 34

3 TUTKIMUKSEN KESKEISET KÄSITTEET ... 36
3.1 Tietoturva ... 36
3.2 Tietoturvapolitiikka ... 40
3.3 Tietoturvakäyttäytyminen ... 42
3.4 (Sosiaalinen) normi ... 44
3.5 (Sosiaalisesta) normista poikkeaminen ... 47
3.6 Sosiaalinen kontrolli ja sosiaalinen järjestys ... 49
3.7 Tietoturvarikkomus ... 50
3.8 Selonteot: pahoitteleva ja oikeuttava ... 51
3.9 Tietoturvakulttuuri ... 53

4 AIEMMAT TUTKIMUKSET ... 55
4.1 Aihepiirin aiemmat tutkimukset ... 55
4.2 Aiempien tutkimusten tulkinnat ... 66
4.2.1 Neutralisointi ... 66
4.2.2 Neutralisoimisteoria ... 70
4.2.3 Muita olettamuksia ... 72
4.2.4 Tutkimustuloksia ... 74
4.3 Neutralisoimisteoriaa testaavat kysymykset ... 75

5 TUTKIMUSMENETELMÄ, AINEISTON HANKINTA JA ANALYYSI .. 88
5.1 Metodologiset lähtökohdat ... 88
5.2 Kvalitatiivisen tutkimusotteen mahdollisuudet ... 89
5.3 Tapaustutkimus ... 90
5.4 Tapaustutkimuksen kritiikki ja sen puolustus ... 92
5.5 Teoriaa rakentava tapaustutkimus ... 93
5.6 Tutkimuksen aineisto ... 96
5.6.1 Tutkimukseen osallistuneet organisaatiot ... 96
5.6.2 Haastatteluaineisto ... 97
5.7 Haastatteluiden haasteet ja toteutus ... 99
5.8 Aineiston analysointi ... 102

6 NEUTRALISOIMISTEORIAN TULKINTA TIETOTURVAKONTEKSTISSA ... 105
6.1 Yhdenmukaisuuden vaatimus ... 105
6.1.1 Sitoutuminen ... 106
6.1.2 Tietoturvapolitiikan merkitys ... 108
6.2 Asenne ... 112
6.3 Perustelu ... 113
6.3.1 Vastuun kieltäminen *("En tarkoittanut sitä")* ... 114
6.3.2 Vahingon kieltäminen *("En vahingoittanut ketään")* ... 117
6.3.3 Uhrin kieltäminen *("Siitäs saivat")* ... 119
6.3.4 Tuomitsijoiden tuomitseminen *("Kaikki kiusaavat minua")* ... 120
6.3.5 Vetoaminen korkeampiin lojaliteetteihin *("En tehnyt sitä itseni vuoksi")* ... 123
6.3.6 Oppiminen ... 126
6.3.7 Ennen vai jälkeen oikeuttaminen ... 127
6.3.8 Uskomukset vs toiminta ... 128
6.4 Selonteot ... 131
6.4.1 Miten? ... 133
6.4.2 Miksi? ... 136

7 KESKUSTELU ... 139
7.1 Tulosten merkitys ja suhteutus ... 139
7.2 Keskustelu käytännön kannalta ... 142
7.3 Tutkimuksen rajoitteet ... 145
7.4 Luotettavuus ja pätevyys ... 146
7.5 Tuleva tutkimus ... 149

8 YHTEENVETO ... 151

SUMMARY ... 153

LÄHTEET ... 155

LIITE 1 ... 168

1 JOHDANTO

1.1 Tutkimuksen lähtökohdat

Uutiskynnyksen ylittäviä tietovuotoja, tietomurtoja, palvelunestohyökkäyksiä ja kyberhyökkäyksiä voi lukea eri medioista lähes päivittäin (kts. esim. Joensuu, 2019; Suomen poliisi, 2019). Siinä missä esimerkiksi yhden kyberhyökkäyksen torjunta voi aiheuttaa lähes miljoonan euron kustannukset (Niemi, 2019), saattaa luottamuksellisten asiakirjojen luovutus vaikuttaa jopa kansalliseen turvallisuuteen (Tasavallan presidentin kanslia, 2017). Valitettavan arkipäiväisempiä esimerkkejä, mutta potentiaalisesti ketä tahansa koskettavia, ovat esimerkiksi hoito- tai muun henkilökunnan tekemät, muihin kuin virka-, työ-, tai palvelussuhteeseen liittyvät, luottamuksellisten tietojen urkinnat tai luovuttamiset (kts. esim Surakka, 2017; Surakka, 2018; Surakka, 2019; Savolainen, 2019). Edellä mainittujen rikosten yhteiskunnallisia seurauksia tai kokonaiskustannuksia on hankala arvioida, koska kustannukset saattavat sisältää organisaation arkaluonteisten tietojen, järjestelmätietojen, tekijänoikeudella suojattujen materiaalien ja luokiteltujen tietojen (Nicho & Kamoun, 2014) lisäksi myös mahdollisen yksilön kokeman pitkäkestoisen inhimillisen kärsimyksen.

Myös tietoturvarikkomusten yhteiskunnallisia kokonaiskustannuksia on vaikea arvioida. Vaikka muun muassa Viestintävirasto (2018) arvio organisaatioiden lisäävän avoimuuttaan kokemistaan tietoturvauhkista, vain harva organisaatio tuo julki työntekijöidensä tietoturvarikkomusten aiheuttamat välilliset tai välittömät kustannukset, koska ne luokitellaan asianomistajarikoksiksi, jolloin asianomistajalla on aloiteoikeus syytteen nostamiseen (Finlex, 2007). ENISAn (2019) julkaisemassa niin sanotussa uhkamaisemaraportissa (engl. *threat landscepe*) organisaatioiden sisäpiiririski jatkaa edelleenkin vuodesta toiseen yhtenä merkittävänä uhkatekijänä. Raportissa tahallisen toiminnan lisäksi merkittävänä riskinä mainitaan huolimattomuus, tietoturvapolitiikan ja –ohjeiden noudattamattomuus, mutta tahatonkin toiminta voi mahdollistaa keinot erilaisten

tieto- ja kyberturvaloukkausten toteuttamiseksi (ENISA, 2019, 69-71). Tutkijoiden arvion mukaan lähes puolet tietoturvaloukkauksista tapahtuu organisaation sisäpuolelta (Crossler, Johnston, Lowry, Hu, Warkentin & Baskerville, 2013, 90).

Teknologian kehitys, internet ja digitalisaatio ovat muuttaneet viime vuosikymmenen aikana yhteiskunnan, elinkeinoelämän ja kansalaisten tapaa toimia. Internetin sanotaankin muodostuneen kriittiseksi infrastruktuuriksi (Valtioneuvosto, 2009), jota ilman monet toiminnot eivät yksinkertaisesti olisi enää mahdollisia (Safa ym., 2015). Enenevässä määrin lisääntyvä teknologian hyödyntäminen asettaa kuitenkin myös haasteita muun muassa luottamuksellisten tietojen käsittelyyn ja suojaamiseen. Riippuvuus tietojärjestelmistä tekee eri organisaatioiden toiminnan myös erittäin haavoittuvaiseksi ja lisääntyvä riippuvuus lisää myös tarvetta ymmärtää ja käsitellä tietojenkäsittely-ympäristöön liittyviä riskejä (Warkentin & Willison, 2009, 101). Vaikka organisaation ulkopuoliset tietoturvauhkat ja tekniset tietoturvaratkaisut näiden ulkoisten uhkien torjumiseen ovat erittäin tärkeitä tutkimusaiheita, yhtä lailla organisaation työntekijät voivat muodostaa uhkan muun muassa vuotamalla organisaation luottamuksellisia asiakirjoja tai tietoja kilpailijalle tai muutoin julkisuuteen.

Huolimatta teknologian jatkuvasta kehityksestä, pelkkä teknologia yksin ei pysty tuottamaan katastrofin kestävää toimivuutta, eikä tekniikka yksin välttämättä pysty tuottamaan täydellistä ratkaisua organisaation kriittisten tietojen turvaamiseen ja suojaamiseen (Siponen ym., 2008; Furnell & Clarke, 2012). Kokonaisvaltaisessa tietoturvastrategissa laitteiston (engl. *hardware*), ohjelmiston (engl. *software*) ja laiteohjelmiston (engl. *firmware*) ohessa myös niin sanottu ”*wetware*”, eli tietojenkäsittelyn inhimillinen elementti, on kriittinen osa kokonaisuutta (Peltier, 2006, 14). Tietoturvauhkat eivät siis kohdistu yksinomaan organisaation tekniseen infrastruktuuriin, vaan haavoittuvuudet syntyvät sosioteknisessä ympäristössä (Furnell & Clarke, 2012; Dhillon ym., 2016). Usein sanotaankin, että ihminen on tietoturvan heikoin lenkki (Bulgurcu ym., 2010; Peltier, 2006, 14; Vacca, 2014, 17; Warkentin & Willison, 2009, 102). Ulkopuolisten niin sanottujen hakkereiden lisäksi virheelliset tai huolimattomat toimintatavat voivat muodostua uhkaksi organisaation tietoturvalle, mutta näiden lisäksi myös luotettavana pidetty työntekijä saattaa pettää koko järjestelmän (Peltier, 2014).

Usein suurin tietoturvaongelma istuukin näppäimistön ja tuolin välissä (Warkentin & Willison, 2009, 102), joten työntekijöiden asenteet ja toiminta ovat kasvaneet yhä merkittävämmäksi tekijäksi tietoturvallisuudessa (Iivonen, 2011, 148; Siponen ym., 2014; D'Arcy ym., 2009). Tutkimukset ovat osoittaneet, että tietoturvarikkomusten, joko tahallisten tai tahattomien, seuraukset voivat olla erittäin vahingollisia. Täysin selvää ei myöskään ole niin sanottujen pienten ja suurten tietoturvarikkomusten välinen ero sekä rikkomusten aikaan saamien seurausten vaikutukset. (Siponen & Vance, 2010; Crossler ym., 2013; Baslow ym., 2013.) Kun tietoturva pettää tai vaarantuu, se ei useinkaan olisi edes mahdollista ilman tahallista tai tahatonta toimintaa (Crossler ym., 2013, 91). Sähköpostiviestiin liitetyn linkin painaminen, liitteen avaaminen tai web-sivulla vierailu saattaa vaikuttaa pieneltä teolta, vaikka teolla voi lopulta olla lähes korvaamattomat seuraukset.

Koska yksilö voi omalla toiminnallaan joko edesauttaa tai vaihtoehtoisesti murentaa organisaation tietoturvan ylläpitämistä, on tietoturvaan liittyvää käyttäytymistä tutkittu erilaisten teoriasuuntausten ja teoreettisten lähtökohtien kautta. Tutkimuksissa on hyödynnetty muun muassa sosiaalipsykologian, moraalipsykologian, kriminologian, terveyspsykologian ja moraalifilosofian käyttäytymismalleja (Moody, Siponen ja Pahnila, 2018, 288.) Eri tutkimusten näkökulmissa on keskitytty muun muassa ymmärtämään, miten vahingollista käyttäytymistä voitaisiin estää tai kuinka työntekijöitä voitaisiin motivoida tietoresurssien tietoturvallisessa käytössä, hallinnoinnissa ja ylläpidossa. Tietoturvan yhteydessä motivoinnin keinoista on esimerkiksi sovellettu Deci ja Ryan motivaatioteoriaa (Kinnunen, 2015) sekä suojelumotivaatioteoriaa (engl. *protection motivation theory*) tai sen osia (Boss ym, 2015; Johnston ym., 2010; Siponen ym., 2014). Suojelumotivaatioteoriassa lähtökohtana on malli, joka mukaan on tärkeää herättää riittävästi pelkoa motivoimaan suositeltavaa tai toivottavaa käyttäytymistä, mutta kuitenkin vain sen verran, että suositellun käyttäytymisen noudattaminen kumoaa pelkoreaktion (Maddux & Rogers, 1983, 470). Tietoturvan yhteydessä on tutkittu, miten pelko voisi muokata käyttäytymistä suositeltujen tietoturvatoimien yhteydessä (Johnston & Warkentin, 2010; Vance, Siponen & Pahnila, 2012).

Käyttäytymisen selittämiseen ja ennustamiseen liittyvistä taustateorioista on tietoturvan yhteydessä sovellettu myös muun muassa perustellun toiminnan teoriaa (engl. *theory of reasoned action, TRA*) (Bauer & Bernroider, 2017; Kim ym., 2014) ja suunnitellun käyttäytymisen teoriaa (engl. *theory of planned behaviour, TPB*) (kts. esim. Ifinedo, 2012; Bulgurcu ym., 2010; Johnston & Warkentin, 2010). Näiden teorioiden keskeisenä käyttäytymistä ohjaavana käsitteenä on aikomus, johon vaikuttavat asenne, subjektiiviset normit sekä yksilön kyky hallita käyttäytymistä (Fishbein & Ajzen, 2011).

Lisäksi tietoturvakäyttäytymisen tutkimuksissa eräs usein käytetyistä teorioista on peloteteoria (engl. *deterrence theory*) (D'arcy & Herath, 2011). Peloteteorialla on yhteys kriminologiaan, ja rikollisen ja poikkeavan käyttäytymisen ymmärtämiseen, mutta joidenkin tutkimusten mukaan sen olettamukset ovat päteviä myös tietoturvakäyttäytymisen havainnoinnissa (Johnston ym., 2015, 120). Peloteteorian keskeisenä ajatuksena on, että teon seurausten pelko estää toimimasta tietyllä tavalla ja siten esimerkiksi rangaistuksen pelko estää rikoksia. Teorian taustaoletuksena on, että henkilö ikään kuin vertailee seurausten vakavuutta suhteessa rangaistuksen todennäköisyyteen päättäessään rikkoa sosiaalista normia tai vakiintuneita käytäntöjä. (Johnston ym., 2015.) Toisaalta on esitetty, ettei seuraamusten tai rangaistusten pelko välttämättä ohjaa työntekijöiden tietoturvakäyttäytymistä, koska työntekijät oikeuttavat tietoturvarikkomuksiaan neutralisoimistekniikoiden avulla. Siposen ja Vancen (2010) tutkimuksen mukaan rangaistuksen tai sanktioiden pelko ei välttämättä ohjaa työntekijöiden tietoturvakäyttäytymistä, koska työntekijät hyödyntävät erilaisia neutralisoimistekniikoita ja järkeilevät niiden avulla toimintaansa, jolloin seuraukset menettävät tehonsa. Edellä esitellyt teoriat viittaavat ikään kuin yksilön rationaaliseen ajatte-

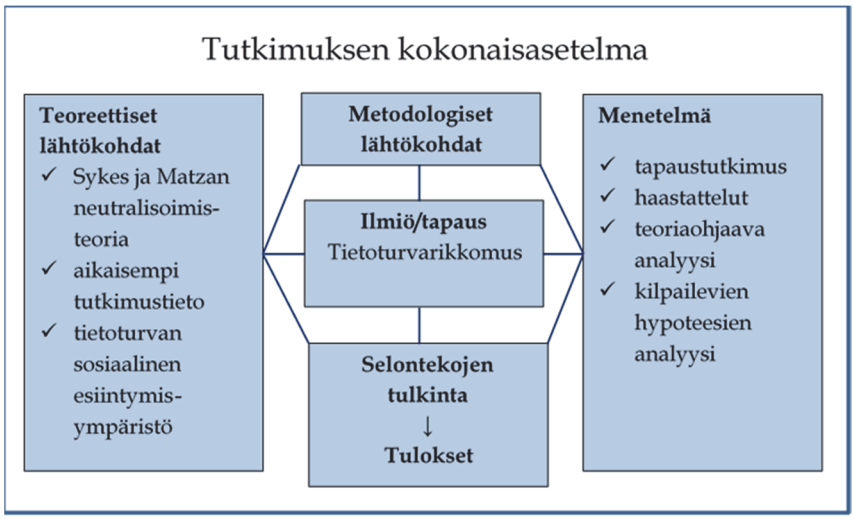
luun ja harkittuun päätöksentekoon. Yksilön on siis kyettävä arvioimaan erilaisten tapahtumien seurauksia ja niiden perusteella suhteuttamaan omaa toimintaansa.

Tämän tutkimuksen lähtökohtana ja motivaationa on ollut tarkastella sitä, kuinka rationaalisesti ihminen oikeastaan toimii rikkoessaan tietoturvapolitiikan mukaisia ohjeita, sääntöjä ja määräyksiä, vai voisiko taustalla olla muita selittäviä tekijöitä. Työntekijöiden näkökulmaan perustuva tutkimus on perusteltua, sillä aiheesta on tällä hetkellä vielä verrattain vähän tutkimuksia.

1.2 Tutkimuksen tarkoitus

Vaikka työntekijöiden toimesta tehdyt tietoturvarikkomukset eivät itsessään ole ilmiönä uusi, niillä on vielä suhteellisen lyhyt historia. Ilmiö ei myöskään ole tieteellisesti vieras. Kuitenkin empiirinen tutkimus työntekijöiden tietoturvarikkomusten taustasyistä on vielä alussa ja niin sanottujen arkihavaintojen takaa tulisi löytää täsmällisempää tietoa. Tämän tutkimuksen tarkoituksena on teoreettisten lähtökohtien, aiemman tutkimustiedon, kerätyn empiirisen tutkimusaineiston keskusteluttamisen ja analysoinnin kautta löytää lisäymmärrystä, laajentaa näkökulmaa ja tuoda uutta tietopohjaa työntekijöiden selonteoista, joilla he selittävät tai perustelevat tietoturvarikkomuksiaan. Tutkimuksen päätehtävänä on esittää revisioitu neutralisoimisteoria tietoturvakontekstiin ja esittää sille empiiristä tukea. Sana ”revisio” tarkoittaa suomen kielessä tarkastusta, uudelleen muotoiltua tai muovailtua, muutosta, uudistusta tai korjausta (Turtia, 2010).

Tutkimus pyrkii vastaamaan tutkimuskysymykseen: ”Miten työntekijät selittävät ja perustelevat tietoturvapolitiikan ja -ohjeiden noudattamattomuutta?” Tutkimuskysymykseen vastaamisen tukena tarkastellaan myös yksilön tietoturvakäyttäytymisen taustalla vaikuttavia tekijöitä sekä pyritään ymmärtämään niitä lähtökohtia, jotka johtavat työntekijän tekemään tietoturvarikkomukseen. Tässä laadullisessa tutkimuksessa tutkimuskysymystä peilataan tutkimusta ohjanneen kriminologian neutralisoimisteorian kautta, jolloin se samalla rajaa tutkimusta. Tutkimuksen kokonaisasetelma on esitelty kuviossa 1.



KUVIO 1 Tutkimuksen kokonaisasetelma

Tutkimuksen teoreettisena lähtökohtana mainittua Gresham Sykesin ja David Matzan neutralisoimisteoriaa on pidetty yhtenä vaikutusvaltaisimmista kriminologian teorioista (Maruna & Copes, 2005, 222-223). Neutralisoimisteoria toi 1950-luvulla esille tuolloin tuntemattoman käsitteen *"poikkeavuuden oikeutus"* (engl. *justifications of deviant*). Se liittyy rikollisen tai sosiaalisista normeista poikkeavan teon puolustukseen tai perusteluun, joka ei välttämättä ole pätevä oikeusjärjestelmissä tai laajemmin yhteiskunnassa, mutta jolla rikollinen perustelee ja oikeuttaa tekonsa (Sykes ja Matza, 1957, 666). Sykes ja Matzan (1957) neutralisoimisteorian keskeisen väittämän mukaan ihminen oikeuttaa normeista poikkeavan käyttäytymisensä neutralisoimistekniikoiden avulla, ja välttää näin itsesyytösten aiheuttaman syyllisyyden ja häpeän kyetäkseen säilyttämään vahingoittumattoman minäkuvan. Toisaalta neutralisoimistekniikat toimivat Sykesin ja Matzan (1957, 666) mukaan myös poikkeavan käyttäytymisen mahdollistajana, jolloin teon oikeutus tehdään jo ennen tekoa.

Sykesin ja Matzan neutralisoimisteoriaa on sovellettu useissa tietoturvakäyttäytymiseen liittyvissä tutkimuksissa. Tämän tutkimuksen teoreettiset lähtökohdat koostuvatkin neutralisoimisteorian lisäksi myös aiemmasta tutkimustiedosta. Sen avulla on pyritty muodostamaan käsitys siitä, miten teoriaa on aiemmissa tutkimuksissa tulkittu, miten sitä on sovellettu sekä vertailtu aiemmin käytettyjä tutkimusmenetelmiä. Lisäksi on tarkasteltu muun muassa sitä, kuinka kattavasti aiemmat tutkimukset ovat huomioineet Sykes ja Matzan teorian keskeisiä olettamuksia. Jotta neutralisoimisteoriaa voidaan tarkastella tietoturvakontekstissa, on tutkimuksen keskiössä olevaa ilmiötä tarkasteltava sen sosiaalisessa esiintymisympäristössä. Tästä syystä tutkimukseen on liitetty myös sosiaalisen elämän käsitteitä.

Aiemmissa neutralisoimisteoriaa tietoturvan yhteydessä soveltaneissa tutkimuksissa on enimmäkseen käytetty kvantitatiivisia tutkimusmenetelmiä. Tässä tutkimuksessa analysoitavan aineiston keräämisessä haluttiin poiketa aiemmista tutkimuksista, ja antaa työntekijöiden itsensä kertoa kokemuksistaan,

ajatuksistaan, uskomuksistaan ja tunteistaan. Tämä päätös ohjasi samalla myös tutkimusstrategian ja metodologian valintaa.

Mikään tutkimus harvoin aloitetaan niin sanotusti puhtaalta pöydältä, eli ilman tutkijan omia ennakko-oletuksia tai ennakkotietoa. Walshamin (2006, 324-325) näkemyksen mukaan jo tutkimuksen teorian valinta on pääosin subjektiivinen päätös, eli ilman tutkijan omia kokemuksia, taustaa ja kiinnostuksen kohdetta, tutkimukseen valittu teoriakaan ei voi välttämättä toimia inspiraation lähteenä eikä siten anna erilaisten oivallusten mahdollisuuksia (Walsham, 2006, 324-325). Teorian käyttö luo kuitenkin tutkimukselle vahvan teoreettisen perustan ja lähestymistavan (Walsham, 1995, 76). Tässä tutkimuksessa teorian valintaan ohjasi tutkijan esiymmärrys siitä, että eri organisaatioiden sekä johto että muu henkilökunta rikkovat tietoturvapolitiikan ohjeita. Kysymystä ja ihmettelyä siitä, miksi järkevä aikuinen ihminen toimii näin, haluttiin tarkastella Sykesin ja Matzan teoriaa vasten muun muassa sen yleismaailmallisuuden vuoksi. Samalla neutralisoimisteoria toimi tämän tutkimuksen käsitteellistämisen ja jäsentelyn tukena. Teoria esitellään yksityiskohtaisemmin luvussa kaksi. Tutkijan tiedostamien ennakko-oletusten vuoksi tutkimusaineiston analyysin ja keskusteluttamisen apuna käytettiin eri analyysimenetelmien yhdistelmää, jotka esitellään luvussa viisi.

1.3 Aiheen valinnan perustelu

Aihe on tärkeä monestakin syystä. Ensinnäkin, tilanteessa jossa organisaation toimintaan kohdistuva uhka tulee organisaation sisältäpäin lähes yhtä merkittävästi kuin ulkoapäin, on tietoturvatutkimuksessa perusteltua kiinnittää huomiota teknisten tietoturvakomponenttien lisäksi myös työntekijöihin, eli järjestelmiä käyttäviin ihmisiin. Työntekijöillä on pääsy organisaation tietoihin, jota tänä päivänä usein kutsutaan jo organisaation omaisuudeksi. Jotta tuo tietoomaisuus voitaisiin turvata, on tärkeää pyrkiä selvittämään työntekijöiden tietoturvakäyttäytymisen taustalla vaikuttavia syitä ja tekijöitä. Toinen tärkeä syy tutkimukselle on muutokset sosioteknisessä ympäristössä. Dhillon ym., (2016) mukaan sosiotekninen ympäristö koostuu sekä ihmisistä että teknologiasta, jotka kumpikin muovaavat toisiaan. Tämän päivän sosiotekninen ympäristö ei ole stabiili eikä sitä voi luokitella toimintamalliksi, joka olisi itsestäänselvyyksiksi muodostuneiden toimintatapojen, tulkintakehysten ja ongelmanratkaisumallien muodostama kokonaisuus, vaan sen oletetaan muuttuvan jatkuvasti (Lyytinen & Newman, 2008, 606-607). Muun muassa internet ja nopeasti kehittyvät erilaiset teknologiat ovat tarjonneet uudenlaisia tuotteita ja liiketoimintamalleja tietoturvan jäädessä auttamattomasti näiden jalkoihin (Bone, 2017, xvii-xviii).

Tämän tutkimuksen näkemyksen mukaan aiemmissa tietoturvatutkimuksissa sovellettu Sykes ja Matzan (1957) neutralisoimisteoria luotiin hyvin erilaiseen ympäristöön kuin tämän päivän sosiotekninen ympäristö. Alkuperäinen neutralisoimisteoria on antanut arvokasta näkökulmaa poikkeavuuden ja rikollisuuden selittämiseen, mutta se ei välttämättä sellaisenaan sovellu selittämään

työntekijöiden tietoturvakäyttäytymistä ja tietoturvapolitiikan ja –ohjeiden noudattamattomuutta. Maailma, kulttuurit, (yhteiskunta)tieteellinen tutkimus, kuin myös muun muassa suhtautuminen auktoriteetteihin ovat muuttuneet valtavasti siitä, kun ensimmäinen neutralisoimisteoria hahmoteltiin (Maruna & Copes, 2005, 224; Topalli, 2005, 824). Huolimatta siitä, että edelleen muun muassa organisaatioiden sisällä vallitsee tietynlainen sosiaalinen järjestys omine sosiaalisine normeineen, niitä ei välttämättä voida rinnastaa Sykesin ja Matzan teorian oletuksiin. Vaikka aiemmat, erityisesti tietojärjestelmätieteen, tutkimukset ovat antaneet arvokasta tietoa neutralisoinnin roolista tietoturvarikkomusten yhteydessä, ei aiempien tutkimusten lähestymistapa työntekijöiden neutralisoinnin hyödyntämiseen ole välttämättä ollut riittävän järjestelmällinen ja kattava. Sykes ja Matzan (1957) teorian keskeisin olettamus erilaisten neutralisoimistekniikoiden hyödyntämiseen liittyy syyllisyyden ja häpeän välttämiseen. Aiemmat tutkimukset (kts. esim. Siponen & Vance, 2010; Barlow ym., 2013; Bauer & Bernroider, 2017) ovat ikään kuin olettaneet syyllisyyden välttämisellä olevan yhteyttä neutralisointiin nimenomaan tietoturvakontekstissa tutkimatta kuitenkaan tätä yhteyttä tarkemmin.

Tämän tutkimuksen teoreettisena kontribuutiona on tuoda uutta tietoa työntekijöiden selonteoista ja selityksistä, joilla he selittävät tietoturvarikkomuksiaan. Jotta pystyisimme ymmärtämään tietoturvarikkomuksiin liittyvää selittämistä ja selontekoihin liittyvää hyväksyntää, tarvitaan aiempaa enemmän tietoa työntekijöiden näkemyksistä, kokemuksista ja asenteista. Tämä tutkimus on tiettävästi ensimmäinen tietoturvaan liittyvä tutkimus, jossa neutralisoimisteorian soveltumista tietoturvarikkomuksia selittävänä teoriana tarkastellaan kriittisesti yhdistämällä sekä neutralisoimisteorian että aiempien tutkimusten kriittinen tarkastelu.

Muu muassa Tsohou ym., (2015, 140) ja Willison ym., (2018, 288) mainitsevat, kuinka nykyinen tietoturvatutkimus vaatisi käyttäjälähtöisempää lähestymistapaa, jotta kyettäisiin paremmin ymmärtää mekanismeja, jotka ohjaavat tietoturvapolitiikan noudattamista ja muokkaavat tietoturvakäyttäytymistä. Tämä tutkimus haluaa omalta osaltaan monipuolistaa tietoturvatutkimusta, ja auttaa kiinnittämään enemmän huomiota edelleen vähäisesti tutkittuun ja vielä epäselvään puoleen työntekijöiden tietoturvakäyttäytymisessä. Aiemmat neutralisoimisteoriaa tietoturvakontekstissa soveltaneet tutkimukset ovat korostaneet aiheen tutkimisen tarpeellisuutta ja ehdottaneet aiheeksi muun muassa sitä, miten erilaiset neutralisoimistyypit liittyvät erilaisiin rikkomustyyppeihin (Moody ym., 2018), sekä sitä, mikä rooli häpeällä oikeastaan on työntekijöiden tietoturvarikkomuksissa (Silic ym.,2017).

Tutkimuksen käytännön kontribuutiona on tutkitun tiedon perusteella tarkastella, millaiset arkipäiväiset tilanteet voivat olla tietoturvan näkökulmasta riskialttiita. Lisäksi tutkimustulosten odotetaan tuovan tietoa, voiko tietoturvapolitiikka dokumentteineen itsessään vaikuttaa negatiivisesti työntekijöiden tietoturvakäyttäytymiseen. Ilman työntekijöiden näkemyksiä, eli tietojenkäsittelyn inhimillisen elementin huomioimista, ei tietoturvaakaan voida kehittää kokonaisvaltaisesti, joten tutkimuksen tulosten odotetaan tukevan organisaatioiden jatkuvaa

tietoturvatyötä. Tutkimustulosten odotetaan tarjoavan käytännön ratkaisuja, joita voidaan hyödyntää tietoturvajohtamisessa, tietoturvaan liittyvässä organisaatioiden sisäisissä koulutuksissa sekä tietoturvakulttuurin kehittämisessä.

Tutkimuksen yhteiskunnallinen merkitys nousee siitä tosiasiasta, että niin kutsuttu kybertoimintaympäristö on viime vuosikymmenenä muuttunut. Tuoreessa Suomen kyberturvallisuusstrategiassa (2019, 8) mainitaan, kuinka jokainen yksilö on tärkeä kybertoimija ja voi omilla teoillaan vaikuttaa kyberturvallisuuteen. Sekä julkiselle että yksityiselle sektorille asetut teknologian hyödyntämiseen liittyvät tavoitteet, kuten muun muassa yhteisten tietovarantojen hyödyntämiseen, sähköisiin palveluihin sekä uudenlaisten liiketoimintamallien kehittämiseen liittyvät tavoitteet edellyttävät tietoturvallisuuden eri osa-alueiden jatkuvaa tarkastelua. Vaikka erilaisen teknologian, kuten tekoälyn ja robotiikan uskotaan tuovan ratkaisuja moniin inhimillisistä tekijöitä johtuviin ongelmiin, ne eivät siltikään toistaiseksi poista kaikkia niitä valintatilanteita, joita organisaatioiden työntekijät päivittäisessä työssään tekevät. Tästä syystä erilaisissa valintatilanteessa päätöksiä tekevien työntekijöiden näkökulman tutkiminen on merkityksellistä.

1.4 Tutkimuksen keskeiset käsitteet

Tietoturvakäyttäytymisen tarkastelu Sykes ja Matzan neutralisoimisteoriaa vasten rajaa tutkimusta, mutta tuo samalla mukanaan lukuisia käsitteitä. Neutralisoimisteoria itsessään ei sisällä tietojärjestelmätieteen käsitteitä, joten tässä tutkimuksessa käytettävien käsitteiden osalta on johdonmukaista tukeutua myös muiden tieteenalojen määritelmiin. Seuraavaksi esitellään tämän tutkimuksen keskeiset käsitteet tiivistettynä. Käsitteet esitellään tarkemmin luvussa kolme.

Tietoturva: Tässä tutkimuksessa tietoturvalla ymmärretään niitä hallinnollisia käytäntöjä ja teknisiä ratkaisuja, joilla organisaation toiminnan ja jatkuvuuden kannalta keskeisten tietojen ja tietojärjestelmien luottamuksellisuus, eheys ja saatavuus turvataan.

Tietoturvapolitiikka: Tässä tutkimuksessa tietoturvapolitiikalla ymmärretään organisaation strategisia tavoitteita ja tietoturvatoimintaa tukevia linjauksia, politiikkoja, ohjeita, määräyksiä ja sääntöjä, joiden avulla turvataan organisaation toiminnan kannalta keskeisen tiedon luottamuksellisuus, eheys ja saatavuus.

Tietoturvakäyttäytyminen: Tässä tutkimuksessa tietoturvakäyttäytyminen ymmärretään organisaation työntekijöiden käyttäytymisenä ja toimintatapoina, joilla he joko edesauttavat tai murentavat organisaation tietoturvaan liittyvien periaatteiden toteuttamista.

Tietoturvarikkomus: Tässä tutkimuksessa tietoturvarikkomuksella ymmärretään mitä tahansa työntekijän toimintaa, joka aiheuttaa tietoturvan vaarantumisen.

Sosiaalinen normi: Tässä tutkimuksessa (sosiaalinen) normi ymmärretään käyttäytymissääntönä, jolla on kuitenkin niin laaja hyväksyntä, että yksilö ym-

märtää normin olemassa olon ja kykenee sisäistämään sen. Määritelmässä tukeudutaan Ewaldin (2003, 59) mainintaan, eli normi on suhteellinen ja muuttuva, joten yksilön on kyettävä suhteuttamaan käyttäytymisensä normin mukaiseksi. Yksilöllä on siis riittävät tiedot ja taidot normin mukaisen käyttäytymisen noudattamiseen. Erittäin pelkistetty esimerkki sosiaalisesta normista Suomessa on jonottaminen. Jonottamisen sääntöjä ei välttämättä ole kirjoitettu mihinkään, mutta siltikään kenellekään ei tarvitse selittää, mitä jonottaminen täsmällisesti tarkoittaa. Jonossa etuilijaa paheksutaan, ja vaikkei tekoon liitykään mitään virallista rangaistusta, etuilu ikään kuin loukkaa muita.

Sosiaalisesta normista poikkeaminen: Tässä tutkimuksessa poikkeavuudella tarkoitetaan käyttäytymistä, joka eroaa sosiaalisesta normista ja poikkeaa hyväksyttävästä tavasta toimia. Sosiaalisesta normista poikkeaminen tarkoittaa samalla sisäistetyn (sosiaalinen) normin tietoista rikkomista.

Sosiaalinen kontrolli ja sosiaalinen järjestys: Tässä tutkimuksessa sosiaalisella kontrollilla ymmärretään yhteiskunnan, kulttuurin tai yhteisön luomia, osin sanattomiakin, käyttäytymiseen liittyviä sääntöjä, kuinka yksilön tulisi toimia hyväksyttävällä tavalla kulloinkin kyseessä olevassa yhteiskunnassa, kulttuurissa tai yhteisössä. Vaikka sosiaalista kontrollia ei välttämättä ilmaista sanallisesti tai kirjallisesti, sosiaalista järjestystä ylläpidetään muun muassa paheksumalla niitä, jotka eivät noudata hyväksyttäviä tapoja, vaan poikkeavat niistä, eikä yksilö voi olla havaitsematta omaa poikkeavuuttaan tai olla tiedostamatta sitä, että rikkoo sosiaalista normia.

1.5 Tutkimuksen rakenne

Tutkimuksessa on kaikkiaan kahdeksan lukua. Ensimmäisen luvun tarkoituksena on ollut johdattaa lukija aiheeseen. Tutkimuksen teoreettisten lähtökohtien laajuuden vuoksi, ne on jaettu kolmeen päälukuun. Luvussa kaksi esitellään tutkimuksen keskeisin teoria, eli neutralisoimisteoria. Lukuun kolme on koottu tutkimuksen keskeisimmät käsitteet. Tämä järjestys on valittu siitä syystä, että käsitteet tukevat neljännessä luvussa tehtävää aiempien tutkimusten tarkastelua. Luvussa neljä tarkastellaan myös aiempien tutkimusten tulkintoja neutralisoimisteoriasta ja sen olettamuksista, sekä sitä, kuinka kvalitatiivisilla menetelmillä on mitattu neutralisoimisteorian olettamuksia sekä erilaisia neutralisoimistekniikoita. Luvussa viisi esitellään tutkimuksen metodologia sekä perustellaan aineiston hankintaan ja analysointiin liittyviä valintoja. Luvussa kuusi neutralisoimisteorian keskeisiä oletuksia sekä neutralisoimistekniikoita verrataan tietoturvakontekstissa tutkimusaineiston kautta. Luvussa seitsemän käydään tutkimukseen liittyvä keskustelu, arvioidaan tutkimuksen luotettavuutta sekä esitellään jatkotutkimusehdotuksia. Viimeinen luku sisältää tutkimuksen yhteenvedon.

2 TEOREETTISET LÄHTÖKOHDAT

Tutkimuksen keskeisin teoria, neutralisoimisteoria, toimii tässä tutkimuksessa niin vahvana tukirankana, että se ansaitsee tulla esitellyksi ennen tutkimuksen keskeisten käsitteiden läpikäyntiä. Selvyyden vuoksi mainittakoon, että tässä tutkimuksessa alkuperäisen teorian termeistä ”*neutralization*” ja ”*techniques of neutralization*” käytetään suomenkielisiä käännöksiä neutralisointi ja neutralisoimistekniikat. Lisäksi on vielä mainittava, että luku sisältää runsaasti suoria, englanninkielisiä lainauksia Sykes ja Matzan teoriasta. Suomennokset näistä lainauksista on tekijän vapaasti suomentamia.

2.1 Neutralisoimisteorian perusta ja väitteet

Yhdysvaltalaisten kriminologien Gresham Sykesin ja David Matzan (1957) teorian perustana on toiminut Edwin H. Sutherlandin differentiaalisen assosiaation teoria. (Termille ei tiettävästi löydy suomennosta.) Vaikka Sutherland (1992, 89) esitteli rikollista käyttäytymistä selittävässä teoriassaan kaikkiaan yhdeksän väitettä, silti teorian ydin kiteytyy siihen, kuinka yksilöstä tulee rikollinen:

> “A person becomes delinquent because of an excess to definitions favorable to violation of law over definitions unfavorable to violation of law. This is the principle of differential association.” (Sutherland ym., 1992, 89)

Differentiaalisen assosiaation periaatteen mukaan yksilöstä tulee rikollinen, kun lain rikkomisen määritelmät ylittävät lain noudattamisen määritelmät. Sykesin ja Matzan neutralisoimisteoria ei pohjaudu täysin Sutherlandin teorian ydinosaan, vaan painottuu rikollisen käyttäytymisen oppimiseen. Seuraavaksi esitellään nämä Sutherlandin teoriasta poimitut rikollisen käyttäytymisen oppimiseen liittyvät keskeiset väitteet.

> “Criminal behavior is learned. Negatively, this means that criminal behavior is not inherited, as such.” (Sutherland ym., 1992, 88-89)

> "Criminal behavior is learned in interaction with other persons in a process of communication. This communication is verbal in many respects, but it also includes "the communication of gestures"." (Sutherland ym., 1992, 89)

> "The principal part of the learning of criminal behavior occurs within intimate personal groups. Negatively, this means that the impersonal agencies of communication, such as movies and newspapers, play a relatively unimportant part in the genesis of criminal behavior." (Sutherland ym., 1992, 89)

> "When criminal behavior is learned, the learning includes (a) techniques of committing the crime, which are sometimes very complicated, sometimes very simple; (b) the specific direction of motives, drives, rationalizations and attitudes." (Sutherland ym., 1992, 89)

> "The specific direction of motives and drives is leaned from definitions of the legal codes as favorable or unfavorable." (Sutherland ym., 1992, 89)

> "The process of learning criminal behavior by association with criminal and anticriminal patterns involves all of the mechanisms that are involved in any other learning. Negatively, this means that the learning of criminal behavior is not restricted to the process of imitation." (Sutherland ym., 1992, 90)

Sutherlandin teorian mukaan rikollisuus ei siis ole peritty ominaisuus, vaan se opitaan vuorovaikutuksessa toisten ihmisten kanssa. Rikollisuuteen oppiminen sisältää rikosten tekemisen tekniikat, motiivin, asenteen ja rationalisoinnin (järkiperäistämisen), eikä siten rajoitu vain tiettyjen käyttäytymismallien jäljittelyyn (Sutherland ym., 1992, 88-90; Sykes & Matza, 1957, 664).

Sykes ja Matza (1957, 664) eivät kritisoineet Sutherlandin teorian keskeisiä väitteitä rikollisuuteen oppimisesta, mutta he mainitsevat:

> "Unfortunately, the specific content of **what** is learned -as opposed to the process by which it is learned- has received relatively little attention in either theory or research."

Sykes ja Matza siis kritisoivat sitä, ettei teorioissa ja tutkimuksissa oltu kiinnitetty riittävästi huomioita siihen, ***mitä*** oppimisprosessissa opitaan, eli opintosisältöön. Sykes ja Matza kritisoivat[1] myös Albert K. Cohenin rikollisuuskäsitystä, jonka mukaan rikollista käyttäytymistä ylläpidetään ja vahvistetaan käyttäytymissäännöillä, jotka ovat ristiriidassa vallitsevien arvojen ja normien kanssa. Tämän tutkimuksen tulkinta Sykes ja Matza (1957) julkaiseman, nuorisorikollisuuteen keskittyvän "*Techniques of neutralization: a theory of delinquency*" -artikkelin lähtökohdista oli Sykesin ja Matzan halu kritisoida 1950-luvulla vallinneita rikollisuuskäsityksiä sekä pyrkimys täydentää rikollisen tai poikkeavan käyttäytymisen tutkimusta.

Sykes ja Matza kyseenalaistivat ajatuksen vallitsevan yhteiskunnan arvoihin nähden käänteisestä, erillisestä rikollisesta alakulttuurista esittämällä neljä väitettä, joiden pääkohdat esitellään seuraavaksi.

---

1 "Cohen sees the process of developing a delinquent sub-culture as a matter of building, maintaining, and reinforcing a code for behavior which exists by opposition, which stands in point by point contradiction to dominant values, particularly those of the middle class." (Sykes & Matza, 1957, 664)

Sykesin ja Matzan ensimmäinen väite

> "In the first place, if there existed in fact a delinquent sub-culture such that the delinquent viewed his illegal behavior as morally correct, we could reasonably suppose that he would exhibit no feelings of guilt or shame at detection or confinement." (Sykes & Matza, 1957, 664)

> "More important, however, is the fact that there is a good deal of evidence suggesting that many delinquents do experience a sense of guilt or shame, and its outward expression is not to be dismissed as a purely manipulative gesture to appease those in authority." (Sykes & Matza, 1957, 664-665)

Ensimmäinen Sykesin ja Matzan väite perustui siihen, että jos olisi olemassa (nuoriso)rikollisten alakulttuuri, silloin rikolliset pitäisivät rikollista käyttäytymistä moraalisesti oikeana ilman syyllisyyden ja häpeän tunteita. Sykesin ja Matzan mukaan huolimatta rikollisista, jotka eivät tunne rikoksistaan syyllisyyttä tai häpeää, on silti tärkeä tuoda esille se, että nuorisorikolliset tuntevat aidosti syyllisyyttä ja häpeää. (Sykes &Matza, 1957, 664-665.)

Sykesin ja Matzan toinen väite

> "In the second place, observers have noted that the juvenile delinquent frequently accords admiration and respect to law-abiding persons" (Sykes ja Matza, 1597, 665).

> "While supposedly thoroughly committed to the deviant system of the delinquent sub-culture, he would appear to recognize the moral validity of the dominant normative system in many instances." (Sykes & Matza, 1957, 665)

> "Instead, the juvenile delinquent would appear to be at least partially committed to the dominant social order in that he frequently exhibits guilt or shame when he violates its proscriptions, accords approval to certain conforming figures, and distinguishes between appropriate and inappropriate targets for his deviance." (Sykes & Matza, 1957, 666).

Sykesin ja Matzan toisen väittämän voi käänteisesti tulkita niin, että jos olisi rikollisten alakulttuuri, rikollisten tulisi arvostaa vain sellaisia henkilöitä, jotka edistävät rikollista elämäntapaa ja hylätä muiden mielipiteet. Kuitenkin Sykesin ja Matzan mukaan nuorisorikollinen näyttäisi olevan sitoutunut, ainakin osittain, vallitsevaan yhteiskuntaan ja kykenisi erottamaan sopivan ja sopimattoman toiminnan. Nuorisorikollinenkin myöntää arvostavansa lainkuuliaisia ihmisiä ja voi myös itse paheksua laitonta toimintaa (Sykes & Matza, 1957, 665-666).

Sykesin ja Matzan kolmas väite

> "In the third place, there is much evidence that juvenile delinquents often draw a sharp line between those who can be victimized and those who cannot. Certain social groups are not to be viewed as "fair game" in the performance of supposedly approved delinquent acts while others warrant a variety of attacks. In general, the potentiality for victimization would seem to be a function of the social distance between the juvenile delinquent and others and thus we find implicit maxims in the world of the delinquent such as "don't steal from friends" or "don't commit vandalism against a church of your own faith." (Sykes & Matza, 1597, 665).

Kolmantena Sykes ja Matza epäilivät myös nuorisorikollisten varauksetonta rikosten hyväksyntää. Jos rikoksentekijä hyväksyisi ehdoitta rikollisen toiminnan, silloin voisi olettaa, että rikollinen kohtelisi kaikkia uhrejaan samoin. Sykesin ja Matzan (1957, 665) mukaan nuorisorikollinen pystyy kuitenkin erottamaan tilanteet, kuten ajan ja paikan, jolloin rikollinen toiminta ei ole hyväksyttävää. Muun muassa kavereilta ei varasteta tai oman uskontokunnan kirkkoon ei kohdisteta ilkivaltaa.

Sykesin ja Matzan neljäs väite

> "In the fourth place, it is doubtful if many juvenile delinquents are totally immune from the demands for conformity made by the dominant social order." (Sykes & Matza, 1597, 665).

Neljännen Sykesin ja Matzan väittämän mukaan olisi epätodennäköistä, että nuorisorikollinen korvaisi jollain toisella järjestelmällä vallitsevan yhteiskunnan arvot ja normit, tai olisi täysin immuuni sen yhdenmukaisuuden[2] (engl. *conformity*) vaatimukselle.[3] Sykes ja Matza kyseenalaistivat myös ajatuksen siitä, että vanhempien asenne edesauttaisi rikollisuutta. (Sykes & Matza, 1957, 665.)

2.2 Poikkeavuuden oikeutus

Koska Sykes ja Matza halusivat täydentää aiempien teorioiden ja tutkimusten puutteita, he keskittyivät tutkimuksessaan myös siihen, ***mitä*** yksilö neutralisoi (rationalisoi) tai oikeuttaa tehdessään normeista poikkeavan, syyllisyyttä ja häpeää aiheuttavan teon[4]. Sykesin ja Matzan (1957, 666) näkökulman mukaan nuorisorikollisen käyttäytyminen perustuu samaan tapaan arvoihin ja normeihin kuin lainkuuliainenkin käyttäytyminen. Ihmisen käyttäytymiseen liittyy kuitenkin se ongelma, että lakeja, joihin uskotaan, rikotaan silti. Sykes ja Matza (1957, 666) mainitsevat:

> "A basic clue is offered by the fact that social rules or norms calling for valued behavior seldom if ever take the form of categorical imperatives. Rather, values or norms appear

[2] Sanalla *conformity* voidaan viitata konformismiin, eli pyrkimykseen sopeutua ja mukautua yhteisön vaatimuksiin sekä noudattaa yhdenmukaisuutta. (Turtia, 2010, 276)

[3] "In other words, if the delinquent does hold to a set of values and norms that stand in complete opposition to those of respectable society, his norm-holding is of a peculiar sort. While supposedly thoroughly committed to the deviant system of the delinquent sub-culture, he would appear to recognize the moral validity of the dominant normative system in many instances." (Sykes & Matza, 1957, 665)

[4] "Instead, the juvenile delinquent would appear to be at least partially committed to the dominant social order in that he frequently exhibits guilt or shame when he violates its proscriptions, accords approval to certain conforming figures, and distinguishes between appropriate and inappropriate targets for his deviance." (Sykes & Matza, 1957, 666)

> as qualified guides for action, limited in their applicability in terms of time, place, persons, and social circumstances." (Sykes & Matza, 1957, 666)

Sykes ja Matzan käyttivät teoriassaan termiä "*categorical imperative*", mutta eivät teoriassaan selitä termiä tarkemmin. Onkin oletettavaa, että Sykes ja Matza viittasivat termillä *categorical imperative*[5] Kantin etiikan keskeiseen periaatteeseen. Sykes ja Matza (1957, 666) eivät mitä ilmeisimmin kuitenkaan uskoneet Kantin ehdottomuuteen, koska heidän mukaansa sosiaalisen järjestelmän säännöt ja normit vaativat harvoin, jos koskaan, ehdotonta pakkoa. Sykesin ja Matzan mukaan arvot ja normit näyttäytyvät pikemminkin toimintaa ohjaavana ja rajoittuneena sovellettavaksi tiettyyn aikaan, paikkaan, henkilöön tai sosiaaliseen tilanteeseen. Sykes ja Matza (1957, 666) nostivat esimerkiksi, kuinka moraalisesti tappaminen on väärin, paitsi vihollista vastaan käydyssä sodassa. Heidän mukaansa yhteiskunnan normatiivinen järjestys ei siis sisällä sääntöjä, jotka ovat sitovia kaikissa olosuhteissa (Sykes & Matza, 1957, 666). Juuri tämä joustavuus on erottamaton osa rikoslakia ja rikoksien puolustamista (engl. *defenses to crimes*). Kun yksilö esittää tekonsa perusteena välttämättömyyttä, järjettömyyttä, humalaa, pakkoa tai itsepuolustusta, normatiivisen järjestelmän joustavuus antaa Sykesin ja Matzan mukaan yksilölle mahdollisuuden sekä moraalisen syyllisyyden (engl. *moral culpability*) että yhteiskunnan asettamien rangaistusten välttämisen, mikäli hän pystyy osoittamaan, että teosta puuttui rikollinen tarkoitus (engl. *criminal intent*) (Sykes & Matza, 1957, 666).

Sykesin ja Matzan (1957, 666) väitteen[6] mukaan suuri osa nuorisorikollisuudesta rakentuu poikkeavuuden oikeutuksen (engl. *justifications for deviance*) perustalle. Oikeutuksesta käytetään myös ilmaisua rationalisointi[7]. Sykesin ja Matzan (1957, 667) mukaan poikkeavaan ja rikolliseen elämäntyyliin päädytään oppimisprosessin kautta. Sykes ja Matza (1957, 667) esittävät:

> "It is by learning these techniques that the juvenile becomes delinquent, rather than by learning moral imperatives, values or attitudes standing in direct contradiction to those of the dominant society." (Sykes & Matza, 1957, 667)

Tuossa prosessissa ei opita vallitsevan yhteiskunnan vastaisia arvoja ja asenteita, vaan eri tekniikoiden avulla opitaan neutralisoimaan poikkeavasta

---

[5] Kategorinen imperatiivi viittaa Immanuel Kantin etiikan keskeiseen periaatteeseen, jonka mukaan on toimittava vain sellaisten periaatteiden mukaan, joista voisi muodostaa yleisen lain. (Tieteen termipankki, 2016)

[6] "It is our argument that much delinquency is based on what is essentially an unrecognized extension of defenses to crimes, in the form of justifications for deviance that are seen as valid by the delinquent but not by the legal system or society at large."(Sykes & Matza, 1957, 666)

[7] Rationaalistaa, rationalisoida tarkoittaa 1) järkeistää, tehdä järkiperäiseksi, tarkoituksenmukaiseksi, 2) psykologiassa sana tarkoittaa järkeistää, etsiä järkiperäistä tai sosiaalisesti hyväksyttäviä vaikuttimia teoille, jotka ovat varsinaisesti niitä vailla, 3) taloudessa sana tarkoittaa toimia työn hyötysuhteen ja tuottavuuden kohottamiseksi. (Turtia, 2010, 479)

käyttäytymisestä aiheutuvaa tai seurannutta syyllisyyttä ja häpeää. Yksilö suojelee neutralisoinnin avulla itseään omilta itsesyytöksiltään[8] ja järkeistää poikkeavaa tekoaan sillä, että jos teko ei nyt niin oikein ollutkaan, se on silti hyväksyttävää.[9] Sykes ja Matza (1957, 667) teorian keskeisenä argumenttina voidaan pitää sitä, että neutralisoinnilla ei tarkoiteta yksinomaan poikkeavan tai rikollisen teon jälkeistä oikeutusta. Teorian mukaan rationalisointi (neutralisointi) voi edeltää tekoa, jolloin poikkeavuuden oikeutus toimii rikollisuuden mahdollistajana[10]. Tähän teorian jopa kriittiseen osuuteen on kohdistunut paljon arvostelua, jota käsitellään myöhemmin tässä luvussa. Sykes ja Matza (1957, 667) viittaavat[11] siihen, kuinka useat rikolliset näyttäisivät olevan tietoisia erilaisista sosiologisista ja psykologisista selitysmalleista, mutta eivät tarkemmin käsittele näiden selitysmallien yhteyttä rikollisuuden mahdollistajana. Koska Sykes ja Matza eivät teoriassaan keskittyneet siihen, missä tekniikoiden oppimisprosessi tapahtuu, voidaan olettaa, että oppiminen tapahtuu Sutherlandin teorian mukaisesti vuorovaikutuksessa muiden kanssa. Tämän tutkimuksen rajaus sulkee kuitenkin oppimisteorioiden laajemman käsittelyn tutkimuksen ulkopuolelle.

Sykes ja Matzan teoriassa opintosisältö, eli poikkeavan käyttäytymisen oikeuttamisen tekniikat, on jaettu viiteen päätyyppiin ja ne muodostavat keskeisen sisällön koko teoriasta. Tekniikoita kutsutaan neutralisoimis-tekniikoiksi ja ne on nimetty: denial of responsibility (*vastuun kieltäminen*), denial of injury (*vahingon kieltäminen*), denial of victim (*uhrin kieltäminen*), condemnation of the condemners (*tuomitsijoiden tuomitseminen*) ja appeal to higher loyalties (*vetoaminen korkeampiin lojaliteetteihin*). (Sykes & Matza, 1957, 667–669.) Seuraavaksi käydään läpi kunkin neutralisoimistekniikan sisältö.

2.2.1 Vastuun kieltäminen

Sykesin ja Matzan (1957, 667) mukaan vastuun kieltämisen (engl. *denial of responsibility*) tarkoituksena on torjua tai vähentää sosiaalisten normien rikkomisesta aiheutuvia rikollisen omia itsesyytöksiä sekä muiden osoittamaan paheksuntaa tai tuomitsevuutta. Sykes ja Matza (1957, 667) esittävät:

> "As a technique of neutralization, however, the denial of responsibility extends much further than the claim that deviant acts are an "accident" or some similar negation of personal accountability." (Sykes & Matza, 1957, 667)

---

[8] "They are viewed as following deviant behavior and as protecting the individual from self-blame and the blame of others after the act." (Sykes & Matza, 1957, 667)

[9] "In this sense, the delinquent both has his cake and eats it too, for he remains committed to the dominant normative system and yet so qualifies its imperatives that violations are "acceptable" if not "right."" (Sykes & Matza, 1957, 667)

[10] "They are viewed as following deviant behavior and as protecting the individual from self-blame and the blame of others after the act. But there is also reason to believe that they precede deviant behavior and make deviant behavior possible." (Sykes & Matza, 1957, 666)

[11] "A number of observers have wryly noted that many delinquents seem to show a surprising awareness of sociological and psychological explanations for their behavior and are quick to point out the causal role of their poor environment." (Sykes & Matza, 1957, 667)

Neutralisoimismenetelmänä vastuun kieltäminen ulottuu siis pidemmälle kuin väitteeseen, että poikkeava teko olisi onnettomuus. Sykes ja Matza (1957, 667) selittävät:

> "It may also be asserted that delinquent acts are due to forces outside of the individual and beyond his control such as unloving parents, bad companions, or a slum neighborhood. In effect, the delinquent approaches a "billiard ball" conception of himself in which he sees himself as helplessly propelled into new situations." (Sykes & Matza, 1957, 667)

Eli rikollinen voi siis väittää, että hänen tekonsa johtuvat ulkopuolisista tekijöistä tai vaikutteista, kuten rakkaudettomista vanhemmista, huonosta seurasta tai huonosta asuinalueesta (slummista). Rikollinen näkee itsensä ikään kuin olosuhteiden uhrina tai ympäristön tuotteena. Sykesin ja Matzan (1957, 667) mukaan:

> "From a psychodynamic viewpoint, this orientation toward one's own actions may represent a profound alienation from self, but it is important to stress the fact that interpretations of responsibility are cultural constructs and not merely idiosyncratic beliefs." (Sykes & Matza, 1957, 667)

Vapaasti suomennuttuna vastuun kieltäminen voi psykodynaamisesta näkökulmasta edustaa syvällistä vieraantumista itsestään, mutta Sykesin ja Matzan mielestä on kuitenkin tärkeä korostaa sitä, että vastuun tulkitseminen on kulttuurin muodostama eikä omaperäinen uskomus. (Sykes & Matza, 1957, 667.) Tässä neutralisoimismenetelmässä Sykes ja Matza (1957, 667) viittavat oppimiseen:

> "By learning to view himself as more acted upon than acting, the delinquent prepares the way for deviance from the dominant normative system without the necessity of a frontal assault on the norms themselves." (Sykes & Matza, 1957, 667)

Tämän tutkimuksen tulkinnan mukaan Sykes ja Matza tarkoittivat teoriassaan, ettei rikollisen tarvitsisi käydä vallitsevia arvoja tai normeja vastaan, koska hän oppii näkemään itsensä vallitsevan kulttuurin ja ympäristön tuotteena. Muut ihmiset ja ympäristö ikään kuin hallitsevat niin vahvasti, ettei yksilö koe olevansa vastuussa siihen, mihin tilanteeseen on joutunut tai mitä tekee. Koska Sykes ja Matza viittaavat teoriassaan kulttuurin rakenteisiin (engl. *cultural constructs*), tämän tutkimuksen tulkinnan mukaan on oletettavaa, että vastuun kieltämiseen sisältyy silloin jokin kulloinkin kyseessä olevan kulttuurin yleisesti hyväksytty selitys. Eli yksilön ei ikään kuin tarvitse edes ottaa vastuuta elämästään eikä tekemisistään, kunhan oppii yleisesti hyväksytyn selityksen, jolla oikeuttaa sosiaalisista normeista poikkeamisen. Sykes ja Matza teoria jättää kuitenkin epäselväksi, miksi kokea syyllisyyttä ja häpeää, jos selitys on yleisesti hyväksytty. Toisaalta Sykes ja Matza eivät teoriassaan käsittele, sisäistääkö yksilö ensin sosiaalisen normin, jonka jälkeen hänelle opetetaan vallitsevan kulttuurin hyväksytyt selitykset. Minor (1981, 300) ei pohdi vastuun kieltämisen tekniikkaa samankaltaisesti, mutta viittaa silti siihen, kuinka ehdollinen moraali on helpommin ylitetty kuin ehdoton moraali, joten yhteiskunta, joka hyväksyy rikoksille useita tekosyitä, helpottaa samalla hienovaraisesti näitä rikoksia.

2.2.2 Vahingon kieltäminen

Toisen neutralisoimistekniikan sisältö keskittyy rikollisen tai poikkeavan teon tekemisestä aiheutuvan vahingon kieltämiseen (engl. *denial of injury*). Sykes ja Matza (1957, 667) esittävätkin:

> "For the delinquent, however, wrongfulness may turn on the question of whether or not anyone has clearly been hurt by his deviance, and this matter is open to a variety of interpretations." (Sykes & Matza, 1957, 667)

Rikollinen kyseenalaistaa, onko joku selvästi kärsinyt hänen rikollisesta tai poikkeavasta toiminnastaan, ja tämä kyseenalaistus on avoin erilaisille tulkinnoille. Sykes ja Matza (1957, 667) mainitsevat:

> "Vandalism, for example, may be defined by the delinquent simply as "mischief"-after all, it may be claimed, the persons whose property has been destroyed can well afford it. Similarly, auto theft may be viewed as "borrowing," and gang fighting may be seen as a private quarrel, an agreed upon duel between two willing parties, and thus of no concern to the community at large." (Sykes & Matza, 1957, 667)

Rikollinen tulkitsee esimerkiksi ilkivallan olleen vain vahinko tai kepponen, tai autovarkaus olikin vain auton lainaamista. Rikollinen siis tietää toimivansa lainvastaisesti, mutta tulkitsee, ettei toiminta aiheuta suurta tai merkittävää haittaa. Sykes ja Matza (1957, 667) viittaavat kriminologiassa tunnettuihin oikeudenvastaisten tekojen erotteluun "*mala in se*" ja "*mala prohibita*"[12]. Samoin rikollinen voi tehdä samankaltaista erottelua arvioidessaan tekojensa vakavuuden ja niiden seurausten välistä yhteyttä. (Sykes & Matza, 1957, 667.) Erottelu siitä, mikä on yksiselitteisesti rikollista toimintaa ja mikä puolestaan kulttuurillisesti hyväksyttävää tai suvaittua käyttäytymistä, ei aina ole selkeä (Carrabine ym., 2004, 131). Toisaalta Sykes ja Matza (1957, 668) viittaavat:

> "Since society sometimes agrees with the delinquent, e.g., in matters such as truancy, "pranks," and so on, it merely reaffirms the idea that the delinquent's neutralization of social controls by means of qualifying the norms is an extension of common practice rather than a gesture of complete opposition." (Sykes & Matza, 1957, 668)

Yhteiskunta/yhteisö on siis toisinaan rikollisen kanssa yhtä mieltä siitä, että toiminta on pikemmin yleisen käytännön jatke kuin sen vastakohta.

Tämän tutkimuksen tulkinnan mukaan opintosisältönä vahingon kieltämiseen liittyy eräs ristiriita. Jos yhteiskunta tai yhteisö jättää tulkinnan varaiseksi rikollisen tai sosiaalisista normeista poikkeavan teon vakavuuden ja seurausten välisen yhteyden, miksi yksilö edes kokisi teostaan syyllisyyttä ja häpeää, jota lieventääkseen kieltää vahingon.

[12] "Mala in se –termillä tarkoitetaan pahaa itsessään, kun taas mala prohibata –termillä tarkoitetaan pahaa, koska se on kielletty. Mala in se –termillä viitataan asioihin, jotka luontaisesti tuomitaan ja jotka säilyvät rikoslaissa aikakaudesta toiseen." (Laine, 2007, 19, 34).

2.2.3 Uhrin kieltäminen

Kolmas neutralisoimistekniikka, uhrin kieltäminen (engl. *denial of victim*), liittyy moraalitunteiden kumoamiseen. Sykes ja Matza (1957, 668) esittävät:

> ”Even if the delinquent accepts the responsibility for his deviant actions and is willing to admit that his deviant actions involve an injury or hurt, the moral indignation of self and others may be neutralized by an insistence that the injury is not wrong in light of the circumstances. The injury, it may be claimed, is not really an injury; rather, it is a form of rightful retaliation or punishment.” (Sykes & Matza, 1957, 668)

Vaikka rikollinen hyväksyisi olevansa vastuussa aiheuttamastaan teosta, hän ei silti koe tehneensä olosuhteisiin nähden mitään väärää. Pikemminkin hän kokee tekonsa eräänlaisena laillisena kostona tai rangaistuksena, jossa uhri muutetaan väärintekijäksi (engl. *the victim is transformed into a wrong-doer)* (Sykes & Matza, 1957, 668). Esimerkkeinä Sykes ja Matza (1957, 668) mainitsevat:

> ”Assaults on homosexuals or suspected homosexuals, attacks on members of minority groups who are said to have gotten "out of place," vandalism as revenge on an unfair teacher or school official, thefts from a "crooked" store owner-all may be hurts inflicted on a transgressor, in the eyes of the delinquent.” (Sykes & Matza, 1957, 668)

Vähemmistöryhmien edustaja, virkamies tai vaikkapa yrittäjä voikin olla rikollisen silmin syyllinen eikä hän itse. Oikeutta voidaan etsiä myös lain ulkopuolelta, kuten Sykes ja Matza (1957, 668) mainitsevat*:*

> ”... Robin Hood, and his latter day derivatives such as the tough detective seeking justice outside the law, still capture the popular imagination, and the delinquent may view his acts as part of a similar role.” (Sykes & Matza, 1957, 668)

Rikollinen voi siis kokea olevansa hyväntekijä eikä rikollinen. Myös rikoksen uhrin olemassaolon kieltäminen liittyy tähän kolmanteen tekniikkaan. Sykes ja Matza (1957, 668) selittävät:

> ”Insofar as the victim is physically absent, unknown, or a vague abstraction (as is often the case in delinquent acts committed against property), the awareness of the victim's existence is weakened.” (Sykes & Matza, 1957, 668)

Kun uhri on fyysisesti poissa, tuntematon tai epämääräisen abstrakti, kuten tilanne muun muassa omaisuusrikoksissa usein on, tietoisuus uhrin olemassa olosta sivuutetaan. Sykes ja Matza (1957, 668) lisäävät vielä:

> ”Internalized norms and anticipations of the reactions of others must somehow be activated, if they are to serve as guides for behavior; and it is possible that a diminished awareness of the victim plays an important part in determining whether or not this process is set in motion.” (Sykes & Matza, 1957, 668)

Sisäistetyt normit ja toisten reaktioiden ennakointi on jotenkin aktivoitava, jotta ne toimisivat käyttäytymisen oppaina; ja on mahdollista, että heikentynyt tietoisuus uhrin olemassa olosta on tärkeä osa määritettäessä, aloitetaanko tämä prosessi vai ei.

Tämän tutkimuksen tulkinnan mukaan Sykes ja Matza eivät teoriassaan selitä, mikä tietyssä tilanteessa käynnistää prosessin, kun uhri ei ole poissa, tuntematon tai abstrakti, eli tietoisuus uhrin olemassa olosta ei ole heikentynyt.

2.2.4 Tuomitsijoiden tuomitseminen

Neljäs neutralisoimistekniikka, tuomitsijoiden tuomitseminen (engl. *condemnation of the condemners*), liittyy siihen, kuinka rikollinen siirtää huomion itsestään kohti yhteiskunnan tai yhteisön normien tai lakien noudattamista valvoviin tahoihin. Sykes ja Matza (1957, 668) selittävät:

> "The delinquent shifts the focus of attention from his own deviant acts to the motives and behavior of those who disapprove of his violations. This orientation toward the conforming world may be of particular importance when it hardens into a bitter cynicism directed against those assigned the task of enforcing or expressing the norms of the dominant society. Police, it may be said, are corrupt, stupid, and brutal." (Sykes & Matza, 1957, 668)

Rikollinen voi väittää esimerkiksi poliisia korruptoituneeksi, jolloin poliisilla ei olisi oikeutta tuomita toisia. Sykes ja Matza (1957, 668) kuvailevat vielä:

> "The delinquent, in effect, has changed the subject of the conversation in the dialogue between his own deviant impulses and the reactions of others; and by attacking others, the wrong- fulness of his own behavior is more easily repressed or lost to view." (Sykes & Matza, 1957, 668)

Hyökkäämällä niitä kohtaan, jotka eivät hyväksy rikollisen toimintaa, oma lainvastainen käytös on helpompi peittää tai kadottaa.

Sykes ja Matza (1957, 667) tuovat teoriassaan esille, ettei rikollinen edusta radikaalia vastarintaa (engl. *radical opposition*) lainkuuliasta yhteiskuntaa kohtaan. Kuitenkin tuomitsijoiden tuomitseminen -neutralisoimistekniikassa rikollinen haluaa siirtää huomion niihin, jotka valvovat yhteiskunnan normien noudattamista, syyttämällä esimerkiksi poliisia korruptoituneeksi. Tämän tutkimuksen tulkinnan mukaan opintosisältö viittaa ikään kuin siihen, että lakien ja normien olemassaolo on rikollisen mielestä täysin ymmärrettävää ja asianmukaista, mutta noudattamista valvovien tahojen tai instanssien toiminta puolestaan ei.

2.2.5 Vetoaminen korkeampiin lojaliteetteihin

Vetoaminen korkeampiin lojaliteetteihin (engl. *appeal to higher loyalties*) on viimeinen neutralisoimistekniikka, ja liittyy sisäisten ja ulkoisten sosiaalisten kontrollien vaatimuksiin. Sykesin ja Matzan (1957, 669) mukaan:

> "Internal and external social controls may be neutralized by sacrificing the demands of the larger society for the demands of the smaller social groups to which the delinquent belongs such as the sibling pair, the gang, or the friendship clique. It is important to note that the delinquent does not necessarily repudiate the imperatives of the dominant normative system, despite his failure to follow them." (Sykes & Matza, 1957, 669)

Vaikka rikollinen ei kiistäisi vallitsevan normatiivisen järjestelmän (yhteiskunta/yhteisö) välttämättömiä vaatimuksia, hän ei silti noudata niitä. Vaatimukset ikään kuin sivuutetaan pienempien sosiaalisten ryhmien, kuten sisarusten, jengin tai ystävyyssuhteiden vuoksi. Sykes ja Matza (1957, 669) selittävät:

> "... the most important point is that deviation from certain norms may occur not because the norms are rejected but because other norms, held to be more pressing or involving a higher loyalty, are accorded precedence. Indeed, it is the fact that both sets of norms are believed in that gives meaning to our concepts of dilemma and role conflict." (Sykes & Matza, 1957, 669)

Normeista poikkeavuus ei johdu yhteiskunnan normeista itsessään, vaan muuhun sosiaaliseen siteeseen liittyy suurempi lojaliteetti. Vaikka molempiin normeihin siis uskotaan, saattaa yleisten sosiaalisten velvollisuuksien ja ystävyyden välille syntyä rooliristiriita. (Sykes & Matza, 1957, 669.)

Tämän tutkimuksen tulkinnan mukaan rikollinen ikään kuin uskoo tai oppii uskomaan, että lain tai normin rikkominen hyödyttää hänen vahvaa sosiaalista sidettään enemmän kuin lain tai normin mukainen käyttäytyminen. Jos siis yksilö on sisäistänyt yhteiskunnan tai yhteisön sosiaaliset normit, ja niistä poikkeaminen tuottaa syyllisyyttä ja häpeää, on oletettavaa, että tietyssä tilanteessa, henkilössä tai asiassa on yksilölle jotain lain tai normin noudattamista merkittävämpää. Sykes ja Matza eivät kuitenkaan teoriassaan käsittele sitä, mikä saa tietyssä tilanteessa yksilön priorisoimaan lojaliteettia.

"En tarkoittanut sitä", "En todellakaan vahingoittanut ketään", "Siitäs saivat", "Kaikki vain kiusaavat minua" ja "En tehnyt sitä itseni vuoksi" ovat selityksiä, joilla rikolliset oikeuttavat tekojaan. Nämä oikeuttamisen ajattelumallit eivät kuitenkaan ole uusia asioita tai jonkin ideologian luomuksia, vaan ne ovat laajennoksia vallitsevan yhteiskunnan (engl. *society*) yleisistä ajattelutavoista[13]. (Sykes & Matza, 1957, 669.)

Marunan ja Copesin (2005, 255) tulkinnan mukaan yksilö pyrkii neutralisoinnin avulla suojelemaan itseään omantunnontuskilta, kognitiiviselta dissonanssilta, syyllisyydeltä, häpeältä, katumukselta, itsekunnioituksen menetykseltä, julkiselta leimaamiselta tai häpeänleimalta. Tämän tutkimuksen tulkinnan mukaan Maruna ja Copes (2005, 255) viittaavat siihen, että yksilön on selitettävä ja perusteltava sekä itselleen että jollekin toiselle poikkeavan tai rikollisen teon olleen hyväksyttävää. Neutralisointia ei pidä sekoittaa petokseen, huijaukseen tai vilppiin (engl. *deceit*) (Maruna & Copes, 2005, 230). Eräs neutralisoinnin lähikäsitteistä on itsepetos (engl. *self-deception*). Neutralisointi (rationalisointi) eroaa kuitenkin itsepetoksesta, eivätkä käsitteet siten ole tässä tutkimuksessa synonyymejä. Itsepetoksessa voidaan vältellä totuutta samaan tapaan kuin neutralisoinnissa, mutta siinä missä itsepetoksen prosessit voivat olla tiedostamattomia (Ten-

[13] "These "definitions of the situation" represent tangential or glancing blows at the dominant normative system rather than the creation of an opposing ideology; and they are extensions of patterns of thought prevalent in society rather than something created de novo." (Sykes & Matza, 1957, 669)

brunsel & Messick, 2004, 225) neutralisointi edellyttää, että yksilö ymmärtää toimivansa sisäistettyjen normien vastaisesti. Onkin oletettavaa, että päätös poikkeavasta teosta tai lain rikkomisesta edellyttää yksilön tietoista perusteltua päätöstä. Vaikka itsepetokseen liittyykin paradoksi siitä, että yksilön on tiedettävä, että on jotain, mitä on piilotettava ja pidettävä salassa (Tenbrunsel & Messick, 2004, 226), tämän tutkimuksen tulkinnan mukaan neutralisoinnissa on silti olemassa lisäksi joku ulkopuolinen, jolle yksilö kokee olevansa selitysvelvollinen.

2.3 Neutralisoimisteorian soveltaminen

Neutralisoimisteoriaa on sovellettu erittäin laajasti, ja sitä pidetään yhtenä kaikkein luovimpana ja visionäärisimpänä teoreettisena kehityksenä viime vuosisadan kriminologiassa (Maruna & Copes, 2005, 224-225). Neutralisoimisteorialla onkin ollut vaikutusta myös rikosoikeudellisiin järjestelmiin ja rangaistusten menettelytapoihin (Maruna & Copes, 2005, 239). Lisäksi on viitteitä siitä, että neutralisoimisteorian soveltamisalaa on mahdollista laajentaa perinteisten arvojärjestelmärajojen yli ja soveltaa kaikentyyppisiin rikollisiin riippumatta siitä, miten tärkeitä tavanomaiset tai epätavanomaiset arvot heille ovat (Topallin, 2005, 797-798, 823). Maruna ja Copes (2005, 223) viittaavat Hazanin (1991) toteamukseen siitä, kuinka neutralisoimistekniikat ovat yleismaailmallisia ja sovellettavissa missä tahansa tilanteessa, jossa toiminnan ja uskomusten välillä on epäjohdonmukaisuutta.

Sykesin ja Matzan (1957) muotoilema neutralisoimisteoria lieneekin yksi useimmin mainituista, merkittävimmistä ja vaikutusvaltaisimmista rikollista tai poikkeavaa käyttäytymistä selittävistä teorioista (Maruna & Copes, 2005, 222-223). Teorian avulla selitettäviä rikoksia ovat olleet muun muassa naisten väkivaltarikokset (Lattu, 2016), murha (Levi, 1981), kansanmurha (Alvarez, 1997) ja talousrikokset eli niin sanotut valkokaulusrikokset (Heath, 2008). Teoriaa on käytetty myös selittämään sitä, kuinka nykypäivän saksalaiset nuoret pyrkivät välttämään leimautumisen holokaustiin (Hazani, 1991). Neutralisoimisteoriaa on sovellettu myös ei-rikollisiin tutkimuksiin. Muun muassa Topallin (2005) tutkimus käsitteli sitä, kuinka niin sanotut kovan linjan huumekauppiaat sekä tasku- ja autovarkaat käsittelevät syyllisyyden tunteitaan toimiessaan epäsovinnaisia ja rikollisia arvoja vastaan. Muita poikkeavan käyttäytymisen neutralisointia käsitelleitä, ei-rikollisia tutkimuksia ovat muun muassa opiskelijoiden alkoholin käyttöön liittyvä neutralisointi (Piacentini ym, 2012), psykiatrisen sairaalan potilaiden pakkokeinoihin osallistuneiden vartijoiden hyödyntämät neutralisoimistekniikat (Johston & Kilty, 2016) sekä kuluttajien käyttämät neutralisoimistekniikat asenteiden ja todellisen käyttäytymisen välillä kestävän kehityksen mukaisessa ostokäyttäytymisessä (Gruber & Schlegelmilch, 2014). Neutralisoimisteoriaa tietoturvakontekstissa soveltaneet tutkimukset käsitellään tarkemmin luvussa neljä.

2.4 Neutralisoimisteoriaan liittyvää kritiikkiä

Vaikutusvaltaisuudestaan huolimatta Sykesin ja Matzan teoriaa on tulkittu eri tavoin ja siihen on kohdistunut myös kritiikkiä. Marunan ja Copesin (2005, 226) mukaan neutralisoimisteoria ei voi selittää kaikkia rikollisuuden ja poikkeavuuden ilmiöitä itsessään. Maruna ja Copes (2005, 248) viittaavat tutkimuksiin, joissa erityisesti taparikollisuuteen on yhdistetty muun muassa masentuneisuutta, stressaavia elämän tapahtumia, päihteiden käyttöä ja alhaista sosiaalista asemaa. Toisaalta Marunan ja Copesin (2005, 248-249) lisäävät vielä, kuinka niin sanotusti henkisesti terveilläkin ihmisillä on taipumus kääntää elämässään tapahtuvat myönteiset asiat omiksi ansioikseen ja taas puolestaan negatiiviset tapahtuvat ulkoisista tekijöistä aiheutuviksi. Lisäksi persoonallisuustyypit voivat vaikuttaa siihen, kuinka vastuussa yksilö kokee omasta käyttäytymisestään olevan (Maruna & Copes, 2005, 250). Vaikka edellä mainituilla tutkimuksilla onkin liittymäpintaa neutralisoimisteoriaan ja sen keskeiseen sisältöön, ei tämän tutkimuksen kontekstissa voida käsitellä laajasti eri ulottuvuuksia, joiden avulla ihminen suojelee itseään itsesyytöksiltä tai kielteisiltä mielikuvilta itsestään. Muun muassa Leon Festinger vuonna 1957 julkaisema kognitiivisen dissonanssin teoria viittaa uskomusten ja käyttäytymisen väliseen ristiriitaan, ja siihen, kuinka yksilö voi järkeistämällä minimoida dissonanssin tunnetta (Festinger, 1957).

Topalli (2005, 798) esittää:

> ”The underlying assumption of neutralization theory was (and is) that delinquents, despite their involvement with offending, maintain a strong bond to conventional society and are invested in maintaining a perception of themselves as good. To resolve their contemplated law-breaking with this desired self-identity, they use neutralization techniques—preemptive self-talk justifications and excuses—to assuage anticipated guilt.” (Topalli, 2005, 798.)

Topallin tulkinnan mukaan neutralisoimisteorian taustaolettama on, että rikollisuudestaan huolimatta rikolliset ylläpitävät vahvan siteen vallitsevaan yhteiskuntaan. Kunnollisuuden minäkuvaa ylläpitääkseen rikolliset käyttävät neutralisointitekniikoita, eli ennaltaehkäiseviä perusteluja ja tekosyitä ennakoidun/odotetun syyllisyyden lieventämiseksi. (Topalli, 2005, 798.) Maruna ja Copes (2005, 230-231) nostavat Sykes ja Matzan (1957, 666) teoriasta kohdan ”*precede deviant behavior and make deviant behavior possible*”. Marunan ja Copesin tulkinnan mukaan[14] Sykes ja Matza ehdottivat tiettyä kronologista järjestystä, eli neutralisoinnit eivät ole pelkästään teon jälkeistä järkeilemistä, vaan neutrali-

[14] ”Finally and most important, Sykes and Matza (1957, p. 666) claim that neutralizations "precede deviant behavior and make deviant behavior possible." In this brief phrase, they make two crucial claims that are often overlooked in empirical work. First, they suggest a specific chronological sequence: neutralizations are not just a posteriori rationalizations; they precede delinquency and make deviant behavior possible. Second, and just as important, they emphasize that this order is not meant to imply a deterministic or causal relationship.” (Maruna & Copes, 2005, 231)

sointi (voi) edeltää rikollisuutta ja tehdä poikkeavan käytöksen siten mahdolliseksi. Lisäksi Maruna ja Copes ovat tulkinneet Sykes ja Matzan teoriaa siten, ettei edellä mainitun järjestyksen ole tarkoitus merkitä syy-yhteyttä (Marunan & Copesin, 2005, 231).

Vaikka esimerkiksi Topallin[15] (2005, 799) tulkinnan mukaan neutralisointia käytetään ennen rikoksen tekemistä, on tuohon etukäteen tapahtuvaan neutralisointiin kohdistunut myös kritiikkiä. Muun muassa Maruna ja Copes (2005, 221, 227) esittävätkin kysymyksen: miten voi neutralisoida jotain mitä ei ole vielä tehnyt. Toisaalta Maruna ja Copes nostavat ongelmaksi: miten etukäteispohdinnasta voitaisiin luotettavasti kerätä todisteita, ja kuinka neutralisoimistekniikoiden käyttämistä jälkikäteistarkastuksena voitaisiin mitata (Maruna & Copes, 2005, 227). Myös Agnew (1994, 555-556) mainitsee Sykes ja Matzan teoriaan liittyvistä haasteista, kuten muun muassa empiirisen tuen riittämättömyydestä. Lisäksi Agnew (1994, 555-556) esittää saman ongelman kuten Maruna ja Copes edellä, eli on vaikeaa määritellä, edeltääkö vai seuraavako neutralisointi rikollisuutta. Kuten tässä luvussa on aiemmin mainittu, Sykes ja Matza esittävät olevan syytä uskoa, että perustelut ja järkeilyt edeltävät poikkeavaa käyttäytymistä ja tekevät poikkeavan käyttäytymisen mahdolliseksi. Kuitenkaan he eivät teoriassaan selitä tai perustele, miten tai mistä sen voi havaita. Maruna ja Copes (2005, 271) rinnastavat ”neutralisointi ennen tekoa tai teon jälkeen” ikään kuin vastaavaksi syy-seuraus-ongelmaksi kuin ”kumpi oli ensin: muna vai kana”. Maruna ja Copes (2005, 230) kuitenkin korostavat huomioimaan empiirisissä tutkimuksissa neutralisoinnin järjestyksen.

Kuten jo aiemmin tässä luvussa on esitelty, Sykes ja Matza halusivat teoriallaan kumota käsityksen erillisestä rikollisten alakulttuurista, joka olisi ristiriidassa vallitsevien arvojen ja normien kanssa. Lisäksi Sykes ja Matza korostivat teoriansa alkuosassa neljän väitteen kautta sitä, ettei yksilö torju yhteisön yhdenmukaisuuden vaatimuksia (engl. *the demands for conformity*). Sykes ja Matzan teorian keskeinen sisältö taas keskittyy siihen, kuinka rikollinen pyrkii neutralisoimistekniikoiden avulla poistamaan sosiaalisten normien rikkomiseen liittyvät syyllisyyden ja häpeän tunteet. Agnew (1994, 555-556) tulkinnan mukaan Sykesin ja Matzan teoria keskittyi (nuoriso)rikollisiin, jotka olivat, enemmän tai vähemmän, tavanomaisiin arvoihin sitoutuneita (engl. *committed to conventional beliefs*). Sekä Topallin (2005, 804) että Agnew:in (1994, 555-556) mukaan on kuitenkin oletettavaa, etteivät esimerkiksi väkivaltarikolliset välttämättä ole edes sitoutuneet niin sanottuihin tavanomaisiin uskomuksiin (engl. *conventional beliefs)* ja arvoihin (engl. *conventional norms).* Kuten Topalli (2005, 804) mainitsee:”*...these individuals maintain little or no guilt for their offending behavior*”. Myös Minor (1981, 300) viittaa sitoutumiseen ja siihen, kuinka neutralisointi on tarpeetonta niille, jotka ovat sitoutuneet poikkeavuuteen (engl. *deviance*).

Minor (1981, 297-298) nostaa esille myös yhden neutralisoimistekniikan kaksitahoisuuden. Minorin mukaan uhrin kieltäminen –tekniikassa uhri, jonka

[15] ”Because they acknowledge that their behavior is wrong, they are forced to employ neutralizations before committing crimes to reconcile their offending with their desired self-image.” (Topalli, 2005, 799)

katsotaan ansaitsevan kohtalonsa, kuten esimerkiksi vähemmistöryhmän edustaja, ja uhri, jonka olemassaolo sivuutetaan, ovat merkitykseltään erilaiset. Minorin mukaan niin sanottu näkymätön uhri olisi käsitteellisesti lähempänä vahingon kieltämistä kuin uhrin kieltämistä. (Minor, 1981, 297-298.)

Tämän tutkimuksen tulkinta Sykes ja Matzan teoriaan liittyvistä haasteista on lisäksi se, ettei teoriassa selkeästi esitellä, kokeeko rikollinen itsensä poikkeavaksi, jolloin hän esimerkiksi kieltää vastuun ja puolustautuu muiden paheksunnalta neutralisoinnin avulla, vai oikeuttaako rikollinen tekonsa, jottei häntä leimattaisi poikkeavaksi. Toisaalta teoria ei myöskään selitä muun muassa sitä, mikä tietyssä tilanteessa on niin houkuttelevaa, että sosiaalisiin normeihin sitoutunut päätyy rikkomaan tai päättää rikkoa normeja.

Koska Sykes ja Matza esittävät teoriassaan, että oikeutukset ja perustelut ovat kulttuurisidonnaisia, ja ne opitaan sosiaalisen vuorovaikutuksen kautta, tämän tutkimuksen tulkinnan mukaan se voisi tarkoittaa, että poikkeavan teon tekijä tietäisi siten jo etukäteen, millainen teko tulisi aiheuttamaan syyllisyyttä ja häpeää. Voidakseen toimia sosiaalisista normeista poikkeavasti, tekijän olisi joko tiedettävä tai opittava ne keinot, joilla voisi järkeistää toimintaa tai opittava järkeistämään tai neutralisoimaan tekoon liittyvä syyllisyys. Myös Suoninen (1997) viittaa kulttuurisidonnaisuudella siihen, ettei yksilö voi valita mitä tahansa selitystä, vaan sen on oltava perusteltavissa kulttuurisesti hyväksyttävällä tavalla.

2.5 Tutkimusten haasteet

Neutralisoimisteoriaa on eri tutkimuksissa sovellettu hyödyntäen sekä kvalitatiivisia että kvantitatiivisia tutkimusmenetelmiä. Kvalitatiiviset tutkimukset ovat pääosin perustuneet haastatteluihin, ja kvantitatiiviset menetelmät ovat puolestaan keskittyneet mittaamaan neutralisointia muun muassa erilaisten asteikkojen ja luokittelujen avulla (Maruna & Copes, 2005, 259-260, 262-263). Molempiin tutkimussuuntiin liittyy kuitenkin omat haasteensa. Maruna ja Copes (2005, 260) mukaan kvalitatiivisessa tutkimuksessa jo tutkimusasetelma itsessään saattaa vääristää tutkimustulosta, koska haastattelutilanne tekee usein selväksi, kuka on poikkeva, jolloin haastateltava haluaa puolustaa itseään (Maruna & Copes, 2005, 260) ja neutralisoimistekniikat tarjoavat näin haastateltaville heidän kaipaamansa selityksen (Hindelang, 1970, 503). Topallin (2005, 802) mukaan haastatteluympäristökin saattaa vääristää tutkimustulosta. Laitosympäristö, kuten esimerkiksi vankila, voi vaikuttaa muistoihin ja arvioihin silloisista olosuhteista, jotka lopulta johtivat rikokseen. Näkemykset ja mielikuvat tapahtumasta voivat siten olla vääristyneitä. Maruna ja Copes (2005, 260) arvostelevat sitä, ettei kvalitatiivissa tutkimuksissa ole voitu kehittää neutralisoimisteoriaa lukuun ottamatta uusien neutralisoimistekniikoiden tunnistamista. Kvalitatiiviset tutkimukset eivät myöskään juuri koskaan sisällä vertailuryhmää. Tällöin tutkimus jättää epäselväksi sen, onko poikkeavan teon neutralisoinnissa kyse laajemmasta yhteiskunnan hyväksymästä uskomuksesta vai oliko kyse lopulta vain ainutlaatuisesta (uniikista) tutkimuksesta. Tästä syystä kvalitatiivisiin tutkimuksiin liittyy

aina näytteen valinnan ja yleistettävyyden ongelmat. (Maruna & Copes, 2005, 260.)

Jokainen tapahtuma, yhtä hyvin niin sanottu normaali kuin poikkeava, sisältää monia tulkintoja, jolloin yksilö saattaa tuntea syyllisyyttä ja häpeää asiasta, joka on toiselle täysin merkityksetön. Toisaalta täysin järkeväkin selitys voidaan tulkita järkeilynä tai itsepetoksena, tai päinvastoin, järkeily voidaan tulkita järkevänä selityksenä. (Mills, 1940, 970.) On myös täysin mahdollista, että ajan mittaan jonkin teon paheksunta häviää, mikä voi johtaa joko yhdenmukaisuuden vaatimuksiin mukautumiseen tai siihen, ettei yksilö koe edes tekevänsä mitään pahaa tai väärää (Minor, 1984, 1018). Myös Leon Festingerin (1957) luomassa kognitiivisen dissonanssin teoriassa viitataan uskomusten/asenteen ja käyttäytymisen väliseen ristiriitaan. Festinger (1962, 9) käyttää käsitettä kognitio (engl. *cognition*) viittaamaan tietämystä, joka yksilöllä on muun muassa itsestään, tunteistaan ja toiveistaan. Kun yksilö uskoo tai tietää, että hänen tulisi tehdä jotain, mutta jättää silti tekemättä, muodostuu näiden kahden kognition, uskomuksen ja todellisen teon, välille ristiriita, joka ikään kuin herättää kognitiivisen dissonanssin tilan. Yksilö pyrkii epämiellyttävästä tunteesta eroon joko muuttamalla uskomusta/asennetta tai käyttäytymistään. (Festinger, 1962, 6-8.) Festinger (1962, 2) käyttää esimerkkinä tupakointia, eli tupakoitsija tietää tupakoinnin terveyshaitat, mutta tuntee silti nauttivansa tupakoinnista niin paljon, että tupakointi on sen arvoista, tai yksilö uskoo tai uskottelee itselleen, etteivät terveyshaitat ole niin vakavia, että niiden vuoksi lopettaisi tupakoinnin. Kun siis ajatusten, uskomusten tai asenteen ja toiminnan välistä ristiriitaa pyritään pienentämään tai poistamaan, siihen liittyvässä toiminnan oikeutuksessa on tunnistettavissa samankaltaisuutta kuin neutralisoinnissa. Lisäksi päätöksenteon jälkiseen vakuutteluun tai itselleen perusteluun liittyy samoja piirteitä kuin neutralisoinnissa.

Vaikka edellä mainituilla tutkimuksilla ja teorioilla onkin liittymäpintaa neutralisoimisteoriaan ja sen keskeiseen sisältöön, ei tämän tutkimuksen kontekstissa ole tarkoituksen mukaista käsitellä kaikkia ulottovuuksia, ja kognitiivisia vääristymiä, joiden avulla ihminen suojelee itseään itsesyytöksiltä tai kielteisiltä mielikuvilta itsestään. Sykes ja Matza (1957, 669-670) mainitsevat tutkimuksensa rajoitteet ja kehottavatkin tulevia tutkijoita järjestelmälliseen lähestymistapaan sekä pyrkimykseen ymmärtää paremmin neutralisoimistekniikoiden sisäistä rakennetta, kuten uskomuksia ja asenteita, sekä niiden suhdetta erilaiseen rikolliseen käyttäytymiseen.

3 TUTKIMUKSEN KESKEISET KÄSITTEET

Tässä luvussa esitellään tutkimukseen liittyviä keskeisiä käsitteitä. Luvun alku lähtee liikkeelle tietoturvaan ja sen hallintaan organisaatioympäristössä liittyvistä käsitteistä. Kuten johdanto luvusta käy ilmi, rajautuu tämän tutkimuksen keskiössä oleva ilmiö niin sanottuun inhimilliseen tietoturvaan. Tästä syystä tietoturvaan liittyvien käsitteiden määrittelyssä painotus on enemmän yksilön toiminnassa kuin tietoturvan teknisessä näkökulmassa. Jotta kaikki eri käsitteet voidaan sitoa tutkimuksen niin sanottuna punaisena lankana toimineen Sykes ja Matza (1957) neutralisoimisteorian olettamuksiin, on käsitteiden määrittelyssä tukeuduttu joiltain osin myös muihin kuin tietojärjestelmätieteessä käytettyihin määritelmiin. Tutkimuksen kontekstissa ei ole relevanttia käydä läpi eri käsitteiden ja määritelmien historiallisia taustoja ja kehitystä, vaan käsitemäärittelyn kautta rajataan tutkimusongelmaa ja pyritään yleisellä tasolla kuvailemaan, mitä eri käsitteillä tässä tutkimuksessa tarkoitetaan.

3.1 Tietoturva

> ”Onnellinen se, joka on löytänyt viisauden, se joka on tavoittanut tiedon, sillä parempi on viisaus kuin hopea, tuottoisampi on tieto kuin kulta.” (Raamattu, Sananlaskujen kirja 3:13-18)

Vaikka tiedon sanotaan olevan arvokkuudeltaan tämän ajan öljy, edellä mainittu sitaatti osoittaa, ettei tiedon arvokkuuden korostaminen kuitenkaan ole aiheena uusi, vaan tiedon arvo ymmärrettiin jo muinaisina aikoina. Tämän päivän sähköisessä muodossa oleva tieto on kuitenkin voimavarana erittäin haavoittuvainen, koska niillä tekniikoilla, joilla tietoa muun muassa välitetään, kerätään, tallennetaan ja käsitellään nopeasti ja helposti esimerkiksi digitaalitalouden käyttöön, samoilla tekniikoilla tietoa voidaan myös vahingoittaa, muuttaa tai tuhota (Humphreys, 2016, 3). Tämän päivän tietojenkäsittely-ympäristö sisältää lukuisia organisaation toiminnan kannalta arvokkaita, suojattavia tietoja ja kohteita (Safa ym., 2015, 66). Moni organisaation toiminta on tänä päivänä täysin riippuvainen

erilaisten tietojen hyödynnettävyydestä (Humphreys, 2016, 5). Tuo riippuvuus lisää kuitenkin myös mahdollisia tietoturvaan kohdistuvia uhkia ja riskejä (Humphreys, 2016, 4-5). Organisaation tietoturvatoimintaa voikin tänä päivänä kuvata riskien hallinnaksi (Bodin, Gordon & Loeb, 2008, 1), jonka tarkoituksena on säilyttää tiedon luottamuksellisuus, eheys ja saatavuus (Hsu, Lee & Straub, 2012, 919). Riskien hallinnan keinona voidaan esimerkiksi tietoturvauhka-analyysin avulla määritellä ne organisaation kriittiset toiminnat ja tiedot, joita halutaan turvata. Samalla voidaan arvioida tietoturvauhkat, joilta halutaan suojautua sekä peilata organisaation omia haavoittuvuuksia suhteessa uhkien todennäköisyyteen. (Raggad, 2010, 113, 291-292; Höne & Eloff, 2002, 402; Peltier, 2014, 44.) Riskejä voidaan arvioida tiedon luottamuksellisuuteen, eheyteen ja saatavuuteen kohdistuvien uhkien perusteella. Riskianalyysin avulla voidaan tehdä päätöksiä riskin pienentämiseksi, siirtämiseksi tai hyväksymiseksi (Safa ym., 2015, 66; Peltier, 2014, 51- 55; Raggad, 2010, 305).

Huolimatta siitä, että tietoturvasta puhutaan paljon, eikä tietoturva sanaa voida tänä päivänä sivuuttaa missään organisaatioympäristössä, tietoturvan määrittelyn vaikeutena on se, etteivät määritelmät niinkään kerro mikä tietoturva on, vaan mitä se tekee (Andersonin, 2003, 309-310). Tietoturvaa on määritelty muun muassa seuraavasti:

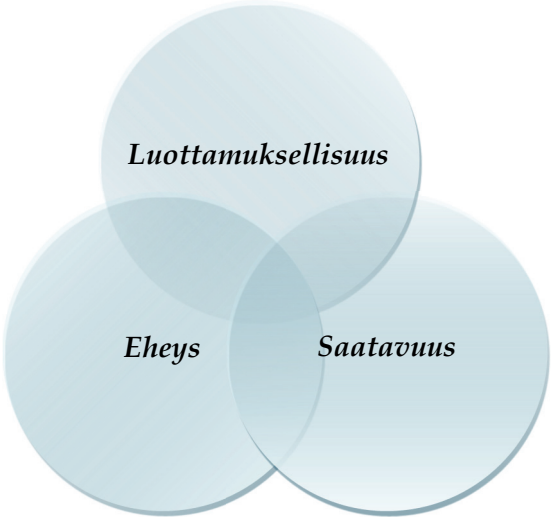
> ”Tietoturvallisuudella tarkoitetaan tietojen ja palvelujen, järjestelmien ja tietoliikenteen suojaamista ja varmistamista niihin kohdistuvien riskien hallitsemiseksi sekä normaali- että poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä. Tietoturvallisuuden tavoitteena on tietojen luottamuksellisuuden, eheyden ja käytettävyyden turvaaminen laitteisto- ja ohjelmistovikojen, luonnontapahtumien sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhilta ja vahingoilta.” (Vahti, 2009)

Vaikka edellä esitelty määritelmä on kattavuudessaan erittäin laaja, tarkastellaan seuraavaksi silti, mitä tietoturvan on tarkoitus tehdä tai mihin sillä pyritään.

Tietoturvalla halutaan suojautua muun muassa hyökkäyksiltä, jotka kohdistuvat tietoverkkoon, mutta yhtä hyvin suojautumista tarvitaan viruksilta, aggressiivisilta haittaohjelmilta, luonnonkatastrofeilta, sähkökatkoilta, varkauksilta, vandalismilta, sosiaaliselta manipuloinnilta (engl. *social engineering)* tai muilta ei-toivotuilta tapahtumilta (Andress, 2014, 3, 123). Ohjelmistojen ja vaikkapa lähdekoodien lisäksi organisaation toiminnan kannalta tärkeä fyysinen ympäristö ja siellä toimivat ihmiset kuuluvat osana turvattavaan kokonaisuuteen (Andress, 2014, 3). Fyysiseen ympäristöön voivat kuulua esimerkiksi toimitilat ja konesalit. Andress (2014, 3) korostaa kuitenkin sitä, miten ihmiset ovat usein arvokkain voimavara, jota ilman organisaation toimintaa ei voitaisi edes harjoittaa. Ilman ammattitaitoisia ihmisiä tietoturvan käyttäminen ja ylläpitäminen epäonnistuvat hyvinkin nopeasti huolimatta siitä, että kaikki muu omaisuus varmuuskopioineen pyrittäisiin suojaamaan katastrofia vastaan.

Raggad (2010, 17-18) määritteleekin tietoturvan tarkoittavan hallinnollisia ja teknisiä toimenpiteitä, joilla organisaation toiminnan ja palveluiden jatkuvuuden turvaavia tietoja ja tietojärjestelmiä suojataan luvattomalta käytöltä, tietojen

paljastumiselta, muuttamiselta tai tuhoutumiselta (Raggad, 2010, 17-18). Kansainvälisen tietoturvan hallintajärjestelmän ISO/IEC 27002 –standardin mukaan tietoturva koostuu kolmesta tiedolle asetetusta tavoitteesta, joita ovat luottamuksellisuus (engl. *confidentiality)*, eheys (engl. *integrity*) ja saatavuus (engl. *availability*) (Calder, 2008). Vaikka nämä niin sanotut tietoturvan kulmakivet (kuvio 2) eivät välttämättä auta määrittelemään sitä, mikä tietoturva on, niiden avulla on silti mahdollista tarkastella tietoturvan laajuutta.



KUVIO 2 Tietoturvallisuuden kulmakivet (mukaillen, Andress, 2014, 5)

Tiedon luottamuksellisuus ilmentää sitä, ettei tietoa luovuteta oikeudettomien prosessien tai henkilöiden käyttöön (Calder, 2008). Luottamuksellisuuden voidaan katsoa toteutuvan, mikäli kyetään todistamaan, että esimerkiksi salassa pidettäviin tietoihin on pääsy vain sallituilla käyttäjillä ja järjestelmillä. Luottamuksellisuuden ongelmasta taas kertoo esimerkiksi onnistunut salakatselu tai –kuuntelu, tai salassa pidettävien ja arkaluonteisten henkilötietojen luvaton käyttö tai luovuttaminen (Andress, 2014, 6). Teknologian avulla luottamuksellisuutta voidaan pyrkiä varmistamaan esimerkiksi salauksella, varmenteiden käytöllä, pääsyn- ja käytönvalvonnalla (Vacca, 2014; Bishop, 2003; Raggad, 2010, 27), mutta tekniikalla ei yksinomaan voida taata sitä, käsitteleekö esimerkiksi käyttäjä tietoja lopulta luottamuksellisesti. Tekniikka ei myöskään voi täysin varmistaa, ettei käyttäjä esimerkiksi lähetä sähköpostin liitetiedostoa väärälle taholle, tai ettei käyttäjä siirrä tai unohda luottamuksellisia tietoja väärään paikkaan.

Tiedon eheydellä tarkoitetaan sekä tiedon oikeellisuutta ja täydellisyyttä, että myös tiedon käsittelytapojen varmistamista siten, ettei tietoon kohdistu perusteettomia ja hallitsemattomia muutoksia (Calder, 2008). Eheyttä pyritään varmistamaan esimerkiksi salauksella, konfiguraatioiden hallinnalla, muutosten ja pääsyn hallinnalla, varmuuskopioinnilla ja erilaisilla lokitiedoilla (Raggad, 2010, 27; Casey, 2008). Lokitiedolla tarkoitetaan dokumenttia jonkin tapahtuman to-

teutumisesta jonakin tiettynä hetkenä (Valtiovarainministeriö, 2009). Vaikka teknisillä ratkaisuilla pyritään parantamaan tiedon eheyttä, tekniikalla ei vielä toistaiseksi pystytä täysin poistamaan esimerkiksi dokumentointivirheitä tai kaikkia ohjelmointivirheitä. Käyttäjän rooli eheyden turvaamisessa on edelleen merkittävä.

Tiedon saatavuudella tarkoitetaan sitä, että tietojen tulee olla käyttäjien ja tietojärjestelmien hyödynnettävissä haluttuna aikana (Calder, 2008). Saatavuuteen liittyvät ongelmat voivat johtua esimerkiksi sähköviasta, järjestelmä- tai sovellusvirheestä, palvelunestohyökkäyksestä tai muusta tietojärjestelmään kohdistuvasta hyökkäyksestä (Andress, 2014, 7). Saatavuuden turvaamiseen olevia teknologisia ratkaisuja ovat muun muassa verkonvalvonta, kahdennetut tiedot, ohjelmisto- ja datavarmistukset, järjestelmien klusterointi ja maantieteellinen hajauttaminen (Vacca, 2014; Raggad, 2010, 27). Vaikka organisaatiot ovat investoineet suuriakin summia esimerkiksi tieto- ja kyberturvallisuustekniikoihin ja erilaisiin tilannekuvajärjestelmiin, siltikään tekniikka ei ole toistaiseksi kyennyt poistamaan niin sanottuun kognitiiviseen hakkerointiin liittyviä riskejä. Tänä päivänä järjestelmän kaatava haittaohjelma voi aktivoitua yhtä hyvin verkkosivulla vierailun seurauksena kuin liitetiedoston avaamisen myötäkin. (Bone, 2017, 134-135, 70-72.) Tekniikka ei siis toistaiseksi ole vielä kyennyt täysin poistamaan käyttäjän toimista aiheutuvia tietoturvaongelmia.

Kuten jo aiemmin mainittiin, edellä esitellyt tietoturvan kolme niin sanottua kulmakiveä eivät välttämättä enää nykyisin kuvaa tietoturvaa riittävän kattavasti. Whitman ja Mattord (2011, 12-15) lisäävätkin luottamuksellisuuden, eheyden ja saatavuuden rinnalle myös tiedon tarkkuuden (engl. *accuracy*), autenttisuuden (engl. *authenticity*), käytettävyyden (engl. *utility*) ja hallittavuuden (engl. *possession)*. Tiedon tarkkuudella tarkoitetaan, että tieto on oikeaa ja virheetöntä. Tarkkuuteen liittyy luottamus siitä, ettei tietoon ole kohdistunut perusteettomia, tahallisia tai tahattomia, muutoksia. (Whitman & Mattord, 2011, 12.) Esimerkiksi henkilöiden ja pankin välinen maksuliikenne olisi haastavaa, mikäli tiedon tarkkuuteen ei voitaisi luottaa. Tiedon autenttisuus tarkoittaa, että tieto on alkuperäinen ja muun muassa siellä, missä se luotiin ja minne se sijoitettiin, varastoitiin tai siirrettiin (Whitman & Mattord, 2011, 12-13.) Tietoturvan kannalta autenttisuus tarkoittaa myös väärentämättömyyttä, eli esimerkiksi sitä, että digitaalinen objekti todella on se, mikä väittää olevansa. Whitman ja Mattord (2011, 12-13) nostavatkin autenttisuuden haasteeksi esimerkiksi sähköpostihuijaukset (engl. *email-spoofing)*, joissa käyttäjälle tutuksi naamioidun organisaation tai henkilön nimissä yritetään urkkia käyttäjän tunniste- ja/tai henkilötietoja. Tiedon hyödyllisyydellä tarkoitetaan, että pelkkä tiedon saatavuus ei tee vielä tiedosta arvokasta, vaan tiedon on oltava myös käyttäjälle hyödyllinen ja esitettynä ymmärrettävässä muodossa (Whitman & Mattord, 2011, 15). Tiedon hallinta tarkoittaa omistusoikeuden tai valvonnan laatua tai tilaa. Esimerkiksi tilanteessa, jossa organisaation entinen työntekijä päättäisi kopioida organisaation kriittisiä tietoja myydäkseen ne kilpailijalle, tietojen siirtyminen organisaation ulkopuolelle tarkoittaisi tiedon hallinnan rikkoontumista. Mikäli tiedot olisi kuitenkin salattu organisaation tietojärjestelmässä, ilman oikeaa salauksen purkamismenetelmää,

salattu tieto olisi hyödytön, eikä tiedon luottamuksellisuus välttämättä rikkoontuisi. (Whitman & Mattord, 2011, 15.) Tiedon hallinnan suojaaminen on kuitenkin tärkeä osa tietoturvaa, ja siihen kohdistuvat uhkat voivat aktivoitua ilman luottamuksellisuuden tai saatavuuden elementtejä (Parker, 1995).

Tietoturva kaikkineen on monimutkainen kokonaisuus, eikä siten tarkoita yksittäistä ohjelmistoa, laitetta, työkalua tai edes joukkoa erilaisia teknisiä ratkaisuja, vaan tietoturvan toteuttaminen edellyttää laajaa joukkoa isompia ja pienempiä organisaation strategioita, linjauksia ja päätöksiä. Samaan tapaan kuin tietojärjestelmä on hyödyllinen vain, jos ihmiset käyttävät sitä, myös erilaiset tietoturvatekniikat, strategiat, linjaukset, prosessit, ohjeet ja määräykset ovat hyödyllisiä vain, jos niitä oikeasti hyödynnetään (Siponen, 2000, 31). Tietoturva on organisaation omaa aktiivista toimintaa ja siten loputon prosessi, jolla suojataan organisaatioympäristössä olevia tietoja ja tietojärjestelmiä sekä siellä tuotettavia tietoja. Tietoturva vaatii jatkuvaa työtä, jota ei täysin voi ulkoistaa. (Baskerville ym., 2008, vii.) Seuraavaksi tarkastellaan sitä, miten tuota monimutkaista prosessia voidaan ohjata.

3.2 Tietoturvapolitiikka

Sanotaan, että ainoa todellinen tietoturvallinen järjestelmä on sellainen, joka on kytketty pois päältä, valettu betoniin ja sinetöity lyijypohjaiseen huoneeseen, jota vartiovat aseistetut vartijat, ja siltikin järjestelmän turvallisuutta voidaan edelleen epäillä (Andress, 2014, 3). Vaikka edellä mainittua järjestelmää voitaisiin pitää tasoltaan kohtuullisen turvallisena, se ei varmasti olisi käyttökelpoinen eikä tuottava. Turvallisuuden tason nosto saattaa siis vähentää tuottavuuden tasoa, ainakin hetkellisesti. (Andress, 2014, 3.) Se, kuinka äärimmäisen tiukaksi tietoturva viritetään, riippuu organisaation ylimmän johdon asettamista turvattavaan omaisuuteen liittyvistä hallintaprosesseista, mutta ennen kaikkea organisaation toimintaan liittyvistä strategioista (Raggad, 2010, 61-63; Von Solms & Von Solms, 2004, 372).

Peltierin (2014, 2) mukaan koko tehokkaan tietoturvatoiminnan päämäärät, tavoitteet ja menettelytavat arvioidaan ja asetetaan organisaation ylimmällä tasolla. Nämä päätökset eivät pakosti edellytä organisaation johdon syvällistä ymmärrystä tietoturvan teknisistä ratkaisuista. Sen sijaan ylimmän johdon tulee olla tietoinen tämän päivän tietojenkäsittely-ympäristön monimutkaisuudesta sekä kyetä arvioimaan, mitä tietoturvariskejä organisaation omaan toimintaa liittyy (Bone, 2017, 8).

Erilaiset standardit, kuten muun muassa ISO/IEC27001, PCI DSS ja NIST (Calder, 2008; Humphreys, 2016, 14; Wright, 2009; National Institute of Standards and Technology, NIST, 2013) tarjoavat niin sanottuja parhaita käytänteitä organisaation tietoturvan hallintaan, mutta yleisluonteisuutensa vuoksi ne eivät välttämättä sellaisenaan tarjoa organisaation todellisiin, päivittäisiin tarpeisiin liittyviä käytännön ohjeita (Siponen & Willison, 2009, 270; Höne & Eloff, 2002, 407-

409; Niemimaa & Niemimaa, 2017, 1-2). Standardit eivät juurikaan keskity työntekijöihin ja siihen, miten ohjataan, mitataan tai muutetaan heidän käyttäytymistään (Da Veiga & Eloff, 2010, 197). Organisaatio on useimmiten itse oman toimintansa paras asiantuntija, joten silloin se on myös paras asiantuntija oman tietoturvatoimintansa ohjaamiseen.

Standardien muokkaaminen organisaation tavoitteisiin ja käytäntöihin edellyttää pohdintaa siitä, mitä käytäntöjä organisaation tietoturvapolitiikkaan sisällytetään ja miksi. Tietoturvapolitiikka on dokumentti, joka selittää tietoturvan tavoitteet ja käsitteistöt kaikille organisaation käyttäjille. (Höne & Eloff, 2002, 402.) Tietoturvapolitiikassa tulisi yhdistää sekä tekniset että hallinnolliset ohjeet organisaation hyväksymälle tietoturvavaatimusten tasolle. Samalla dokumentaation tulee määritellä toimenpiteet asetettujen vaatimusten saavuttamiseksi, eli tietoturvan käytännön toteuttamiseen hyväksytyt ohjeet, turvatoimet ja käytännöt. (Karyda, Kiountouzis & Kokolakis, 2005, 248.) Tietoturvapolitiikka onkin tehokkaan tietoturvan kulmakivi (Peltier, 2014, 2), jossa määritellään riskit, vastuut ja tiedon turvaamisen periaatteet, eli esimerkiksi sen, miten tietoja turvataan, ketkä käyttäjät tai mitkä prosessit oikeutetaan käyttämään mitäkin tietoja sekä sen, millaiseen toimintaan tietojen käyttö hyväksytään. (Raggad, 2010, 11, 161, 172–180.)

Vaikka tietoturvapolitiikan tulisi siis ennen kaikkea ohjata toimintaa, tuo Vacca (2014, 34–35) esille sen, että edullisuudestaan huolimatta tietoturvapolitiikka on ohjauskeinona kuitenkin usein kaikkein vaikein toteuttaa. Jotta tietoturvapolitiikka tukisi ja ohjaisi organisaation toimintaa, hyvä tietoturvapolitiikka ei ole vain yksi dokumentti. Pikemminkin se voi olla joukko organisaation toiminnan eri osa-alueisiin määriteltyjä tietoturvapolitiikkoja. Näitä voivat olla esimerkiksi sähköpostiin, etätyöhön, mobiiliteknologian ja verkon resurssien käyttöön määritellyt käytännöt. Tietoturvapolitiikkojen on oltava helposti ymmärrettävä kokonaisuus ja niin kattavia, että ne ohjaavat työntekijöitä organisaation toiminnan kaikissa eri tilanteissa. (Vacca, 2014, 34–35, 43–50.). Tietoturvapolitiikat eivät ole vain teknisesti hallittavissa olevia käytäntöjä ja menettelyitä, vaan joukko ohjeita, joiden tarkoituksena on ohjata ja säädellä tietoturvakäyttäytymistä, ja määritellä organisaation työntekijöiden tehtävät ja vastuut tietojen ja resurssien turvaamiseksi (Bulgurcu ym., 2010, 526-527; Boss ym., 2009, 152–153). Tietoturvapolitiikkoja on säännöllisin väliajoin arvioitava suhteessa muuttuviin tai uusiin tietoturvariskeihin, (Vacca, 2014), koska on syytä muistaa, ettei organisaation tietoturvapolitiikalla ole vaikutusta organisaation ulkopuolella oleviin käyttäjiin (Von Solms, 1999). Vaikka tietoturvapolitiikkojen täytäntöönpano edellyttää sekä useiden toimintojen muokkaamista, että työntekijöiden menettelytapojen muuttamista (Karyda ym., 2005, 248), silti tietoturvapolitiikkoja on pidettävä organisaation mahdollisuuksina, eikä rajoittavina sääntökirjoina. Niiden painopisteen tulisi olla pitkän aikavälin muutosten saavuttamisessa niin työntekijöiden asenteessa tietoturvaa kohtaan kuin organisaation tietoturvakulttuurin luomiseksi. (Vacca, 2014, 19.) Samalla viestitään myös asiakkaille ja sidosryhmille,

että he voivat olla varmoja tietojensa asianmukaisesta hallinnoinnista ja suojaamisesta. Näin säilytetään samalla organisaation kannalta tärkeä maine sekä kilpailukyky. (Watkins, 2013, 15–17.)

Von Solms ja Von Solms (2004, 372) ovat koonneet tiivistettynä organisaation tietoturvaohjelman luomiseen ja tietoturvan toteuttamiseen liittyvistä kompastuskivistä 10 niin sanottua kuolemansyntiä, jotka kaikki tulee välttää. Ne esitellään seuraavaksi tutkimuksen tekijän vapaasti suomentamana.

> ”1. Ei ymmärretä, että tietoturva on johdon vastuulla.
> 2. Ei ymmärretä, että tietoturva ei ole tekninen asia.
> 3. Ei ymmärretä, että tietoturvan hallinta on monimutkainen asia, jossa ei ole olemassa niin sanottua hopealuotia tai yksittäistä tehokasta ja suoraviivaista ratkaisua.
> 4. Ei ymmärretä, että tietoturvasuunnitelman on perustuttava tunnistettuihin riskeihin.
> 5. Ei ymmärretä, että kansallisilla ja kansainvälisillä tietoturvan parhailla käytännöillä on tärkeä rooli tietoturvan hallinnassa.
> 6. Ei ymmärretä, että tietoturvapolitiikka on yritykselle ehdoton välttämättömyys tietoturvan toteutumiseksi.
> 7. Ei ymmärretä, että tietoturvan noudattamisen toimeenpano ja valvonta on organisaatiolle ehdoton välttämättömyys tietoturvan toteutumiseksi.
> 8. Ei ymmärretä, että asianmukainen organisaatiotasoinen tietoturvan hallintorakenne on yritykselle ehdoton välttämättömyys tietoturvan toteutumiseksi.
> 9. Ei ymmärretä tietoturvatietoisuuden keskeistä merkitystä käyttäjien keskuudessa.
> 10. Tietoturvapäällikölle/-johtajalle ei anneta riittäviä valtuuksia velvollisuuksien hoitamiseen.” (Von Solms & Von Solms, 2004, 372.)

3.3 Tietoturvakäyttäytyminen

Sanotaan, että ketju on yhtä vahva kuin sen heikoin lenkki. Tietoturvan näkökulmasta työntekijän sanotaan usein olevan tietoturvan heikoin lenkki (Vroom & Von Solms, 2004, 193; Bulgurcu ym., 2010; Peltier, 2006, 14; Vacca, 2014, 17), joten työntekijöiden merkittävää roolia organisaation tietoturvatoiminnan käytännön toteutusprosessissa ei turhaan korosteta (Niemimaa & Niemimaa, 2017, 17). Tyypillisesti ihmisen käyttäytymiseen keskittyvä tieteenala on psykologia, koska käyttäytyminen sisältää lukuisia psyykkisiä toimintoja, kuten tahtominen, havaitseminen, ajatteleminen, päätteleminen, kuvitteleminen, tunteiden kokeminen ja muistaminen (Järvinen, 2018). Myös tietoturvakirjallisuudessa ihmisen käyttäytymiseen liittyvien taustateorioiden kirjo on laaja ja Moody ym., (2018, 288) esittelevätkin kuusi tietoturvan yhteydessä käytettyä psykologian teoriaa. Psykologisten teorioiden tarkoituksena on auttaa tunnistamaan yleiset periaatteet, joilla voidaan ymmärtää paremmin, miksi ihmiset käyttäytyvät kuten käyttäytyvät tai tekevät (selitys) ja ennustaa tai arvioida ennakolta, miten ihmiset käyttäytyvät tietyissä tilanteissa (ennuste) (Gawronski & Bodenhausen, 2015, 3). Mitä sitten tarkoitetaan nimenomaan tietoturvakäyttäytymisellä?

Terminä tietoturvakäyttäytymisellä tarkoitetaan organisaation työntekijöiden käyttäytymistä ja tapoja niissä tilanteissa, jolloin työntekijöiden tulee noudattaa organisaation tietoturvapolitiikkaa, eli kun työntekijät käyttävät organisaation tietojärjestelmiä, ohjelmistoja, laitteita ja verkkojärjestelmiä (Guo, 2013, 243). Tietoturvan kokonaisuus on siis hyvin laaja sisältäen esimerkiksi tavat, miten organisaation työntekijät käsittelevät salasanojaan, miten he käsittelevät organisaatiotietoja tai miten he käyttävät verkon resursseja (Guo, 2013, 243).

Stanton, Stam, Mastrangelo ja Jolton (2005, 126 -127) ovat tutkimuksessaan esittäneet kuusi tietoturvan käyttäytymismallia, joihin liittyy sekä työntekijän tekninen asiantuntijuus (engl. *technical expertise*) että teon tarkoituksellisuus (engl. *intentionality*). Lisäksi Stanton ym., (2005, 127) jakavat mallissaan tietoturvakäyttäytymisen tarkoituksellisesti haitalliseen, neutraaliin ja tarkoituksellisesti hyödylliseen käyttäytymiseen. Neutraalilla tarkoitetaan käyttäytymistä, jossa työntekijällä ei ole erityistä aikomusta edesauttaa, muttei myöskään tahallisesti vahingoittaa tietoturvan toteutumista. Mallin mukaan käyttäytyminen voi olla tahallista tuhoamista (engl. *intentional destruction*), vahingollista väärinkäyttöä (engl. *detrimental misuse*), vaarallista korjailua (puuhastelua) (engl. *dangerous tinkering*), kokemattomuus virheitä (engl. *naïve mistakes*), tietoista varmuutta (engl. *aware assurance*) ja perustaitoja (engl. *basic hygiene*) (Stanton ym., 2005, 127). Tahalliseen tuhoamiseen liittyvä käyttäytyminen edellyttää tekijältään sekä teknistä osaamista että vahvaa tarkoitusta vahingoittaa organisaation resursseja. Vahingollinen väärinkäyttö ei välttämättä vaadi hyvää teknistä asiantuntemusta, vaan siihen riittää teon tarkoituksellisuus, eli tarkoitus aiheuttaa vahinkoa, haittaa tai sääntörikkomuksia. Vaaralliseen korjailuun (puuhasteluun) liittyvä käyttäytyminen vaatii teknistä osaamista, vaikkakaan mitään selkeää tarkoitusta vahingon aiheuttamiseen ei ole. Kokemattomuudesta johtuvat virheet eivät vaadi teknistä osaamista, eikä niihin liity haitan tai vahingon tarkoituksellisuutta samaan tapaan kuin vahingollisessa väärinkäytössä. Tietoinen varmuus liittyy käyttäytymiseen, joka vaatii teknisen osaamisen lisäksi myös vahvan myönteisen asenteen organisaation resurssien suojaamiseen. Myös niin sanottuihin perustaitoihin liittyvä käyttäytyminen osoittaa myönteistä tahtoa organisaation resurssien suojaamiseksi, vaikkei vaadi teknistä osaamista. (Stanton ym., 2005, 126–127.) Stanton ym., (2005) tutkimuksessa esitellyt tietoturvakäyttäytymisen mallit viittaavat työntekijöiden aktiiviseen toimintaan. Kuitenkin myös passiivisuus, eli tekemättömyys voi olla osa tietoturvakäyttäytymistä, joko negatiivisessa tai positiivisessa merkityksessä.

Eri organisaatioiden tietoturvapolitiikoissa sanotaan usein, kuinka tietoturvaohjeet ja -määräykset koskevat jokaista organisaation järjestelmiin ja laitteisiin käyttöoikeuden omaavaa henkilöä. Jotta jokainen osaa huomioida kulloinkin kyseessä olevan organisaation tietoturvapolitiikan mukaisen toiminnan, on tietoturvakäyttäytyminen sidoksissa myös työntekijän tietoturvatietoisuuteen. Eli tietämykseen ja ymmärrykseen organisaation tietoturvan tavoitteista, joihin työntekijä on sitoutunut (Bulgurcu ym., 2010, 532-533). Työntekijän tietoturvatietoisuuteen liittyy myös ymmärrys niistä tietoturvauhkista, jotka kohdistuvat ky-

seessä olevan organisaation arvokkaisiin tietoihin (Vacca, 2014, 19). Tietoturvatietoisuuden voikin sanoa olevan ratkaisevan tärkeää organisaation tietoturvan hallintajärjestelmän (engl. *information security management system, ISMS)* tavoitteiden toteutumiselle.

Tässä tutkimuksessa tietoturvakäyttäytyminen ymmärretään organisaation työntekijöiden käyttäytymisenä ja toimintatapoina, joilla he joko edesauttavat tai murentavat organisaation tietoturvaan liittyvien periaatteiden toteuttamista. Yksilön tietoturvakäyttäytyminen ei ole irrallaan organisaation tietoturvakulttuurista, vaan heijastelee organisaatiokulttuurin sosiaalisia normeja, arvoja ja käyttäytymismalleja. Sosiaalinen normi on eräs tämän tutkimuksen niin sanottuna punaisen lankana toimineen neutralisoimisteorian keskeisistä käsitteistä, joten seuraavaksi tietoturvakäyttäytymistä peilataan sosiaaliseen normiin.

3.4 (Sosiaalinen) normi

Sykes ja Matza käyttävät teoriassaan termejä sosiaalinen normi (engl. *social norms*), sosiaalinen kontrolli (engl. *social control*), vallitseva sosiaalinen järjestys (engl. *dominant social order*) sekä vallitseva normatiivinen järjestelmä (engl. *dominant normative system*). Sykes ja Matza eivät kuitenkaan omassa artikkelissaan suoraan määrittele näitä käsitteitä, vaikkakin viittaavat artikkelissaan oikeudelliseen järjestelmään (engl. *legal system)*, eli lakiin. Sykes ja Matza loivat teoriansa 50-luvulla, ja maailma on muuttunut siitä ajasta hyvinkin paljon. Sanotaan, että eilispäivän normirikkomus voi olla tämän päivän normi, mutta mikä oikeastaan on (sosiaalinen) normi? Eri tutkimuksen tarkoituksesta ja asiayhteydestä riippuen normille ja sosiaaliselle normille löytyy eri tieteenaloilla erilaisia määritelmiä, eikä tietoturvakirjallisuuskaan tee poikkeusta tässä asiassa. Koska sosiaalista normia ja tietoturvapolitiikkaa tullaan tutkimuksessa myöhemmin vertaamaan, esitellään seuraavaksi, miten sosiaalista normia on määritelty.

Parsonsin (1968, 75) mukaan normi on verbaalinen kuvaus konkreettisesta toimintatavasta, jota pidetään toivottavana, ja johon liittyy velvoite (engl. *injunction*) toimia tulevaisuudessakin tämän mukaisesti. Hornen (2001, 4) mukaan todennäköisesti yleisimmin hyväksytty näkemys normista on, että se säätelee käyttäytymistä erilaisten ilmauksien kautta (engl. *statements*). Allardtin ja Littusen (1984, 21) lyhyt määritelmä sosiaalisesta normista kuuluu näin: ”sosiaalinen normi on käyttäytymissääntö, jota tuetaan pakottein”. Edellä esitellyt määritelmät antavat vaikutelman ikään kuin tiukoista säännöistä, joita tulisi ehdottomasti noudattaa. Vaikka Parsons (1968, 75) käyttääkin normia kuvaillessaan esimerkkinä sotilaan kuuliaisuuden välttämättömyyttä, hän viittaa silti ikään kuin siihen, että normin aikaansaamien yhteisten toimintatapojen tavoitteena on lopulta hyödyttää kaikkia ryhmän jäseniä. Yksi näkökulma on siis määritellä normit säännöiksi, joiden rikkomisesta seuraa rangaistus (Fishbein ja Ajzen, 2011, 129). Toisenlainen näkökulma normiin on, etteivät normit ole pelkästään sääntöjä, vaikka normien on katsottu olevan ainakin osittain vastuussa sosiaalisen käyttäytymisen säätelyssä (Opp & Hechter, 2001, xi-xii; Ewald, 2003, 14; Dubois, 2003,

2). Normit eivät ole irrallaan sosiaalisesta käyttäytymisestä (Ewald, 2003, 51), joten ne voivat tarjota yleisiä linjauksia sopivasta tai sopimattomasta käyttäytymisestä, sekä siitä mikä on hyväksyttävää tai sallittua käyttäytymistä ryhmässä tai yhteisössä (engl. *society)* (Fishbein & Ajzen, 2011, 129). Eräs näkökulma normeille on määritellä se toiminnan säännönmukaisuudeksi (Fishbein & Ajzen, 2011, 129).

Sosiaalinen normi voidaan jakaa myös kuvailevaan (deskriptiivinen, engl. *descriptive*) tai velvoittavaan (injuktiivinen, engl. *injunctive*) (tai määräävään/ohjaavaan[16] eli preskriptiivinen, engl. *prescriptive*) (Dubois, 2003, 1; Fishbein & Ajzen, 2011, 131). Kuvailevalla normilla viitataan tietyn ryhmän enemmistön tapaan tehdä tai ajatella (Dubois, 2003, 1). Tällaiset tapahtumat ovat siis tilastollisesti yleisimpiä. Normin tilastollisuudella viitataan myös siihen, kuinka normi palvelee säännön noudattamisen ja siitä poikkeamisen mittana, ja viittaa siten keskiarvoon (Ewald, 2003, 14). Kuvaileva normi vastaa muun muassa kysymyksiin ”mitä useimmat muut ihmiset tekevät” tai ”mitä käytöstapoja yleensä käytetään” (Brauer & Chaurand, 2010, 491). Herath ja Rao (2009b, 158) ovat esittäneet, että tietoturvapolitiikan noudattamisen yhteydessä kuvaileva normi tarkoittaisi tilannetta, jossa työntekijä haluisi noudattaa samanlaista käyttäytymismallia, mikäli näkisi myös muiden työntekijöiden noudattavan rutiininomaisesti organisaation tietoturvakäytänteitä. Velvoittavat (injuktiiviset normit/preskriptiiviset normit) vastaavat puolestaan muun muassa kysymyksiin "mikä on oikein tai väärin" tai "mitä ihmisten pitäisi tehdä" tai "millainen käyttäytyminen on sosiaalisesti hyväksyttävää ja arvokasta" (Brauer & Chaurand, 2010, 491). Käyttäytymisellä haetaan ikään kuin hyväksyntää (Cialdini & Goldstein, 2004, 598). Tietoturvan näkökulmasta työntekijän tietoturvapolitiikan noudattamiseen voisi siten vaikuttaa esimerkiksi moraalisen kehityksen vaiheet (moraaliperiaatteiden tasot), jolloin yksilö ymmärtäisi tietoturvapolitiikan yhteiseksi velvollisuudeksi (Myyry ym., 2009, 128).

Tutkittaessa, kuinka työntekijät voisivat muodostaa käyttäytymismalleja, ja kuinka heitä rohkaistaisiin sekä sitoutumaan että myös noudattamaan organisaation tietoturvapolitiikkaa, sivutaan tietoturvakirjallisuudessa sosiaalista normia muun muassa normatiivisten uskomusten (engl. *normative beliefs)* (Pahnila ym., 2007; Bulgurcu ym., 2010; Siponen ym., 2014), sosiaalisen vaikutuksen (engl. *social influence)* (Johnston & Warkentin, 2010; Ifinedo, 2014), sosiaalisen kontrollin (engl. *social control*) (Cheng ym., 2013), subjektiivisen normin[17] (engl. *subjective norms*) (Herath & Rao, 2009a; Herath & Rao, 2009b; Ifinedo, 2012) ja henkilökohtaisten normien (engl. *personal norms*) (Yazdanmehr & Wang, 2016; Bauer & Bernroider, 2017) kautta. Useimmissa edellä mainituista tutkimuksista sosiaalisen käyttäytymisen selittämisen ja ennustamisen taustateoriana viitataan joko Ajzenen ja Fishbeinin vuonna 1975 julkaistuun perustellun toiminnan teoriaan (engl. *Theory of Reasoned Action, TRA*), tai Ajzen myöhemmin vuonna 1991 laajentamaan suunnitelmallisen käyttäytymisen teoriaan (engl. *Theory of Planned Beha-*

[16] Käytetään myös termin lähikäsitettä normatiivinen, eli sääntöjen ja määräysten mukaista toimintaa tai ajattelua (Tieteen termipankki, 2019)
[17] Käännös voi olla myös ”sosiaalisen ympäristön aiheuttamat paineet” (Kielitohtori, N.d.)

viour, TPB). Koska edellä mainitut teoriat eivät ole suoraan ohjanneet tätä tutkimusta, esitellään teorioiden keskeinen ajatus seuraavaksi lyhyesti ja verrataan myöhemmin Sykesin ja Matzan teorian argumenttiin.

Fishbein ja Ajzen (2011, 130) mukaan normin voi ymmärtää sosiaalisena paineena käyttäytyä (tai olla käyttäytymättä) tietyllä tavalla. Subjektiivinen normi yhdessä asenteen (engl. *attitude toward the behavior*) ja käyttäytymisen hallinnan (engl. *perceived behavioral control)* kanssa muodostaa käyttäytymisen aikomuksen/tarkoituksen (intention[18], engl. *intention*). Subjektiivinen normi viittaa yksilön käsitykseen siitä, miten useimmat hänen kannaltaan tärkeät ihmiset[19] oletettavasti ajattelevat, kuinka hänen pitäisi (tai ei pitäisi) tietyssä tilanteessa toimia tai käyttäytyä (Fishbein & Ajzen, 2011, 131). (Subjektiivinen normi ei siten viittaa siihen, mitä ”tärkeät muut” oikeasti ajattelevat.) Asenteilla tarkoitetaan käyttäytymiseen liittyviä uskomuksia, jotka perustuvat käyttäytymisestä aiheutuvien, joka myönteisten tai kielteisten seurausten arviointiin (Ajzen, 1991, 191). Käyttäytymisen hallinta heijastelee henkilökohtaisista ja ulkoisista tekijöistä muodostuneita uskomuksia, jotka joko helpottavat tai estävät käyttäytymistä tai toimintaa (Fishbein & Ajzen, 2011, 21). Yksilö siis omaksuu asenteita sosiaalisen vuorovaikutuksen kautta ja tarkastelee, ainakin osittain rationaalisesti, käyttäytymistään suhteessa toisiin ihmisiin. Sosiaalisen paineen lähde on yksilön käsitys siitä, miten muut ihmiset käyttäytyvät (deskriptiivinen normi, engl. *descriptive norm)* tai miten hänen itsensä pitäisi (tai ei pitäisi) käyttäytyä (injuktiivinen normi, engl. *injunctive*) (Fishbein & Ajzen, 2011, 131), jotta käyttäytyminen olisi sosiaalisesti hyväksyttävää (Brauer & Chaurand, 2010, 491). Tietoturvan näkökulmasta, työntekijät motivoituvat noudattamaan tietoturvapolitiikkaa, jos he havaitsevat, että esimiehet, alaiset ja vertaiset noudattavat organisaation laatimia suuntaviivoja tietoturvapolitiikan noudattamisessa (Ifinedo, 2012, 85; Siponen ym., 2014, 220) ja työntekijän suhtautuminen tietoturvapolitiikan noudattamiseen yhdistettynä sosiaalisiin normeihin johtaa siihen, että työntekijä aikoo noudattaa tietoturvapolitiikkaa ja aikomus johtaa todelliseen käyttäytymiseen (Siponen ym., 2014, 219, 222).

Vaikuttaisi sille, että tietoturvakirjallisuudessa sosiaalisen normin käsite eroaa hieman Sykes ja Matzan (1957) neutralisoimisteorian käsityksestä. Se, että yksilön muodostama asenne saa vaikutteita esimiesten, alaisten tai vertaisten käyttäytymiseen suhteuttamisesta, ja näiden niin sanottujen tärkeiden muiden sosiaalinen paine aikaansaa normin, joka vaikuttaa yksilön aikomukseen ja käyttäytymiseen on näkökulmana joustava, koska eri organisaatiossa on erilainen tietoturvapolitiikka ja sen mukaiset säännöt, ohjeet ja tavoitteet. Myös Sykes ja Matza (1957, 666) viittaavat joustavuuteen ja siihen, että arvot ja normit näyttäytyvät pikemminkin toimintaa ohjaavana ja rajoittuneena sovellettavaksi tiettyyn

[18]Intentio viittaa suunnitelmalliseen toimintaan suuntautuvaan tahtoon, pyrkimykseen ja motivaatioon osoittaen, kuinka kovasti henkilö tai ryhmä on valmis ponnistelemaan saavuttaakseen intention kohteena olevan tavoitteen (Tieteen termipankki, 2015).

[19] Ajzen ja Fishbein (2011) käyttävät termiä ”important others”, jolloin kyse voi olla myös yksilöistä tai ryhmästä.

aikaan, paikkaan, henkilöön tai sosiaaliseen tilanteeseen. Kuitenkin neutralisoimisteorian keskeinen argumentti on, ettei poikkeavaa toimintaa voida ennustaa poikkeavilla asenteilla[20] tai subjektiivisella normilla, vaan pikemminkin sillä, missä määrin toimija pystyy neutralisoimaan tai käyttämään neutralisoimistekniikoita yksilöllisen ja/tai sosiaalisen näkemyksen mukaisessa (engl. *social perception*) normirikkomuksessa (Fritsche, 2005, 484). Tämän tutkimuksen tulkinnan mukaan Sykes ja Matza siis tarkoittivat, ettei seura välttämättä tee kaltaisekseen, vaan enemmänkin neutralisoimistekniikoiden oppiminen edesauttaisi näkemään toiminnan, jos nyt ei niin oikeana, niin silti kuitenkin hyväksyttävänä. Siinä missä esimerkiksi perustellun toiminnan teoria (*TRA*) keskittyy tiettyä toimintaa/normia kohti suuntaaviin tekijöihin, neutralisoimisteoria keskittyy enemmänkin niistä poistyöntäviin.

Tässä tutkimuksessa (sosiaalinen) normi ymmärretään käyttäytymissääntönä, jolla on kuitenkin niin laaja hyväksyntä, että yksilö ymmärtää normin olemassa olon ja kykenee sisäistämään sen. Kuten Ewald (2003, 59) mainitsee, normi on suhteellinen ja muuttuva, joten yksilön on kyettävä suhteuttamaan käyttäytymisensä normin mukaiseksi. Yksilöllä on myös riittävät tiedot ja taidot normin mukaiseen käyttäytymisen noudattamiseen, ja hän kykenee erottamaan normin vastaisen käyttäytymisen, normista poikkeavuuden, vaikka normin rikkomisesta ei seuraisikaan selkeästi tiedossa olevaa rangaistusta. Sosiaalisen normin käsitteeseen palataan vielä myöhemmin luvuissa kuusi ja seitsemän. Seuraavaksi pyritään lyhyesti kuvailemaan, miten aiemmin mainittua sanaa ”poikkeavuus” voidaan määritellä.

3.5 (Sosiaalisesta) normista poikkeaminen

Sykes ja Matza (1957, 666) esittävät:”*It is our argument that much delinquency is based on what is essentially an unrecognized extension of defenses to crimes, in the form of justifications for deviance that are seen as valid by the delinquent but not by the legal system or society at large.*” Vaikka Sykes ja Matza viittaavat edellä oikeusjärjestelmään (engl. *legal system*) ja laajempaan yhteiskunnalliseen (engl. *society at large*) näkökulmaan, rajaa tämän tutkimuksen tutkimustehtävä poikkeavuuden käsitettä siten, että poikkeavuuden syvällisempi yhteiskunnallinen merkitys tai laajempi vertailu moraalisiin normijärjestelmiin rajautuu tutkimuksen ulkopuolelle.

Huolimatta siitä, että tietoturvakirjallisuudessa sosiaalisen normin käsite eroaa hieman Sykes ja Matzan neutralisoimisteorian mukaisesta sosiaalisen normin käsitteestä, yhteistä lienee kuitenkin Ewaldin (2003, 54) määritelmä siitä, ettei normi synny kenenkään yksittäisen henkilön ilmoituksella, vaan normin määrittelevät yhteiskunnan tai yhteisön jäsenet (Hirch, 1969, 291). Normin syntymiseen tarvitaan siis ryhmä, jolla on ainakin jossain määrin yhteisymmärrystä

[20] “It is by learning these techniques that the juvenile becomes delinquent, rather than by learning moral imperatives, values or attitudes standing in direct contradiction to those of the dominant society” (Sykes ja Matza, 1957, 667).

(konsensusta) sääntöjen pätevyydestä (Opp & Hechter, 2001, 5). Aina normin alkuperää ei ole helppo nimetä, mutta on sanottu, että normin havaitsee helpoiten poikkeamalla siitä. Poikkeavuus (engl. *deviance*) on käsitteenä ikään kuin normin vastakkainen puoli, eli jokin käyttäytyminen poikkeaa normeista. Poikkeavuus voi tarkoittaa, ja usein tarkoittaakin, eri ihmisille eri asioita, eikä ole olemassa yhtä yksittäistä ”poikkeavuusteoriaa” (Franzese, 2015, 29). Siinä missä vielä jokunen vuosikymmen sitten poikkeavan käyttäytymisen tutkimuksissa keskityttiin mielenterveyden häiriöihin, päihteiden väärinkäyttöön ja rikoksiin, voidaan yhtä lailla tietyssä ryhmässä kokea poikkeavuutena yksilön erilaiset arvot, asenteet, elämäntapa tai elämässä tehdyt valinnat (Franzese, 2015, 6, 13, 28–29). Huolimatta määritelmien eroavaisuuksista niistä on löydettävissä myös yhtäläisyyksiä. Franzesen (2015, 9–10) mukaan poikkeavuus liitetään ensinnäkin käyttäytymiseen ja sosiaaliseen normiin tai yhteiskunnallisesti hyväksyttyyn tapaan tehdä asioita. Toiseksi poikkeavuus liittyy sosiaalisiin prosesseihin ja kommunikointiin. Kolmanneksi eri määritelmissä käytetään ilmaisuja leima, kontrolli, sosiaalinen hylkääminen ja rangaistukset. Näillä viitataan siihen, että poikkeavuus edellyttää reaktiota tai käyttäytymisen tunnistamista esimerkiksi ärsyttävänä, häiritsevänä tai jopa uhkaavana. (Franzese, 2015, 9.) Tarvitaan siis ikään kuin yleisö, joka arvio ja tuomitsee yksilön tai ryhmän toiminnan. Tällä perusteella kuka tahansa voidaan siis tulkita normin rikkojaksi ja poikkeavaksi tietyssä yhteisössä tai ympäristössä. Suomen kielessä poikkeavuutta tai poikkeavaa käyttäytymistä ei sanoina käytetä yksinomaan negatiivisessa merkityksessä. Esimerkiksi jotakin suoritusta saatetaan pitää osoituksena henkilön poikkeuksellisesta rohkeudesta, urhollisuudesta tai lahjakkuudesta.

Robinsonin ja Bennettin (1995, 556–557) mukaan työntekijän poikkeavuuden voi määritellä vapaaehtoisena käyttäytymisenä, joka rikkoo merkittäviä organisaatiosääntöjä ja uhkaa siten organisaation tai sen jäsenten, tai molempien, hyvinvointia. Vapaaehtoisuudella viitataan siihen, että työntekijällä ei ole motivaatiota mukautua sosiaalisen kontekstin mukaisiin normatiivisiin odotuksiin tai hän on motivoitunut rikkomaan niitä. Viralliset ja epäviralliset organisatoriset normit määrittelevät säännöt ja menettelytavat. (Robinson & Bennett, 1995, 556–557.) Tietoturvakirjallisuudessa tietoturvarikkomuksen on tulkittu tarkoittavan poikkeavaa käyttäytymistä, koska sillä rikotaan sosiaalista normia (Siponen & Vance, 2010, 490; Kim ym., 2014; Willison ym., 2018, 273). Tämän tutkimuksen tulkinnan mukaan sosiaalisesta normista poikkeaminen tarkoittaa sisäistetyn (sosiaalinen) normin tietoista rikkomista. Tietoturvakontekstissa sosiaalisesta normista poikkeaminen ei välttämättä aiheuta suoranaista sosiaalista hylkäämistä tai niin sanottua leimaa, mutta poikkeavuuden tunnistamiseen tarvitaan silti ikään kuin yleisö, joka arvio ja tuomitsee tai arvostelee tai paheksuu yksilön tai ryhmän toimintaa. Tässä tutkimuksessa myötäillään myös Hirschin (1969, 291) esittämää ajatusta siitä, missä tilanteessa yksilö kokee, etteivät normit sido häntä. Hirsch (1969, 291) esittää, että jos henkilö ei välitä muiden ihmisten toiveista ja odotuksista, eli jos hän ei ole tietoinen toisten mielipiteistä, eivät normit myöskään sido häntä, ja hän saattaa kokea voivansa vapaasti poiketa niistä.

3.6 Sosiaalinen kontrolli ja sosiaalinen järjestys

Sykes ja Matza (1957,667, 665) käyttivät teoriassaan termejä sosiaalinen kontrolli (engl. *social control*) ja vallitseva sosiaalinen järjestys (engl. *dominant social order*), mutta eivät suoraan määrittele näitä käsitteitä. Sykes ja Matza (1957, 666) nostivat esille ristiriidan "*why men violate the laws in which they believe*" eli miksi lakia, johon uskotaan, silti rikotaan. Sosiaalinen kontrolli puolestaan kääntää kysymyksen asettelua hieman toisenlaiseen suuntaan. Se lähtee liikkeelle kysymyksestä "*why don't we all commit crime* " eli miksi kaikki eivät tee rikoksia (Innes, 2003, 22). Vaikka sosiaalisen kontrollin teorioiden juuret ovat kaukana menneisyydessä (Kuhn, 2009, 6–8), pyritään seuraavaksi määrittelemään yleisellä tasolla, miten sosiaalinen kontrolli ja sosiaalinen järjestys ymmärretään tässä tutkimuksessa.

Oikeustieteessä sosiaalinen kontrolli määritellään seuraavasti:

> "Sosiaalisella kontrollilla tarkoitetaan mekanismeja, jotka ohjaavat yhteisön jäsenen toimimaan normien mukaisesti. Sosiaalisen kontrollin avulla pyritään takaamaan jatkuvuuden kannalta riittävän yhdenmukainen toiminta." (Tieteen termipankki, 2019)

Termiä sosiaalinen kontrolli (engl. *social control*) käytetään viittaamaan siihen reaktioon tai prosessiin, jolla määritellään normeista poikkeavaa käyttäytymistä (Innes, 2003, 3; Black, 1984, 34). Eli kun sosiaalinen kontrolli pettää, tai sitä ei ole, tilanne voi mahdollistaa, vaikkei välttämättä suoranaisesti edesauttaisi, sosiaalisista normeista poikkeamista. Blackin (2010, 2, 6) mukaan lait luovat viralisen sosiaalisen kontrollin, mutta sosiaalista kontrollia esiintyy myös muun muassa perheissä, ystävyyssuhteissa, ammateissa ja organisaatioissa, joten sosiaalinen kontrolli jaetaan usein viralliseen ja epäviralliseen kontrolliin (Innes, 2003, 6-7). Blackin (2010, 6) mukaan lain merkitys kasvaa, kun muiden sosiaalisten kontrollien määrä vähenee, ja päin vastoin. Epävirallisella sosiaalisella kontrollilla saattaakin usein olla merkittävämpi vaikutus kuin virallisella sosiaalisella kontrollilla (Black, 2010, 32–36). Eli niin sanotulla lainvoimalla ei yksinomaan ohjata tai rajoiteta käyttäytymistä. Jos kaikki olisivat kaikkina hetkinä yhtä mieltä siitä, miten kulloinkin tulee käyttäytyä, ei käyttäytymistä silloin tarvitsisi edes ohjata lakien ja sääntöjen avulla (Kuhn, 2009, 2–4).

Innesin (2003, 6–7) mukaan sosiaalisella kontrollilla on läheinen yhteys sosiaaliseen järjestykseen (engl. *social order*), koska sosiaalisen kontrollin tarkoituksena on suojata sosiaalista järjestystä, vaikkakaan sosiaalinen järjestys ei ole yksinomaan sosiaalisen kontrollin tulosta. Innes (2003, 6) selittää sosiaalisen järjestyksen viittaavan yhteiskunnan tai yhteisön olemassaolon ehtoihin, koska jokaisella yhteiskunnalla tai yhteisöllä on oma rakenteensa ja siten myös sosiaalinen järjestyksensä. Huolimatta tietynlaisesta rakenteesta, yhteiskunnan tai yhteisön sosiaalinen järjestys ei ole muuttumaton tai pysähtynyt, vaan yhteiskunnan tai yhteisön jäsenten asenteet, arvot, käytännöt ja toimet vaikuttavat tuohon alati muuttuvaan prosessiin. (Innes, 2033, 6–7.) Elimmepä siis missä tahansa yhteiskunnassa tai yhteisössä, yksilöiden sosiaalista elämää ohjataan erilaisilla ohjeilla,

säännöillä, kielloilla ja rangaistuksilla, joilla yhteiskunta tai yhteisö pyrkii asettamaan rajat, millainen käyttäytyminen on hyväksyttävää ja millainen ei.

Vaikka tietoturvakäyttäytymistä onkin tutkittu paljon, silti sosiaaliseen kontrolliin tai sosiaaliseen järjestykseen viittaavia tietoturvatutkimuksia on verrattain vähän. Sekä Ifinedo (2014) että Cheng, Li, Li, Holm ja Zhai (2013) ovat omissa tutkimuksissaan soveltaneet Travis Hirschin sosiaalisen kontrollin teoriaa (engl. *social control theory*). Hirschin (1969) teorian voinee luokitella kriminologian teoriaksi, koska hän pyrki teoriansa avulla kartoittamaan sosiaalisen kontrollin roolia rikoskäyttäytymisessä. Hirschin (1969) teorian mukaan erilaiset sosiaaliset siteet toimivat ikään kuin sosiaalisena kontrollina ja vaikuttavat siten yksilön käyttäytymiseen. Hirsch (1969, 293–298) esittelee teoriassaan neljä sosiaalisen siteen (engl. *elements of the bond*) elementtiä, jotka ovat teorian mukaan sidoksissa yksilön rikoskäyttäytymiseen. Ensimmäinen näitä Hirschin esittämistä sosiaalisista siteistä on tunnepohjainen side (engl. *attachment*), toinen on sitoutuminen yhteiskunnan/yhteisön rakenteisiin (engl. *commitment*), kolmas tavanomaiseen (lailliseen) toimintaan osallistuminen tai syventyminen (engl. *involvement*) ja neljäs yhteiskunnan/yhteisön sääntöihin (lakiin) uskominen (engl. *belief*). Mikäli yksilö ei koe sidettä tärkeänä tai merkittävänä, yksilön on helpompi poiketa normin mukaisesta käyttäytymisestä. Cheng ym., (2013, 455) tutkimuksessa esitettiin, että työntekijän organisaatioon ja työhön sitoutuminen vaikuttaa merkittävästi työntekijä aikomukseen joko rikkoa tietoturvapolitiikkaa tai noudattaa sitä. Ifinedo (2014, 76) puolestaan esittää, kuinka tietoturvapolitiikan noudattaminen pitäisi niin sanotusti myydä sosiaalisena siten, että tietoturvapolitiikan noudattaminen hyödyttää organisaation jäseniä.

Tämän tutkimuksen tulkinnan mukaan sosiaalinen kontrolli tarkoittaa yhteiskunnan, kulttuurin tai yhteisön luomia, osin sanattomiakin, käyttäytymiseen liittyviä sääntöjä, kuinka yksilön tulisi toimia hyväksyttävällä tavalla kulloinkin kyseessä olevassa yhteiskunnassa, kulttuurissa tai yhteisössä. Kuten aiemmin mainittiin, sosiaalista kontrollia ei välttämättä ilmaista sanallisesti tai kirjallisesti, vaan sosiaalista järjestystä ylläpidetään muun muassa paheksumalla niitä, jotka eivät noudata hyväksyttäviä tapoja, vaan poikkeavat niistä. Tämän tutkimuksen tulkinnan mukaan, huolimatta siitä, ettei sosiaalinen järjestys olisikaan yksinomaan sosiaalisen kontrollin tulosta, yksilö ei silti voi olla havaitsematta omaa poikkeavuuttaan tai olla tiedostamatta sitä, että rikkoo sosiaalista normia.

3.7 Tietoturvarikkomus

Nykysuomen sanakirjan mukaan sana ”rikkomus” tarkoittaa käskyjen, sääntöjen tai tapojen vastaista tekoa (Kielitoimiston sanakirja, 2018). Tietoturvakirjallisuudessa tietoturvarikkomus (engl. *information security violation*) jaetaan suoraan ja epäsuoraan toimintaan (Crossler ym., 2013, 91–92), tahalliseen tai tarkoituksettomaan toimintaan (Stanton ym., 2005, 126–127). Suoralla toiminnalla tarkoitetaan esimerkiksi sabotaasia, varkautta, teollista tai poliittista vakoilua tai muuta mer-

kittävää väärinkäytöstä. Epäsuoriksi luokitellaan esimerkiksi liian yksinkertaisen salasanan valitseminen, työhön liittymättömillä internet-sivustoilla vierailu ja luottamuksellisen tiedon salaamattomana lähettäminen. (Crossler ym., 2013, 91–92.) Tahattomilla rikkomuksilla voidaan tarkoittaa esimerkiksi inhimillistä virhettä, kuten virheellisten tietojen syöttämistä tai vahingossa tapahtuvaa tietojen tuhoamista (Im & Baskerville, 2005, 75). Yleisimpiä tarkoituksellisia tietoturvarikkomuksia ovat esimerkiksi työaseman lukitsemattomuus poistuttaessa työpisteeltä, henkilökohtaisten salasanojen kirjoittaminen näkyviin paikkoihin, salasanojen jakaminen työkavereiden tai ystävien kanssa, arkaluoteisten tietojen kopioiminen suojaamattomalle USB-laitteelle, luottamuksellisten tietojen paljastaminen ulkopuolisille, suojauskonfiguraatioiden käytöstä poistaminen, kannettavien tietokoneiden huolimaton käyttö organisaation ulkopuolelle ja helposti arvattavien salasanojen luominen (Siponen & Vance, 2010, A5).

Huolimatta määritelmien eroavaisuudesta ja tahallisuus- ja vakavuusasteen vaihtelevuudesta, tietoturvarikkomuksella tarkoitetaan mitä tahansa toimintaa, joka aiheuttaa tietoturvan vaarantumisen (Calder & Watkins, 2010). Tässä tutkimuksessa myötäillään edellä mainittua määritelmää.

Kuten edellä mainitaan, tietoturvarikkomuksiin liittyy sekä tarkoituksellisuutta että tahattomuutta, joten onkin täysin oletettavaa, ettei edellä mainittuja tutkimustuloksia olisi saatu ilman jonkinlaisia selityksiä, perusteluita tai arvauksia, miksi jokin rikkomus on tapahtunut. Seuraavaksi tarkastellaan, miten erilaisten tarkoituksellisten tekojen selontekojen ja oikeuttamisten on tulkittu eroavan toistaan.

3.8 Selonteot: pahoitteleva ja oikeuttava

Weinerin (1985) mukaan ihminen rakentaa negatiivisista tapahtumista erilaisia selityksiä hyvinkin spontaanisti, mutta myönteisistä tapahtumista harvemmin. Kuten Sykes ja Matza (1957, 664) toteavat: "*…the social scientist has long since ceased to search for devils in the mind or stigma of the body*", eli mitään toimintaa enää harvemmin selitetään vaikkapa paholaisen riivauksella. Scott ja Lyman (1968, 46) arvioivat, että selonteot ja selitykset ovat ratkaiseva tekijä sosiaalisessa järjestyksessä. Näitä sosiaalisen järjestyksen ylläpitoon liittyviä käsitteitä tarkastellaan seuraavaksi.

Scott ja Lyman (1968) saivat vaikutteita Sykes ja Matzan neutralisoimisteoriasta kirjoittaessaan Accounts- nimisen artikkelinsa (Maruna ja Copes, 2005, 238). Suoninen (1997) on suomentanut Accounts -artikkelissa mainitun "account"-termin viittaavan selontekoon tai selitettävissä olevaan, vaikka selonteko itsessään ei tarkoittaisikaan, jonkin asian olevan selvä. Suoninen (1997) määrittelee selonteoilla tarkoitettavan:"tehdä kielellisesti ymmärrettäväksi tai kulttuurisessa mielessä järjelliseksi omaan toimintaansa tai toisten toimintaa". Kuten Suoninen (1997) määritelmässään mainitsee, selonteot ja selitykset saavat vaikutteensa ympäröivästä kulttuurista, eli ne on oltava perusteltavissa kulttuurisesti hyväksytyllä tavalla.

Scott ja Lyman (1968, 46) esittävät selonteon tarkoittavan selitystä, jolla selitetään ennakoimattoman tai yllättävän käyttäytymisen syitä. Scott ja Lyman (1968, 46) arvion mukaan nämä toimintaa ja käyttäytymistä selittävät selonteot ovat keskeinen osa sosiaalista järjestystä. Selonteot voivat ehkäistä konfliktien tai ristiriitatilanteiden syntymistä, koska ne voivat toimia ikään kuin siltana odotusten (engl. *expectation)* ja toiminnan (engl. *action*) välisessä kuilussa. Tiettyyn kulttuurin syvään juurtuneet tavat voivat olla kulttuurissa elävälle niin itsestäänselviä, ettei selityksille tai selonteoille ole edes tarvetta, vaan enemmänkin niitä ihmettelevää saatetaan kummeksua. (Scott & Lyman, 1968, 47.) Suonisen (1997) tulkinnan mukaan:

> ”Scottille & Lymanille erikoistilanteissa annetut selonteot kertovat normaaleina pidetyistä tavoista ja siitä, millaisia toimintaa ymmärrettäväksi tekeviä syitä pidetään järjellisinä.” (Suoninen, 1997)

Scott ja Lyman (1968, 47) jakavat selonteot kahdenlaisiin: pahoitteleviin (engl. *excuses*) ja oikeuttaviin (engl. *justifications*). Henkilö voi pyrkiä vetoamaan molempiin selontekoihin tai vain jompaan kumpaan toimiessaan väärin, sopimattomasti tai muuten kielteisellä tavalla yllättävästi. Vaikka molemmissa selonteoissa käytetään niin sanotusti kielellisiä, sosiaalisesti hyväksyttyjä keinoja selittää tai perustella tekoa ja sen seurauksia, on selonteoissa silti Scottin ja Lymanin (1968, 47) mukaan ratkaiseva ero. Scottin ja Lymanin (1968, 47) mukaan oikeuttavat selonteot ovat selityksiä, joissa henkilö on vastuussa teostaan, mutta kiistää siihen liittyvän pejoratiivisen laadun, eli teon halveksuttavuuden. Pahoittelevat selonteot puolestaan viittaavat tilanteisiin, joissa yksilö myöntää teon olleen väärä, paha tai epäasianmukainen, mutta kiistää täyden vastuun (Scott & Lyman, 1968, 47).

Tässä tutkimuksessa myötäillään Suonisen (1997) tulkintaa selontekojen eroavaisuuksista. Suonisen (1997) mukaan pahoittelevat selonteot viittaavat tilanteisiin, jotka pyrkivät tekemään rikkomuksia tai poikkeavuutta ymmärrettäväksi kiistämättä rikotuksi tulleen normin mielekkyyttä. Oikeuttavat selonteot puolestaan viittaavat suoraan normin kanssa kilpailevaan normiin, tai sitä suhteellistavaan näkökulmaan. (Suoninen, 1997.) Yhteistä näille erilaisille tavoille selittää sopimatonta tai väärää käytöstä on se, että molemmat tavat linkittyvät osaksi kulttuuria ja sisältävät käsityksiä, kirjoittamattomia sääntöjä ja teorioita siitä, milloin toimija on vastuussa teostaan ja milloin vastuu lievenee tai katoaa, eli millaiset asiat ovat tahdon alaisia tai tahdon ulkopuolella (Suoninen, 1997).

Scott ja Lyman (1968, 48) mainitsevat pahoittelevan selonteon esimerkkinä selityksen onnettomuudesta, koska on tilastollisestikin epätodennäköistä, että sama onnettomuus tapahtuisi samalle henkilölle useasti. Selitys, vaikka se olisikin vain niin sanottu tekoselitys, viittaa kuitenkin sosiaalisesti hyväksyttyyn selitykseen ja lieventää vastuuta teosta. Scottin ja Lymanin (1968, 48) mukaan pahoitteleva selonteko tai puolustus syytöksiä vastaan voi liittyvä myös niin sanottuihin mentaalisiin elementteihin, eli muun muassa tietoon ja tahtoon. Henkilö pyrkii ikään kuin vapautumaan vastuustaan vedoten riittämättömiin, virheelli-

siin tai vääristeltyihin tietoihin. Myös toisten syyllistäminen on eräs pahoittelevista selonteoista, jolloin tekijä vierittää tekonsa syyt jollekin toiselle (Scott & Lyman, 1968, 50). Vaikka Scott ja Lyman (1968, 48–49) viittaavat yksilön käyttävän pahoittelevina selontekoina myös vetoamista vapaan tahdon menetykseen ja biologisiin vietteihin, ei näiden selontekojen käsittely tämän tutkimuksen kontekstissa olisi relevanttia, joten niitä ei käsitellä mainintaa enempää.

Oikeuttamisen selontekojen yhteydessä Scott ja Lyman (1968, 51) viittaavat Sykes ja Matzan (1957) teoriassa esiteltyihin neutralisoimistekniikoihin, eli vahingon kieltämiseen, uhrin kieltämiseen, tuomitsijoiden tuomitsemiseen ja korkeampiin lojaliteetteihin vetoamiseen. Nämä eri tekniikat on esitelty luvussa kaksi. Scott ja Lyman (1968, 52) esittelevät vielä kaksi oikeuttavaa selontekoa: surullisia tarinoita (engl. *sad tales*) ja itsensä toteuttaminen (engl. *self-fulfillment*). Surullinen tarina ankeasta ja kurjasta menneisyydestä halutaan toimivan selityksenä nykyhetkeen johtaneista syistä. Itsensä toteuttaminen viittaa tekoihin, jotka voivat olla lainvastaisia, mutta joita henkilö selittää elämäntapaansa kuuluvina (Scott & Lyman, 1968, 52–53.)

Kuten jo aiemmin mainittiin, sekä Suonisen (1997) että Scott ja Lymanin (1968) esittävät selontekoihin liittyvän kulttuurisidonnaisuuden. Seuraavaksi tarkastellaan lyhyesti, miten organisaation tietoturvakulttuurin on eri tutkimuksissa todettu vaikuttavan tietoturvakäyttäytymiseen.

3.9 Tietoturvakulttuuri

Jokaisella organisaatiolla on oma kulttuurinsa, joka edustaa muun muassa organisaation sosiaalisia normeja, uskomuksia ja käyttäytymismalleja. Jokaisella organisaatiolla on myös omat tietoturvakäytäntönsä, ja tietoturvakulttuuri heijasteleekin organisaatiokulttuuria ja sitä tapaa, miten asioita tehdään tai hoidetaan. Tietoturvakulttuuriin sisältyy siten oletukset siitä, mikä on tai mikä ei ole hyväksyttävää päivittäistä toimintaa tietoturvan näkökulmasta (Martins & Elofe, 2002, 205).

Van Niekerk ja Von Solms (2010) ovat omassa tutkimuksessaan viitanneet Scheinin (1991) organisaatiokulttuurin teoriaan ja muokanneet sen pohjalta neliosaisen tietoturvakulttuurin mallin. Schein (1991, 33–37) jakaa teoriassaan organisaatiokulttuurin rakenteen kolmeen tasoon. Ensimmäisellä tasolla ovat artefaktit ja luomukset. Ensimmäinen taso on siis organisaatiokulttuurin näkyvin taso, joka sisältää fyysisen ja sosiaalisen ympäristön, kuten fyysiset tilat, puhutun ja kirjoitetun kielen sekä havaittavissa olevan käyttäytymisen (Schein, 1991, 32–33). Scheinin (1991) mallissa organisaatiokulttuurin toisella tasolla ovat organisaation viralliset arvot ja normit. Eli ne periaatteet, jotka ovat organisaatiossa tärkeitä ja joita arvostetaan. Koska nuo organisaation toiminnan viralliset periaatteet ovat tietoisesti valittuja, on täysin mahdollista, ettei todellinen toiminta vastaakaan virallisten arvojen mukaista toimintaa, mikäli arvot eivät perustu kulttuurissa tapahtuneeseen oppimiseen. Eli sanotaan yhtä, mutta toimitaan toisin. (Schein,

1991, 33–35.) Organisaatiokulttuurin pohjimmaisella tasolla sijaitsevat organisaation perusoletukset, eli ne pitkän ajan kuluessa muodostuneet käsitykset, uskomukset ja toiminnan periaatteet, jotka ovat muodostuneet niin itsestäänselvyyksiksi, että niiden vastaista käyttäytymistä saatetaan pitää käsittämättömänä (Schein, 1991, 33–35).

Van Niekerkin ja Von Solmsin (2010, 479) tietoturvakulttuurin mallissa on kaikki samat rakenteet kuin Scheinin mallissa, mutta he ovat lisänneet neljänteen tasoon tietämyksen. Se, miten työntekijät käyttäytyvät tietoturvan suhteen muodostuu virallisten periaatteiden, arvojen, niin sanotun hiljaisen tiedon ja tietämyksen yhteisvaikutuksesta (Van Niekerk & Von Solms, 2010, 481). Siten organisaatiokulttuurin jokainen taso voi vaikuttaa tietoturvakulttuuriin joko myönteisesti tai kielteisesti, koska eri tasot ovat vuorovaikutuksessa keskenään. Ilman riittävää tietämystä ja ymmärrystä tietoturvan merkityksestä, ei tietoturvakulttuuri pysty täyttämään sille asetettuja tavoitteita (Van Niekerk & Von Solms, 2010, 481).

Yksilön omat käsitykset, uskomukset ja ennakkoluulot vaikuttavat hänen tietoturvakäyttäytymiseensä (Tsohou, Karyda & Kokolakis, 2015, 128), eikä tietoturvakulttuuri synny itsestään eikä sitä myöskään ylläpidetä itsestään.

4 AIEMMAT TUTKIMUKSET

Tässä luvussa esitellään, kuinka neutralisoimisteoriaa on aiemmissa tutkimuksissa sovellettu selittämään työntekijöiden tietoturvakäyttäytymistä ja tietoturvapolitiikan ja –ohjeiden noudattamattomuutta. Tarkastelussa on mukailtu sekä Websterin ja Watsonin (2002) että Levyn ja Ellisin (2006) ohjeita ja suosituksia, joita kirjallisuuden tarkastelussa tulisi ottaa huomioon. Samalla tarkastellaan, miten aiemmat tutkimukset ovat tulkinneet neutralisoimisteoriaa ja huomioineet tutkimuksissaan alkuperäisen neutralisoimisteorian keskeisiä väittämiä.

4.1 Aihepiirin aiemmat tutkimukset

Aiemman aihepiiriin kuuluvan kirjallisuuden tarkastelu on niin sanottu perusehto mille tahansa tutkimukselle. Sen kautta voidaan tarkastella alan kehitystä ja alueita, joista löytyy jo runsaasti tietämystä, mutta samalla tarkastelu voi paljastaa myös kehityksen esteitä tai alueita, joilla tutkimusta tarvitaan. (Webster & Watson, 2002, xiii.) Levyn ja Elliksen (2006, 183) mukaan kirjallisuuden tarkastelu auttaa hahmottamaan ja tunnistamaan, mitä tutkimusaiheesta jo tiedetään, millaisilla menetelmillä ja lähestymistavoilla aihetta on tutkittu, mitä vielä tulisi tutkia sekä sen, mitä uutta tietoa tekeillä oleva tutkimus voi tuoda olemassa olevaan tietopohjaan.

Tutkimuksen kirjallisuuskatsaus on kerätty tieteellisistä tutkimuksista, artikkeleista ja konferenssijulkaisuista hyödyntäen sekä lehtiä että tietokantoja. Julkaisujen valinnan perusteena käytettiin Ranked MIS Journals –listausta, jolloin julkaisuiksi valikoitui mm. *MIS Quarterly, Communications of the ACM, Decision Support Systems, European Journal of Information Systems, Information & Management, Information Systems Journal, Information Systems Research, Journal of Information Technology, Journal of Management Information Systems ja Computers & security*. Aiempien julkaisujen löytämisessä hyödynnettiin avainsanahakuja kuten muun muassa *"Techniques of Neutralization"*, *"Neutralization Theory"*, *"Neutralization Theory AND information security"*. Lisäksi tarkasteltiin aiempiin tutkimuksiin

viitanneita tutkimuksia, eli ns. eteenpäin ja taaksepäin suuntautuvan kirjallisuuden hakuja. Tietokantahakuja suoritettiin mm. seuraavista: *ABI/INFORM Complete (ProQuest), Elsevier (ScienceDirect), EBSCOhost* ja *Association for Information Systems Electronic Library*.

Artikkeleista etsittiin yhtäläisyyksiä artikkelissa mainittuihin avainsanoihin ja artikkelin abstrakti luettiin. Artikkeleiden valinta perustui siihen, oliko artikkelissa sovellettu Sykes ja Matzan alkuperäistä teoriaa tietoturvan yhteydessä. Julkaisun ajankohdalle ei asetettu aikarajaa. Tarkasteluun sisällytettiin sekä suomenkieliset että englanninkieliset maksuttomat ja vertaisarvioidut julkaisut. Valintakriteerinä pidettiin myös sitä, oliko tutkimus perustunut empiirisiin todisteisiin tai aineistoon, sekä siihen oliko aineisto ja sen koko esitelty riittävän selkeästi. Vaikka jokin artikkeli olisi sisältänyt suosituksia tai ohjeita siitä, miten aihealueen tutkimusta tulisi tehdä, mutta artikkeli ei sisältänyt empiiristä osuutta, niitä artikkeleita ei tarkasteluun otettu mukaan.

Seuraavaksi tarkastellaan, millaisiin näkökulmiin aiemmat, suoraan Sykes ja Matzan (1957) alkuperäisteoriaa ja/tai sen osia tietoturvan yhteydessä soveltaneet, tutkimukset ovat keskittyneet. Taulukossa 1 esitellään kooste aiemmissa tutkimuksissa käytetystä menetelmästä, otanta sekä tutkimusten keskeisimmät löydökset.

TAULUKKO 1 Aiempien tutkimusten kooste

Tekijä/tekijät	Menetelmä	Näyte/otanta	Keskeisimmät löydökset
Barlow ym., (2013) Computers & security, 39, 145-159.	Kyselytutkimus, 36:lla skenaariolla ja seitsemällä hypoteesilla	90 työntekijää, jotka vastasivat neljään satunnaiseen skenaarioon, jolloin näyte oli yhteensä 360 vastausta	Viestinnällisin keinoin voidaan vähentää tietoturvarikkomus aikomuksia. Eri neutralisoimistekniikoilla on erilainen merkitys.
Barlow ym., (2018) Journal of the Association for Information Systems, 19(8).	Kyselytutkimus 24:llä skenaariolla	200 kokoaikaista työntekijää, jotka vastasivat kahteen satunnaiseen skenaarioon, jolloin näyte oli yhteensä 400 vastausta	Viestinnälliset keinot, joilla torjutaan neutralisoimistekniikoita, vähentävät merkittävästi aikomusta rikkoa tietoturvapolitiikkaa.
Bauer & Bernroider (2017) Data Base for Advances in Information Systems (2017), forthcoming.	Kolmivaiheinen tapaustutkimus, joka sisälsi 4 puolistrukturoitua haastattelua, kyselytutkimus ja interaktiivisen esittelyn	2 tietoturvajohtajaa, 1 PR johtaja, 1 turvallisuusjohtaja ja 97 työntekijää	Suhtautuminen tietoturvapolitiikan noudattamiseen on tärkein muuttuja sosiaalisissa ja henkilökohtaisissa normeissa, jotka vaikuttavat tietoturvakäyttäytymiseen.

Tekijä/tekijät	Menetelmä	Näyte/otanta	Keskeisimmät löydökset
Bauer ym., (2017) Computers & security, 68, 145-159.	Kolmivaiheinen tapaustutkimus, joka sisälsi 33 puolistrukturoitua haastattelua	10 tietoturvapäällikköä, 23 työntekijää	Tietoturvatietoisuusohjelmat tulisi mukauttaa käyttäjäryhmittäin. Tällä vähennettäisiin neutralisointia.
Cheng ym., (2014) Computers in Human Behavior, 38, 220-228.	Kyselytutkimus neljällä hypoteesilla	230 työntekijää	Neutralisointi on vahvin ennustaja aikomuksessa rikkoa tietoturvapolitiikkaa. Myös henkilökohtainen hyöty lisää rikkomuksen todennäköisyyttä.
Haag ym., (2015) AIS Electronic Library (AISel) ICIS2015 ja **Haag ym., (2015)** PACIS	Laboratorio koe	148 yliopisto-opiskelijaa	Niin kutsutun varjo-it:n käyttäjät hyödyntävät neutralisoimistekniikoita.
Khansa ym., (2017) Journal of Management Information Systems, 34(1), 141-176.	Kyselytutkimus yhdeksällä hypoteesilla, joista 1 oli alkuperäisen neutralisoimisteorian hypoteesi	Kaksivaiheisen tutkimuksen ensimmäiseen osaan vastasi 451 henkilöä ja toiseen osaan 360	Virallisesta valvonnasta ilmoitus on merkittävästi sidoksissa työhönliittymättömän internet-käyttäytymisen neutralisointiin.
Kim ym., (2014) The Scientific World Journal, 2014	Kyselytutkimus kolmella skenaariolla ja kahdeksalla hypoteesilla (1 neutralisoimisteorian hypoteesi)	194 työntekijää eri aloilta ja eri työtehtävistä	Tietoturvarikkomuksia perustellaan eri neutralisoimistekniikoilla. Minäpystyvyyden tunne ei vaikuta tietoturvapolitiikan noudattamiseen niin vahvasti kuin mm. myönteinen asenne.
Li ym., (2013) In PACIS (p. 169)	Kyselytutkimus kymmenellä hypoteesilla	428 eri ikäistä ja eri koulutustaustan omaavaa työntekijää	Työntekijät hyödyntävät neutralisoimistekniikoita internet väärinkäytön aikomuksissaan lukuun ottamatta vastuun kieltämisen -tekniikkaa.
Nicho & Kamoun (2014) Association for Information Systems.	Monivaiheinen laadullinen tutkimus	Kolme tapausta	Niin sanotut sisäpiiriläiset oikeuttavat toimintansa neutralisoimistekniikoilla.
Nykänen (2011) Väitöskirja. Tampere: Oulun Yliopisto,	Kaksivaiheinen toimintatutkimus	15 työntekijää	Tietoturvakoulutus vaikutti vahingon kieltämisen –tekniikkaan neutralointia hei-

Tekijä/tekijät	Menetelmä	Näyte/otanta	Keskeisimmät löydökset
			kentävästi, muut neutralisoimistekniikat eivät olleet merkittäviä.
Silic ym., (2017) Information & management	Kyselytutkimus 13 hypoteesilla	Neljä organisaatiota, yhteensä 1445 työntekijää eri ammattiryhmistä	Vain ” metaphor of the ledger” neutralisoimis-tekniikalla oli vaikutus varjo-it:n käyttäjien tietoturvapolitiikan rikkomiseen. Häpeä, viralliset tai epäviralliset seuraukset eivät vaikuta rikkomus aikeisiin. Häpeä vaikuttaa epävirallisiin seurauksiin ja joihinkin neutralisoimistekniikoihin. Aikomuksen ja todellisen käyttäytymisen välillä ei ole juurikaan eroa varjo-it:n käyttäjillä.
Siponen & Vance (2010) MIS Quarterly, 34(3), 487-A12.	Kyselytutkimus kolmella skenaariolla ja neljällä hypoteesilla	Kolme organisaatiota, yhteensä 1449 työntekijää eri ammattiryhmistä	Neutralisointi vaikuttaa merkittävästi työntekijöiden aikomukseen rikkoa tietoturvapolitiikkaa
Siponen ym., (2020) Computers & Security, 88, 101617.	Kvasikokeellinen tutkimus, jossa kontrolli- ja koeryhmä (21/66 hlö)	Monikansallisen yhtiön 87 työntekijää	Neutralisoimista on mahdollista vähentää tietoturvakoulutuksen avulla.
Willison ym., (2018) Information Systems Journal.	Kyselytutkimus neljällä skenaariolla ja 12 hypoteesilla	968 työntekijää eri ammattiryhmistä (näyte kaikkiaan 3872, koska jokainen kävi läpi neljä skenaariota)	Prosessuaalinen epäoikeudenmukaisuus on yhteydessä väärinkäytöksiin sekä neutralisoimistekniikoiden hyödyntämisen aikomuksiin.

Barlow, Warkentin, Ormond ja Dennis (2013) tutkimuksessa keskitytään tarkastelemaan viestinnällisten keinojen tehokkuutta tietoturvapolitiikan noudattamattomuuden aikomuksissa. Barlow ym., (2013, 147, 149) esittävät, kuinka organisaatioiden tietoturvaa käsittelevä viestintä, kuten esimerkiksi tietoturvakoulutus, saattaa usein painottua vain varoittamaan tietoturvarikkomusten seurauksista. Tutkijoiden mukaan tällainen kielteisiin seurauksiin keskittyvä koulutus vaikuttaa siihen, kuinka yksilö käsittelee asian ja saattaa siten vaikuttaa siihen, että työntekijät neutralisoivat negatiivisen kehyksen mielestään. Barlow ym., (2013) tutkimuksessa sovellettiin yhtä alkuperäisen neutralisoimisteorian neutralisoimistekniikka yhdessä kehysteorian (engl. *framing theory*) kanssa. Kehysteorian mukaan tapa, jolla asia esitellään, vaikuttaa siihen, kuinka ihminen asian käsittelee. Tutkijoiden mukaan: ”*Our results suggest that security communication*

and training that focuses on neutralization techniques is just as effective as communication that focuses on deterrent sanctions in persuading employees not to violate policies, and that both types of framing are equally effective." (Barlow ym., 2013, 145). Eli neutralisoimistekniikoihin keskittyvä koulutus ja viestintä ovat yhtä tehokkaita kuin viestintä, joka keskittyy seurauksilla pelotteluun, jolloin molemmat tavat ovat yhtä tehokkaita. Tutkimuksen mukaan, tietoturvaan liittyvän viestinnän, sekä virallisen että epävirallisen, tulisi keskittyä torjumaan neutralisoimistekniikoiden käyttämistä, jolloin viestinnän keinot voivat myös vähentää voimakkaasti aikomusta tietoturvarikkomuksiin. Vaikka tutkijoiden mukaan heidän tutkimuksensa antaa lisätodisteita siitä, että neutralisointi on tärkeä ennustaja aikomuksille rikkoa tietoturvapolitiikkaan, heidän mukaansa neutralisoimistekniikoiden merkitys vaihtelee riippuen siitä, millainen tietoturvarikkomus on kyseessä. (Barlow ym., 2013.)

Barlow, Warkentin, Ormond ja Dennis (2018) tutkimus keskittyy kolmen viestintäkeinon vertailuun, joiden avulla voitaisiin vähentää työntekijöiden aikomusta rikkoa tietoturvapolitiikkaa. Näitä ovat informatiivinen viestintä (engl. *informational communication*), normatiivinen viestintä (engl. *normative communication*) ja antineutralisaatio viestintä (engl. *antineutralization communication*). Informatiivisen viestinnän tarkoituksena on selittää, miksi tietoturvapolitiikat ovat tärkeitä. Normatiivisen viestinnän tarkoituksena on selittää, etteivät muut työntekijät riko tietoturvapolitiikkoja. Antineutralisaation viestinnän tarkoituksena on estää rationalisointi (järkeistämisen). Tutkimuksessa sovelletaan kahta neutralisoimistekniikkaa, joista toinen on alkuperäisestä neutralisoimisteoriasta. Tutkimuksen tarkoituksena on näiden tekniikoiden kautta ymmärtää, minkä tyyppinen viestintä saa aikaan hyvää tietoturvakäyttäytymistä vähentäen samalla neutralisoinnin vaikutuksia. Tutkijoiden mukaan viestinnälliset keinot, jotka on erityisesti suunniteltu torjumaan neutralisoimistekniikoita, vähentävät merkittävästi aikomusta rikkoa tietoturvapolitiikkaa. (Barlow ym., 2018.)

Bauer ja Bernroider (2017) tutkimuksessa neutralisoimisteoriaa sovellettiin yhdessä perustellun toiminnan teorian (engl. *theory of reasoned action*) kanssa. Tutkimuksessa tarkasteltiin työntekijöiden henkilökohtaisten normien ja arvojen merkitystä tietoturvakäyttäytymisessä. Tutkijoiden mukaan asenteet ja neutralisoimistekniikoiden käyttö heijastelevat yksilön henkilökohtaisia moraalisia normeja, ja henkilökohtaiset moraalinormit ovat merkittävän tärkeitä tietoturvakäyttäytymisessä. Tutkijat korostivatkin, kuinka tietoturvapolitiikan noudattamisessa tärkein tekijä on asenne. (Bauer & Bernroider, 2017.)

Bauer, Bernroider ja Chudzikowski (2017) tutkimuksessa neutralisoimisteoriaa sovellettiin erilaisten käyttäjäryhmien tietoturvakäyttäytymisen vertailuun. Tutkijat päättelivät, että työntekijät asettivat päivittäisten työtehtävien hoitamisen sekä asiakastyytyväisyyden etusijalle, jolloin kyse olisi tutkijoiden mukaan ”vetoaminen korkeampiin lojaliteetteihin” –neutralisoimistekniikan hyödyntämisestä. Toinen tutkimuksessa päätelty työntekijöiden käyttämä neutralisoimistekniikka oli ”defense of necessity”, jolloin työntekijä kokee, ettei hänellä ole muuta keinoa tai vaihtoehtoa. (Bauer ym., 2017.)

Cheng, Li, Zhai ja Smyth (2014) tutkimuksessa neutralisoimisteoriaa on sovellettu yhdessä peloteteorian (engl. *deterrence theory*) kanssa. Tutkimus keskittyy työntekijöiden työssä tai työaikana tapahtuvaan työhön liittymättömään internetin käyttöön. Tutkimuksessa neutralisointia tutkittiin yhdessä työntekijän arvioiman tietoturvarikkomukseen liittyvän rangaistuksen vakavuuden, rikkomuksen havaitsemisen varmuuteen sekä rikkomuksesta arvioitujen etujen näkökulmasta. Tutkimusasetelman taustaksi oli valittu henkilökohtaisen internetin käytön aiheuttamat tietoturvauhkat, kuten internet-selailun kautta tehtyjen erilaisten haitta- ja vakoiluohjelmien, virusten ja selainkaappausohjelmien lataukset. Tutkijoiden mukaan neutralisoiminen on vahvin ennustaja työntekijöiden aikomuksessa käyttää internetiä henkilökohtaisiin tarkoituksiin. Tutkijoiden mukaan henkilöt, jotka kokevat hyötyvänsä henkilökohtaisiin tarkoituksiin liittyvästä internetin käytöstä, valitsevat todennäköisimmin riskin, vaikka tietävät olemassa olevan kiinnijäämisen riskin ja sen seuraukset. (Cheng ym., 2014.)

Haag, Eckhardt ja Bozoyan (2015) sekä Haag ja Eckhardt (2015) tutkimukset perustuvat yhteen ja samaan tutkimukseen, joten ne käsitellään tässä kohdassa yhdessä. Tutkimuksessa tarkasteltiin neutralisoimistekniikoiden vaikutusta niin sanotun varjo-it:n hyödyntämiseen. Varjo-it (engl. *shadow IT*) termillä tarkoitetaan erilaisia tietotekniikkaresursseja, joita työntekijät ottavat työpaikalla käyttöönsä ilman organisaation it-osaston suostumusta. Nuo resurssit voivat olla esimerkiksi mobiililaitteita, pilvipalveluita tai muutoin helposti käytettäviä ratkaisuja, joihin on pääsy ilman erityisiä it-taitoja. (Haag ym., 2015, 3.) Tutkimuksen mukaan niin sanottujen varjojärjestelmien käyttäjät hyödyntävät neutralisointia, jolloin poikkeamaa (engl. *deviation*) vähätellään sillä, että organisaation käytänteet ovat perusteettomia, tai varjojärjestelmän käyttö on välttämätöntä eikä aiheuta vahinkoa. (Haag ym., 2015; Haag & Eckhardt, 2015.)

Khansa, Kuem, Siponen ja Kim (2017) tutkimuksessa neutralisoimisteoriaa sovellettiin yhdessä Akersin sosiaalisen oppimisteorian (engl. *social learning theory*) kanssa. Tutkimuksessa tarkasteltiin kahta neutralisoimistekniikkaa, joista toinen oli Sykes ja Matzan alkuperäisen neutralisoimisteorian mukainen, eli ”vastuun kieltäminen” (engl. *denial of injury*). Tutkimuksessa tutkittiin, miten virallisesta valvonnasta ilmoittaminen vaikuttaa työhön liittymättömään internet-käyttäytymiseen. Tutkimuksen tarkoituksena oli sekä kehittää että testata teoreettista mallia, joka olisi sovellettavissa myös muihin käyttytymiseen liittyviin tutkimuksiin, joissa tutkitaan ihmisten poikkeavaa käyttäytymistä sekä organisatoristen kontrollisen tehokkuutta erilaisissa organisatorissa ja yhteiskunnallisissa yhteyksissä. Tutkijoiden mukaan erityisesti neutralisointi liittyy merkittävästi työhön liittyvämättömän intenet-käyttäytymisen aikomukseen vasta kun valvonnasta on virallisesti ilmoitettu. Tutkijoiden mukaan neutralisoiminen yhdessä havaittujen riskien, henkilön oman aiemman työhön liittymättömään internet-käyttäytymiseen (engl. *cyperloafing*) ja vertaisten työhön liittymättömän internetin käytön pystyy ennustamaan työntekijöiden työhön liittymättömän internetin käytön aikomukset. (Khansa ym., 2017.)

Kim, Yang ja Park (2014) tutkimuksen teoreettisen perustan malli oli muodostettu neutralisoimisteorian, perustellun toiminnan teorian (engl. *theory of*

reasoned action, TRA), suunnitelmallisen käyttäytymisen teorian (engl. *theory of planned behaviour, TPB),* rationaalisen valinnan teorian (engl. *rational choice theory*) sekä suojelumotivaatioteorian (engl. *protection motivation theory*) yhdistelmästä. Tutkimukselle asetetun oletuksen mukaan asenteet, normit sekä minäpystyvyys, eli yksilön luottamus omiin kykyihinsä vaikuttavat aikomuksiin noudattaa tietoturvapolitiikkaa. Tutkimuksessa neutralisointia mitattiin hypoteesillä: mitä korkeampi neutralisoinnin taso organisaation jäsenillä on, sitä alhaisempi tietoturvapolitiikan noudattamisen taso organisaation jäsenillä. Tutkijoiden mukaan tutkimuksen tulos tuki edellä mainittua hypoteesia. Tutkijoiden mukaan tulos tuki kaikkia tutkimuksen tarkastelussa sovellettuja neutralisoimistekniikoita. (Kim ym., 2014.)

Li ja Cheng (2013) tutkimus keskittyy työhön liittymättömään internetin käyttöön, ja pyrkii tunnistamaan taustalla vaikuttavia vaiheita, jotka ohjaavat työntekijöitä työpaikalla tapahtuvaan työhön liittymättömään internetin käyttöön. Li ja Cheng (2013) tutkimuksessa niin sanottu internet-väärinkäyttö (engl. i*nternet abuses*) kattaa verkkosivujen selailun lisäksi myös verkko-ostosten tekemisen, erilaisilla keskustelukanavilla tapahtuvan viestinnän sekä äärimmäisenä esimerkkinä verkkorikollisuuteen osallistumisen. Tutkimuksessa neutralisoimisteoriaa sovelletaan yhdessä rationaalisen valinnan teorian (engl. *rational choice theory*) kanssa. Tutkijoiden mukaan tutkimustuloksen perusteella on mahdollista havaita, että neutralisoimistekniikat edeltävät työntekijöiden työhön liittymättömän internetin käyttöä lukuun ottamatta vastuun kieltämisen –neutralisoimistekniikkaa. (Li & Cheng, 2013.)

Nicho ja Kamoun (2014) tutkimuksessa neutralisoinnin roolia tarkastellaan niin sanottujen sisäpiiriläisten muodostaman tietoturvauhkan näkökulmasta. Nicho ja Kamoun (2014, 335) määrittelevät sisäpiiriläisen tarkoittavan muun muassa nykyisiä tai entisiä työntekijöitä, liikekumppaneita, konsultteja tai muita sidosryhmiä ja järjestelmiä, joilla on joko hetkellinen tai pysyvämpi pääsy organisaation järjestelmiin. Tutkimuksen mukaan sisäpiiriläisten muodostama tietoturvauhka on yhtä aikaa sekä vaikea että vakava ongelma, koska sisäpiiriläisillä on usein pääsy organisaation tietoihin, joista ulkopuolisilla ei edes ole tietoa. Tutkimuksessa analysoidaan kolmea erilaista sisäpiiriläisen aiheuttamaan tietoturvauhkaa, joiden kautta pyritään selvittämään, mitkä muuttujat vaikuttavat sisäpiiriläisten väärinkäytöksiin. Ensimmäinen tapaus käsitteli viestinnän puutteellisuutta, toinen tyytymättömän, irtisanotun työntekijän luottamuksellisten tietojen luovuttamista ja kolmannessa tapauksessa luotettavana pidetty henkilö asensi haittaohjelman organisaation järjestelmään. Tutkimuksen mukaan sisäpiiriläiset hyödyntävät neutralisointia oikeuttaessaan rikollisen toimintansa. (Nicho & Kamoun, 2014.)

Nykäsen (2011) tutkimuksessa neutralisoimisteoria toimii tutkimuksen tukena pyrittäessä selvittämään, miten työntekijät neutralisoivat työhön liittymätöntä internetin käyttöään. Tutkimus keskittyy tietoturvakoulutuksen vaikuttavuuteen yksilön ja organisaation tietoturvakäyttäytymisessä. Tutkimuksen mukaan huolellisesti suunnitellulla tietoturvakoulutuksella voidaan vaikuttaa työhön liittymättömän internetin käytön hyväksyttävyyteen siten, että koulutuksen

jälkeen työhön liittymätöntä internetin käyttöä ei pidetty enää niin hyväksyttävänä kuin ennen koulutusta. Koulutuksen jälkeen vahingon kieltäminen (engl. *denial of injury*) –neutralisoimistekniikan osuus oli muuttunut. Tutkimuksen mukaan muut neutralisoimistekniikat eivät tilastollisesti selittäneet merkittävästi yksilön työhön liittymättömän internetin käyttöä. (Nykänen, 2011.)

Silic, Barlow ja Back (2017) tutkimus keskittyy organisaation sisäpiiriläisiin, jotka muodostavat tietoturvauhkan käyttämällä erilaisia niin kutsuttuja varjo-it:n (engl. *shadow it*) ratkaisuja. Silic ym., (2017, 1023) määrittelevät niin laitteet, ohjelmistot kuin mitkä tahansa tekniset ratkaisut, joilla ei ole organisaation it-osaston hyväksyntää varjo-it:n käytöksi. Tutkimuksessa neutralisoimisteoriaa sovelletaan yhdessä peloteteorian (engl. *deterrence theory*) kanssa. Tutkimuksessa tarkastellaan aiotun ja todellisen käyttäytymisen välistä eroa, sekä häpeä merkitystä neutralisoimistekniikoiden ja organisaation tietoturvarikkomusten välillä. Tutkimuksen mukaan kaikilla neutralisoimistekniikoilla ei näyttäisi olevan suoraa vaikutusta organisaation varjo-it käytäntöjen rikkomiseen. Lisäksi tutkimus mainitsee, ettei häpeällä, virallisilla tai epävirallisilla seuraamuksilla näyttäisi olevan mitään varoittavaa vaikutusta niin sanottujen varjojärjestelmien käyttämisen aikomukseen. Tutkimus päätyy oletukseen, ettei kaikilla työntekijöiden käyttämillä neutralisoimistekniikoilla ole tavoitteena lieventää häpeää eikä häpeä siten olisi suhteessa kaikkiin neutralisoimistekniikoihin. Myöskään aikomuksen ja todellisen käyttäytymisen välillä ei tutkimuksen mukaan näyttäisi olevan juurikaan eroa. (Silic ym., 2017.)

Siponen ja Vance (2010) soveltavat tutkimuksessaan neutralisoimisteoriaa yhdessä peloteteorian (engl. *deterrence theory*) kanssa. Tutkimus keskittyy siihen, kuinka työntekijät rationalisoivat aikomuksiaan rikkoa organisaation tietoturvapolitiikkaa. Tutkimuksen keskeisenä näkökulmana on se, ettei rangaistusten tai muiden sanktioiden pelko välttämättä toimi tietoturvakontekstissa, koska työntekijät hyödyntävät erilaisia neutralisoimistekniikoiden ja järkeilevät niiden avulla rikkomuksensa, jolloin seurauksilla pelottelu menettää tehonsa. Tutkimuksen mukaan neutralisointi vaikuttaa merkittävästi alttiuteen rikkoa tietoturvapolitiikkaa. (Siponen & Vance, 2010.)

Siposen, Puhakaisen ja Vancen (2020) tutkimuksessa neutralisoimisteoriaa sovelletaan yhdessä kognitiivisen dissonassin teorian (engl. *cognitive dissonance theory*) kanssa. Tutkimuksessa sovelletaan kognitiivisen dissonanssin teorian periaatteisiin perustuvaa tietoturvakoulutusta ja tutkitaan, vähentääkö koulutus yksilön neutralisoimistekniikoiden hyödyntämistä. Tutkimus keskittyy salasanakäytäntöihin. Tutkimuksen mukaan huolellisesti suunnitellulla tietoturvakoulutuksella, jonka tarkoituksena on perustella ja selittää, miksi yksilön tulisi noudattaa organisaation tietoturvakäytäntöjä, voidaan vähentää salasanakäytäntöihin liittyvää neutralisointia. (Siponen ym., 2020.)

Willison, Warkentin, ja Johnston (2018) tutkimuksessa neutralisoimisteoriaa sovelletaan yhdessä oikeudenmukaisuusteorian (engl. *organizational justice – distributive and procedural*) ja peloteteorian (engl. *deterrence theory)* kanssa. Tutkimus keskittyy tarkastelemaan työntekijän kokeman epäoikeudenmukaisuuden

ja tietoturvarikkomuksen aikomuksen välistä yhteyttä. Tutkimus pyrkii ymmärtämään, kuinka työntekijöiden käsitykset epäoikeudenmukaisuudesta motivoivat tietoisiin tietoturvarikkomuksiin, ja kuinka työnantajan langettamat seuraamukset vaikuttavat näiden aikomusten muodostumiseen ja työntekijän neutralisoimistekniikoiden käyttämiseen. Tutkimuksessa epäoikeudenmukaisuuden kokemukseen sovellettiin sekä distributiivista, eli organisaation palkkoihin ja muihin resurssien jakoon liittyvää epäoikeudenmukaisuutta, että prosessuaalista näkökulmaa, joka liittyy resurssien jakamisessa noudatettaviin menettely- ja toimintatapoihin. Tutkimuksen mukaan vain prosessuaalinen epäoikeudenmukaisuus oli yhteydessä väärinkäytös aikomuksiin ja lisäsi neutralisoimistekniikoiden todennäköisyyttä työntekijän väärinkäytös aikomuksiin. Tutkimuksen mukaan tämä löydös viittaisi siihen, että työntekijöiden väärinkäytös aikomuksiin vaikuttaa enemmän epäoikeudenmukaiset menettely- ja toimintatavat kuin siitä, ettei heille makseta oikeudenmukaista korvausta. Lisäksi tutkimus esittää, että väärinkäytöksestä saatavan rangaistuksen varmuus on tehokkaampi pelote kuin rangaistuksen vakavuus. (Willison ym., 2018.)

Taulukoihin 2 ja 3 on koottuna havainnot siitä, kuinka edellä mainituissa, aiemmissa tutkimuksissa on huomioitu alkuperäisen neutralisoimisteorian neutralisoimistekniikoita (taulukko 2) ja keskeisiä olettamuksia (taulukko 3).

TAULUKKO 2 Tutkimuksissa huomioidut alkuperäisen teorian neutralisoimistekniikat

Alkuperäisen teorian neutralisoimistekniikat					
	denial of responsibility (vastuun kieltäminen)	denial of injury (vahingon kieltäminen)	denial of victim (uhrin kieltäminen)	condemnation of the condemners (tuomitsijoiden tuomitseminen)	appeal to higher loyalties (vetoaminen korkeampiin lojaliteetteihin)
Barlow ym., (2013)		X			
Barlow ym., (2018)		X			
Bauer & Bernroider (2017)	X	X		X	
Bauer ym., (2017)					X
Cheng ym., (2014)	X	X	X	X	X
Haag ym., (2015)		X			
Khansa ym., (2017)		X			
Kim ym., (2014)	X	X		X	X

Li & Cheng (2013)	X	X	X	X	X
Nicho & Kamoun (2014)		X		X	
Nykänen (2010)	X	X		X	X
Silic ym., (2017)	X	X		X	X
Siponen & Vance (2010)	X	X		X	X
Siponen ym., (2020)	X	X		X	X
Willison ym., (2018)		X	X		

TAULUKKO 3 Tutkimuksissa huomioidut muut neutralisoimistekniikat

	Muut neutralisoimistekniikat			
	"defense of necessity"(välttämättömyyden puolustaminen)	"metaphor of the ledger"(tekojen punnitseminen)	"defense of ubiquity" (kaikkialla läsnäolon puolustus)	"claim of relative acceptability" (väite suhteellisesta hyväksytävyydestä)
Barlow ym., (2013)	X	X		
Barlow ym., (2018)	X			
Bauer & Bernroider (2017)	X			
Bauer ym., (2017)				
Cheng ym., (2014)				
Haag ym., (2015)	X			
Khansa ym., (2017)		X		
Kim ym., (2014)	X	X	X	
Li & Cheng (2013)				X
Nicho & Kamoun (2014)	X			

Nykänen (2010)	X	X		
Silic ym., (2017)	X	X		
Siponen & Vance (2010)	X	X		
Siponen ym., (2020)	X			X
Willison ym., (2018)		X		

Taulukossa 3 mainitut neutralisoimistekniikat eivät ole Sykesin ja Matzan alkuperäisestä teoriasta, vaan aiemmat tutkimukset ovat viitanneet muun muassa Minorin (1981), Klockarsin (1974) ja Harrisin ja Dumasin (2009) julkaisemiin neutralisoimistekniikoihin. Taulukkoon 4 on koottuna havainnot siitä, kuinka aiemmissa tutkimuksissa on huomioitu alkuperäisen neutralisoimisteorian keskeisiä väittämiä.

TAULUKKO 4 Sykes ja Matzan alkuperäisen teorian keskeiset väittämät

Alkuperäisen teorian keskeiset väittämät				
	shame (häpeä)	guilt and guilt avoidance (syyllisyys ja syyllisyyden välttäminen)	social control & social order (sosiaalinen kontrolli ja sosiaalinen järjestys)	make deviant behavior possible (neutralisointi mahdollistaa poikkeavan toiminnan)
Barlow ym., (2013)				X
Barlow ym., (2018)				
Bauer & Bernroider (2017)			X	
Bauer ym., (2017)				
Cheng ym., (2014)				
Haag ym., (2015)				
Khansa ym., (2017)				
Kim ym., (2014)				
Li ym., (2013)				

Nicho & Kamoun (2014)				
Nykänen (2010)				
Silic ym., (2017)	X			
Siponen & Vance (2010)			X	X
Siponen ym., (2020)				
Willison ym., (2018)			X	

4.2 Aiempien tutkimusten tulkinnat

Kuten taulukoista 2 ja 3 käy ilmi, aiemmat neutralisoimisteoriaa tietoturvan yhteydessä soveltaneet tutkimukset ovat keskittyneet kattavasti selvittämään, millaiset yksittäiset neutralisoimistekniikat joko ennustavat tai mahdollisesti ennustavat yksilön aikomuksia selitellä, puolustella tai oikeuttaa tietoturvapolitiikan vastaisia toimintatapoja. Tutkimukset ovatkin antaneet arvokasta tietoa neutralisoinnin ja neutralisoimistekniikoiden roolista eri yhteyksissä tapahtuvien tietoturvarikkomusten tai -rikkomusten aikomuksen tutkimisessa.

Aiemmat tutkimukset ovat esittäneet, kuinka sekä neutralisointi (engl. *neutralization*) (kts. esim. Barlow ym., 2013, 153; Bauer ja Bernroider, 2017, 59; Cheng ym., 2014, 223–224; Siponen & Vance, 2010, 496) että neutralisoimistekniikat (engl. *neutralization techniques*) (Li & Cheng, 2013, 8) ennustavat (engl. *predicts*) tietoturvarikkomus aikomuksia (engl. *intention to violate IS security policy*) ja ovat siten tärkeä tietoturvarikkomusten ennustaja (engl. *predictor*). Lisäksi tutkijat ovat esittäneet, että virallisilla tai epävirallisilla sanktioilla on vain vähäinen vaikutus tietoturvarikkomuksen aikomukseen tai todelliseen käyttäytymiseen suhteessa neutralisointiin. (Li & Cheng, 2013, 9; Siponen & Vance, 2010, 495–496; Silic ym., 2017, 1031–1032). Aiempien tutkimusten mukaan yksilön todellista tai aiottua käyttäytymistä on siis mahdollista selittää tai ennustaa paremmin neutralisoimisteorian avulla kuin rangaistuksiin (sanktioihin) perustuvilla teorioilla.

4.2.1 Neutralisointi

Taulukoissa 2, 3 ja 4 mainitut aiemmat tutkimukset ovat monipuolisesti tuoneet erilaisia näkökulmia ja tulkintoja Sykesin ja Matzan alkuperäisestä neutralisoimisteoriasta tietoturvakontekstissa. Tutkimukset eivät ole, yhtä poikkeusta lukuun ottamatta, lähdeluetteloissaan viitanneet Matzan tai Sykesin ja Matzan

myöhempiin julkaisuihin, joten on oletettavaa, ettei aiemmissa neutralisoimisteoriaa tietoturvan yhteydessä soveltaneissa tutkimuksissa ole sovellettu mahdollista jatkokehitettyä tai joiltain osin täydennettyä Sykesin ja Matzan neutralisoimisteoriaa muussa kuin Nykäsen (2011) tutkimuksessa. Seuraavaksi tarkastellaan, mitä yksilö haluaa aiempien tutkimusten tulkinnan mukaan neutralisoinnilla tehdä.

Sanana neutralisointia (taulukko 5) on aiemmissa tutkimuksissa tulkittu moraalittoman tai laittoman teon oikeuttamiseksi (Silic ym., 2017, 1025), moraalisista tietoturvapolitiikan rajoitteista vapautumiseksi (Bauer & Bernroider, 2017, 45) sekä tavanomaisista rajoituksista vapautumiseksi (Siponen ja Vance, 2010, 488). Siponen ja Vance (2010, 497) ovat vielä täydentäneet termiä Marunan ja Copesin (2005, 231) tulkinnalla, joka viittaa tilapäiseen tai väliaikaiseen vapautumiseen moraalisista rajoitteista. Marunan ja Copesin tulkinta on Matzan vuonna 1964 esittelemästä termistä ”drift”, ja sitä ei vielä esiintynyt alkuperäisessä teoriassa.

TAULUKKO 5 Suorat lainaukset aiemmista tutkimuksista sanalle “neutralisointi”

Tulkinnat sanalle neutralisointi	
Barlow ym., (2013)	*“...employees attempt to reduce their guilt or shame for intending to violate IT policies. In their minds, these rationalizations make their actions seem more normal or more necessary than is actually the case”* Barlow ym., (2013, 146)
Barlow ym., (2018)	*“Neutralization is defined as the use of rationalizations when violating a policy.”* Barlow ym., (2018, 692)
Bauer & Bernroider (2017)	*“The basic idea is that people personally free themselves from the moral constraints of ISP requirements so that they may then choose to act in non-compliant ways. In finding excuses, employees may temporarily neutralize certain values before violating ISPs, by, for example, denying any responsibility for the situation*.” Bauer ja Bernroider (2017, 45)
Bauer ym., (2017)	-
Cheng ym., (2014)	*“Neutralization theory postulates that individuals try to convince themselves, and others, that their deviant behavior is justifiable. It represents a priori rationalization that individuals employ in order to convince themselves that deviant behavior is excusable”* Cheng ym., (2014, 220).
Haag ym., (2015)	*”…enables individuals’ likewise to engage in and rationalize deviant activities without suffering from feelings of self-blame or shame*” Haag ym., (2015, 8).
Khansa ym., (2017)	*“Neutralization refers to an employee’s attempt to rationalize, excuse, or justify his or her cyberloafing behavior”* Khansa ym., (2017, 145)
Kim ym., (2014)	*“… that explains how people nullify the existing norms of society by justifying the violation of the norm.”* Kim ym., (2014, 2)
Li ym., (2013)	-
Nicho & Kamoun (2014)	-
Nykänen (2010)	*”...yksilön lainvastaisen käyttäytymisen taustalla vaikuttaa jokin neutralisoiva tekijä, jolla pyritään selittämään toimintaan ryhtymisen syitä. Lähtökohtana*

	on pyrkiä ymmärtämään ja löytämään selitys, mitkä tekijät vaikuttavat normeista poikkeavan käyttäytymisen taustalla ja mitkä ovat ne keskeiset tekijät, jotka vähentävät yksilön syyllisyydentunnetta normien rikkomisesta." Nykänen (2011, 45-46)
Silic ym., (2017)	"*Neutralization is the act of rationalizing or justifying an immoral or illegal act. Neutralization theory suggests that those who commit illegal or illegitimate actions may 'neutralize' certain values which, in other situations, would prohibit them from committing these same actions*" (Silic ym., 2017, 1025).
Siponen & Vance (2010)	*"These techniques provide employees a temporary release from their conventional restraints, including formal and informal sanctions*" Siponen ja Vance (2010, 488) "*..temporary period of irresponsibility or an episodic relief from moral constraint*". Siponen ja Vance (2010, 497)
Siponen ym., (2020)	-
Willison ym., (2018)	"*… offenders who might otherwise feel guilt and shame were able to neutralize these feelings by justifying their behaviours before committing the deviant act.*" Willison ym., (2018, 273)

Neutralisointi on lisäksi aiempien tutkimusten mukaan järkeilyä, jolla vähennetään rikkomukseen liittyvää syyllisyyttä ja häpeää (Barlow ym., 2013, 146). Barlow ym., (2013, 146) tulkinnan mukaan syyllisyyden ja häpeän tunteiden vähentäminen liittyy teon aikomukseen. Barlow ym., (2018, 693) tulkitsivat neutralisointitekniikoiden vähentävän kognitiivista dissonanssia ja muuttavan siten yksilön käsityksiä sääntöjen rikkomisen kielteisistä seurauksista. Tämä tulkinta viittaisi yksilön ennen tekoa tapahtuviin perusteluihin. Myös Willison ym., (2018, 273) sekä Bauer ja Bernroider (2017, 45) viittaavat ennen poikkeavan teon tekemistä tapahtuvaan oikeuttamiseen, jolloin syyllisyyden ja häpeän tunteet neutralisoidaan jo ennen tekoa. Lisäksi Willison ym., (2018, 274–275) täydentävät tulkintaansa Agnew (1994, 561) huomiolla siitä, että neutralisointi on tilannesidonnaista siten, että yksilön on uskottava olevansa tilanteessa, jossa neutralisointia on mahdollista soveltaa. Myös Bauer ja Bernroider (2017, 45) tuovat esille tilannesidonnaisuuden, ja heidän mukaansa työntekijän on ikään kuin löydettävä tekosyitä, jotta he voivat tilapäisesti neutralisoida tiettyjä arvoja. Myös Silic ym., (2017, 1025) viittaavat tilannesidonnaisuuteen tulkitessaan, että ne, jotka tekevät lainvastaisia tai laittomia toimia, voivat neutralisoida tiettyjä arvoja, jotka muissa tilanteissa estäisivät toimimasta samoin. Nykäsen (2011, 45–46) tulkinta "*käyttäytymisen taustalla vaikuttaa jokin neutralisoiva tekijä, jolla pyritään selittämään toimintaan ryhtymisen syitä*" viittaisi myös vielä tekemättömään tekoon.

Cheng ym. (2014) ja Kim ym., (2014) eivät tulkinnassaan esittele tapahtuuko oikeutus etu- vai jälkikäteen. Cheng ym. (2014, 220) mukaan yksilöt yrittävät vakuuttaa sekä itselleen että muille poikkeavan käyttäytymisen olevan perusteltua, ja yksilöt käyttävät näitä perusteluita vakuuttaakseen itselleen, että teko on anteeksiannettavaa (engl. *excusable*). Kim ym., (2014, 2) tulkinnan mukaan neutralisointi on sitä, miten ihmiset perustelevat yhteisön tai yhteiskunnan vallitsevia normeja vastaan tekemänsä rikkomukset. Haag ym., (2015, 8) tulkinnan mukaan

oikeutus voi tapahtua sekä etu- että jälkikäteen, koska neutralisointi mahdollistaa yksilölle sekä harjoittaa poikkeavia tekoja että järkeistää niitä kärsimättä itsesyytöksistä tai häpeästä.

Siponen ja Vance (2010, 488) puolestaan viittaavat teon jälkeen tehtyyn oikeutukseen mainitessaan: "*…rationalizations which allow them to minimize the perceived harm of their policy violations. This rationalizing behavior in turn reduces the deterring effect of sanctions*." Eli rationalisoinnin avulla vähennetään rikkomuksen haittoja.

Vaikka edellä esitellyt tutkimukset ovat lähdeviittausten perusteella soveltaneet tutkimuksissaan Sykesin ja Matzan alkuperäistä neutralisoimisteoriaa, kaikki tulkinnat eivät välttämättä ole suoraan Sykesin ja Matzan alkuperäisestä neutralisoimisteoriasta. Koska Sykes ja Matza (1957, 667) viittaavat teoriassaan oppimiseen ja käyttävät muun muassa termiä "syvällinen vieraantuminen itsestään" (engl. *a profound alienation from self*), voidaan olettaa, ettei silloin viitata mihinkään tilapäiseen, hetkelliseen tai vain kerran tapahtuvaan oikeutukseen jonkin tekniikan avulla. Sykesin ja Matzan teoria tai mikään viidestä neutralisoimistekniikoista ei myöskään viittaa tilannesidonnaisuudella siihen, että yksilö pyrkisi löytämään tietystä tilanteesta jotain neutralisoitavaa. Mikäli neutralisointi johtaisi rikokseen siksi, että rikollinen uskoisi olevansa tilanteessa, jossa neutralisointia voidaan soveltaa, jää aiemmista tutkimuksista kuitenkin puuttumaan muun muassa vallitsevan kulttuurin tai yhteisön vaikutus teon neutralisointiin.

Sykes ja Matza (1957, 667) mainitsevat tekniikoiden oppimisesta:"*It is by learning these techniques that the juvenile becomes delinquent, rather than by learning moral imperatives, values or attitudes standing in direct contradiction to those of the dominant society.*" Vaikka tekniikoiden oppiminen on eräs kriminologian keskeinen olettamus, aiemmat tutkimukset eivät juurikaan käsittele sitä.

Tämän tutkimuksen tulkinta Sykesin ja Matzan teoriasta on se, että Sykes ja Matza halusivat ikään kuin koota hajanaisista ja irrallisista puolutusmekanismeista viisi eri tekniikkaa, joita ei kuitenkaan voi irrottaa erilleen Sykesin ja Matzan keskeisistä väitteistä ilman, että yksittäisen neutralisoimistekniikan selitysvoima heikkenee tai katoaa.

Sykes ja Matza (1957, 666) eivät teoriassaan ota suoraan kantaa moraaliin tai moraalittomuuteen, vaikka mainitsevatkin "*The moral injunction against killing, for example, does not apply to the enemy during combat in time of war, although a captured enemy comes once again under the prohibition*." Edellä mainitut tutkimukset (Siponen ja Vance, 2010, sekä Bauer & Bernroider, 2017 ja Silic ym., 2017) viittaavat neutralisoinnin tarkoittavan moraalittoman teon oikeuttamista tai oikeutuksen avulla moraalisista rajoitteista vapautumista. Tutkimuksista ei käy ilmi, millaisista moraalisista rajoitteista ihminen vapautuu oikeuttaessaan tietoturvarikkomuksen, ja kokeeko työntekijä tietoturvarikkomuksen tai tietoturvarikkomuksen aikomuksen moraalittomana tekona tai millainen tietoturvarikkomus olisi työntekijän näkökulmasta moraaliton. Vaikka Sykes ja Matza viittaavat edellä niin sanottuun moraalisääntöön, aiemmat tutkimukset eivät käsittele, millaisia moraalisääntöjä tietoturvarikkomusten aikomukseen liittyy. Kuitenkin Siponen ja Vance (2010, 498) viittaavat Kohlbergin (1969) moraalikehitystä kuvaavaan teoriaan ja siihen, kuinka tietyssä moraalikehityksen vaiheessa vain rangaistuksen

pelko estää yksilöä toimimasta sääntöjen vastaisesti. Siponen ja Vance (2010, 498) esittävät:

> "In addition, according to the theory of cognitive moral development (Kohlberg 1969), individuals at the "obedience" stage of moral development are only deterred by threat of sanctions. This suggests that formal sanctions should be used because of their effectiveness in deterring these individuals."

Siponen ja Vance (2010) jättävät tutkimuksessaan avoimeksi, tarkoittavatko he, että tietoturvan yhteydessä ei vielä ole saavutettu sellaista moraalikehityksen tasoa, jossa tietoturvapolitiikkaan liittyvät lait ja säännöt ymmärrettäisiin yhteisiksi velvollisuuksiksi, joita kaikkien olisi noudatettava.

4.2.2 Neutralisoimisteoria

Aiemmat neutralisoimisteoriaa tietoturvan yhteydessä soveltaneet tutkimukset eroavat hieman tulkinnoissaan siinä, mitä Sykes ja Matza halusivat tuoda tutkimuksellaan esiin. Silic ym., (2017, 1024) tulkinnan mukaan "*Neutralization theory suggests that citizens that abide by rules and those who do not both believe in the norms and values of the community in general*." Silic ym., (2017, 1024) viittaavat siis siihen, että olisi sääntöjä noudattavat kansalaiset ja sitten ne, jotka eivät usko yhteiskunnan normeihin ja arvoihin. Siponen ja Vance (2010, 489) ovat puolestaan tulkinneet "*Neutralization theory claims that both law-abiding citizens and those who commit crimes or rule-breaking actions believe in the norms and values of the community in general."* Eli sekä lainkuuliaiset kansalaiset että rikoksentekijät tai säännönvastaisesti toimivat uskovat yleisesti yhteisön normeihin ja arvoihin.

Sykes ja Matza (1957, 665) ovat esittäneet:

> "In other words, if the delinquent does hold to a set of values and norms that stand in complete opposition to those of respectable society, his norm-holding is of a peculiar sort. While supposedly thoroughly committed to the deviant system of the delinquent sub-culture, he would appear to recognize the moral validity of the dominant normative system in many instances." (Sykes & Matza, 1957, 665).

Koko Sykesin ja Matzan teorian ajatuksena oli todistaa, ettei ole erillistä rikollisten alakulttuuria, jonka arvot olisivat vallitsevan yhteiskunnan arvoihin nähden käänteisiä. Sykes ja Matza esittivät:

> "In short, the theoretical viewpoint that sees juvenile delinquency as a form of behavior based on the values and norms of a deviant sub-culture in precisely the same way as law-abiding behavior is based on the values and norms of the larger society is open to serious doubt" (Sykes ja Matza, 1957, 666).

Eli (nuoriso)rikollisen käyttäytyminen perustuu samalla tavalla arvoihin ja normeihin kuin lainkuuliainen käyttäytyminen.

Verrattaessa Silic ym., (2017, 1031–1032) ja Siposen ja Vancen (2010, 496) tutkimustuloksia on kuitenkin mielenkiintoista havaita, että teorian päinvastaisesta tulkinnasta huolimatta, tutkimustulokset myötäilevät toisiaan. Kummassa-

kin tutkimuksessa todetaan muun muassa virallisten ja epävirallisten seuraamusten vähäinen merkitys tietoturvarikkomuksiin. Tuloksen voi tulkita siten, että se vahvistaa virallisten ja epävirallisten seuraamusten merkityksettömyyttä, koska riippumatta siitä uskooko yksilö yhteisön normeihin ja arvoihin vai ei, organisaation asettamat viralliset ja epäviralliset seuraamukset menettävät tietoturvarikkomuksissa joka tapauksessa merkityksensä. Toki voidaan kysyä, miksi työntekijä sitten kokisi rikkomuksistaan syyllisyyttä ja häpeää, jota neutraloisi jonkin neutralisoimistekniikan avulla, jos hän ei edes usko (tässä tapauksessa) tietoturvapolitiikkaan ja sen sääntöihin, kun seuraamuksellakaan ole mitään merkitystä. Toisaalta tulkintaerot voivat viitata myös siihen, ettei Sykesin ja Matzan teorian keskeisiä olettamuksia ole huomioitu riittävän laajasti.

Sykesin ja Matzan (1957) teoriaa on lisäksi tulkittu siten, että yksilö reflektoi omaa käyttäytymistään (Nykänen, 2011, 45) eli käy sisäistä keskustelua itsensä kanssa (engl. *internal thought exercises*) ja pystyy neutralisoimistekniikoiden avulla säilyttämään myönteisen minäkuvan (Cheng ym., 2014, 224) tai minimoimaan itsesyytöksiä (Silic ym., 2017, 1024) sekä vakuuttamaan itselleen, että käyttäytyminen on tietyissä tilanteissa perusteltavissa muun muassa ymmärtämättömyyteen, välttämättömyyteen, vahinkoon tai epäoikeudenmukaisuuteen vedoten (Haag, 2015, 8; Willison ym., 2018, 268). Yksilö pyrkii neutralisoimistekniikoiden avulla neutralisoimaan toistuvat lainvastaiset tai käyttäytymisnormien vastaiset teot (Nykänen, 2011, 46), ja taas toisaalta neutralisoimistekniikat tarjoavat tilapäisen vapauden tavanomaisista tai moraalisista rajoitteista (Siponen & Vance, 2010, 488, 497; Bauer ja Bernroider 2017, 45) tilanteessa, jossa neutralisointia on ylipäätään mahdollista soveltaa (Willison ym., 2018, 274–275). Neutralisoimistekniikat antavat rikoksentekijöille mahdollisuuden luopua sisäistetyistä normeista ja julkisen arvostelun vaikutuksista, jolloin rikolliset voivat vapaasti tehdä rikoksia ilman syyllisyyden ja häpeän tunteita (Willison ym., 2018, 268).

Vaikka aiemmissa tutkimuksissa sekä "neutralisointi" että "neutralisoimisteoria" tulkinnoissa viitataan rikkomukseen, poikkeavaan käyttäytymiseen tai mahdolliseen suunniteltuun poikkeavaan tekoon liittyvään häpeään ja syyllisyyteen ja näiden tunteiden neutraloimiseen, ei aiempien tutkimusten tulkinnoissa ole huomioida seuraavaa Sykesin ja Matzan (1957, 666) esittämää väitettä:

> "Instead, the juvenile delinquent would appear to be at least partially committed to the dominant social order in that he frequently exhibits guilt or shame when he violates its proscriptions, accords approval to certain conforming figures, and distinguishes between appropriate and inappropriate targets for his deviance." (Sykes ja Matza, 1957, 666).

Aiemmissa tutkimuksissa ei ole huomioitu erityisesti sitä, onko tietoturvapolitiikka rinnastettavissa Sykes ja Matzan mainitsemaan "*dominant social order*", ja sisältyykö tietoturvaan jokin vallitseva sosiaalinen järjestys. Sykes ja Matza (1957, 666–667) mainitsevat:

> "These justifications are commonly described as rationalizations. They are viewed as following deviant behavior and as protecting the individual from self-blame and the blame of others after the act. But there is also reason to believe that they precede deviant behavior and make deviant behavior possible." (Sykes ja Matza, 1957, 666)

Sykes ja Matza kuitenkin jatkavat vielä seuraavasti:

> "Disapproval flowing from internalized norms and conforming others in the social environment is neutralized, turned back, or deflected in advance. Social controls that serve to check or inhibit deviant motivational patterns are rendered inoperative, and the individual is freed to engage in delinquency without serious damage to his self image." (Sykes ja Matza, 1957, 666–667)

Aiemmissa tutkimuksissa on käsitelty oikeutusta teon aikomukseen, tekoa ennen tai teon jälkeen, mutta aiemmat tutkimukset eivät ole käsitelleet muun muassa sitä, miten neutralisointi mahdollistaa poikkeavan käyttäytymisen. Aiempien tutkimusten mukaan, huolimatta siitä, että tietoturvarikkomus ei olisikaan rikos, neutralisoimisteoria soveltuu selittämään tietoturvarikkomuksia, koska sillä rikotaan sosiaalista normia, eli organisaation tietoturvapolitiikkaa, jonka työntekijä on sisäistänyt ja johon hän on sitoutunut, ja siten tietoturvarikkomus on poikkeavaa käyttäytymistä (Siponen & Vance, 2010, 490; Kim ym., 2014; Willison ym., 2018, 273). Vaikka Siponen ja Vance (2010, 490), Kim ym., (2014, 2) sekä Nykänen (2011, 45–46) viittaavat tutkimuksissaan normien rikkomiseen, ei aiemmissa tutkimuksissa ole kuitenkaan tutkittu sitä, onko tietoturva rinnastettavissa sosiaaliseen normiin ja millainen sosiaalinen kontrolli on yhteydessä tietoturvapolitiikkaan.

Aiemmissa tutkimuksissa sekä Barlow (2013, 154) että Silic ym., (2017, 1031) ovat tulkinneet Siposen ja Vancen (2010) tarkoittaneen, että kaikilla neutralisointitekniikoilla on samanlainen vaikutus. Toisaalta tutkimukset ovat tulkinneet, että tilanteesta ja olosuhteista riippuen neutralisoimistekniikoilla on eroja eri tietoturvarikkomusten välillä (kts. esim. Barlow ym., 2013; Bauer ja Bernroider, 2017; Silic ym., 2017, 1031; Willison ym., 2018). Sykes ja Matza (1957, 670) mainitsevat: *"Certain techniques of neutralization would appear to be better adapted to particular deviant acts than to others, as we have suggested, for example, in the case of offenses against property and the denial of the victim."* Tulkinta eri tekniikoista eri tilanteessa on siis huomioitu aiemmissa tutkimuksissa hyvin.

4.2.3 Muita olettamuksia

Tutkimuksissa on korostettu koulutuksen tarpeellisuutta (Li & Cheng, 2013, 9) muun muassa neutralisointia vähentävänä tekijänä (Nykänen, 2011, 260–261). Toisaalta tutkimuksissa on korostettu sitä, että yksilö ei ymmärrä riittävän syvällisesti oman toimintansa seurauksia (Haag ym., 2015, 14; Nykänen, 2011, 267; Siponen ja Vance, 2010, 497). Silic ym., (2017, 1025) tulkinnan mukaan, työntekijät voivat käyttää neutralisointitekniikoita puolutusmekanismina, jonka avulla he heikentävät käyttäytymisensä seurauksia ja tätä kautta vähentävät tai poistavat häpeän, jota he tavallisesti tuntisivat rikkoessaan tietoisesti tietoturvapolitiikkaa. Myös Barlow ym., (2013, 147) korostaa, kuinka tehokas ja kohdennettu viestintä auttaisi työntekijöitä ymmärtämään, että tietoturvapolitiikan vastainen toiminta on virheellistä eikä "normaalia".

Kuten aiemmin mainittiin, Sykes ja Matzan teorian mukaan yksilö on sisäistänyt sosiaaliset normit niin hyvin, että tuntee syyllisyyttä ja häpeää rikkoessaan

niitä. Jos yksilö on sisäistänyt oman organisaationsa tietoturvapolitiikan mukaiset säännöt, ohjeet, lait ja vaatimukset, voidaan olettaa, että yksilö tietää ja tuntee silloin eri tilanteiden toimintatavat ja käyttäytymissäännöt. Ne ovat muodostuneet toimintaa ohjaaviksi (itsestäänselvyyksiksi) ja siten myös rinnastettavissa sosiaalisen normin mukaiseen käyttäytymiseen. Sykes ja Matza eivät viittaa teoriassaan siihen, että yksilö ei ymmärtäisi sosiaalista normia, eikä yksilö oikeuta, tai perustele neutralisoimistekniikoiden avulla sitä, mitä ei ymmärrä, tai mitä ei ole sisäistänyt. Tämä Sykesin ja Matzan väite jää useissa aiemmissa tutkimuksissa huomioimatta.

Sykesin ja Matzan neutralisoimisteorian eräänä keskeisenä väittämänä voidaan siis pitää sitä, että yksilö tuntee syyllisyyttä ja häpeää rikkoessaan vallitsevaa sosiaalista järjestystä ja sosiaalista normia[21]. Yksilö pyrkii neutralisoimistekniikoiden avulla välttämään syyllisyyden[22] ja siten säilyttämään myönteisen minä-kuvan[23].

Useimmissa aiemmissa neutralisoimisteoriaa tietoturvan yhteydessä soveltaneissa tutkimuksissa mainitaan aiemmin esitelty neutralisoimisteorian syyllisyyden välttämiseen liittyvä keskeinen oletus (Barlow ym., 2013, 146; Khansa ym., 2017, 145; Willison ym., 2018, 268). Kuitenkin aiemmissa tutkimuksissa syyllisyyden välttämisen käsittelyssä on puutteita. Muun muassa Nykänen (2011, 48) mainitsee, ettei tutkimuksen kontekstissa ole tarkoituksenmukaista tarkastella yksilön syyllisyyden tunnetta. Aiemmissa tutkimuksissa vain Silic ym., (2017) ja Siponen ja Vance (2010) käsittelevät häpeää. Vaikka Siponen ja Vance (2010, 489) tutkivat tietoturvarikkomusaikeiden yhteyttä eri neutralisoimistekniikoihin, häpeää ei oltu yhdistetty neutralisoimisteorian oletuksiin, vaan virallisiin ja epävirallisiin sanktioihin. Tutkimuksessaan Siponen ja Vance (2010, 492) viittaavat sekä Grasmick ja Bursik (1990) että Nagin ja Paternoster (1993) tutkimustuloksiin, jonka mukaan häpeä toimii pelotteena, ja vähentää yksilön motivaatiota tehdä rikkomuksia. Siposen ja Vancen (2010, 492) yhtenä hypoteesina oli "*Shame negatively affects intention to violate IS security policy*" eli häpeä vaikuttaa kielteisesti tietoturvapolitiikan rikkomukseen. Tutkimustuloksessaan Siponen ja Vance (2010, 495) toteavat, ettei tutkimus tukenut hypoteesia. Koska tutkimuksessa ei mainittu, millainen yhteys häpeällä on neutralisointiin, voidaan kysyä, mikä yhteys häpeällä ja syyllisyyden välttämisellä on tietoturvarikkomukseen, jos häpeä ei vaikuta kielteisesti tietoturvapolitiikan rikkomukseen. Silic ym., (2017, 1024) tutkivat, vaikuttaako häpeä välillisesti neutraloinnissa erityisesti niin kutsutun

[21] "Instead, the juvenile delinquent would appear to be at least partially committed to the dominant social order in that he frequently exhibits guilt or shame when he violates its proscriptions, accords approval to certain conforming figures, and distinguishes between appropriate and inappropriate targets for his deviance." (Sykes & Matza, 1957, 666)

[22] "They are viewed as following deviant behavior and as protecting the individual from self-blame and the blame of others after the act. But there is also reason to believe that they precede deviant behavior and make deviant behavior possible." (Sykes & Matza, 1957, 666)

[23] "Social controls that serve to check or inhibit deviant motivational patterns are rendered inoperative, and the individual is freed to engage in delinquency without serious damage to his self image." (Sykes & Matza, 1957, 667)

varjo-it:n yhteydessä. Silic ym., (2017, 1026, 1032) ovat tulkinneet Siposen ja Vancen (2010, 495) tutkimustuloksen siten, että kaikki neutralisoimistekniikat vähentävät häpeää ja asettaneet hypoteesiksi *"Shame is negatively associated with intentions to use Shadow IT in violation of IT security policies"*, eli häpeä vaikuttaa kielteisesti aikomukseen käyttää varjo-it ratkaisuja organisaation tietoturvakäytäntöjen vastaisesti. Tutkimustuloksessaan Silic ym., (2017, 1032) toteavat, ettei työntekijöiden hyödyntämien neutralisoimistekniikoiden tavoitteena välttämättä ole kaikissa tapauksissa häpeän vähentäminen.

Sykes ja Matza (1957, 667) mainitsevat:"*…but it is important to stress the fact that interpretations of responsibility are cultural constructs and not merely idiosyncratic beliefs*." Eli vastuun kieltäminen on Sykesin ja Matzan mukaan kuitenkin kulttuurisidonnainen eikä pelkästään omaperäinen uskomus. Maruna ja Copes (2005, 297–298) tulkinnan mukaan on oletettavaa, että eri neutralisoinnin tyypit perustuvat siis yhteiskunnan tai yhteisön eri rakenteisiin, jolloin näissä eri rakenteissa on mahdollista esiintyä eroja siinä, millaista neutralisointia kulloinkin käytetään. Neutralisoinnin hyväksyntä olisi siis jollain tapaa sidoksissa myös vallitsevaan kulttuuriin. Maruna ja Copes (2005, 298) ehdottavatkin lisätutkimuksia siitä, miten neutraloinnin hyväksyminen on vuorovaikutuksessa sosiaalisten ja rakenteellisten prosessien kanssa.

Teorian oletukset, jotka pohjustavat siihen, miksi neutralisoidaan tai onko ylipäätään syytä, miksi yksilö neutralisoisi toimintaansa, jäävät useissa aiemmissa tietoturva-aiheisissa tutkimuksissa huomioimatta. Teoriasta on ikään kuin irrotettu erilleen mekanismi, eli neutralisoimistekniikat, joista osa on otettu alkuperäisestä Sykesin ja Matzan teoriasta ja osa muista teorioista tai tutkimuksista, mutta pelkät yksittäiset neutralisoimistekniikat eivät välttämättä selitä toimintaan ryhtymisen syitä, tai sitä, mikä ohjaa yksilön käyttämään neutralisoimistekniikoita. Vaikka aiemmat tutkimukset tuovat esille arvokasta tietoa siitä, kuinka tietoturvarikkomuksia ja niiden aikomuksia neutralisoidaan, aiemmissa tutkimuksissa ei juurikaan kiinnitetä huomiota siihen, onko esimerkiksi tietyssä tilanteessa jotain, joka saa yksilön neutralisoimaan. Marunan ja Copesin (2005, 284) mukaan eri tekniikoita, jotka näyttävät palvelevan samaa tarkoitusta kuin neutralisoimistekniikat, on eri tutkimuksissa tunnistettu vähintään kymmeniä, ellei jopa satoja. Vaikka kaikki käyttävät tekosyitä ja selityksiä, silti kukaan ei käytä niitä kaikissa tilanteissa, joten näiden selitysten käyttöä tulisi pyrkiä ymmärtämään laajemmassa kontekstissa (Maruna & Copes, 2005, 285).

4.2.4 Tutkimustuloksia

Aiemmat neutralisoimisteoriaa tietoturvan yhteydessä soveltaneet tutkimukset erovat hieman tutkimustuloksissaan. Kuten Silic ym., (2017, 1033) esittävät, neutralisoinnilla on samankaltaiset vaikutukset sekä aikomukseen että todellisen käyttäytymiseen. Kuitenkin tutkittaessa työhön liittymättömän internetin käyttöä, Nykänen (2011, 260) ja Li ym., (2013, 9) ovat saaneet toisistaan eroavia tuloksia. Nykäsen (2011, 260) mukaan tietoturvakoulutuksen jälkeen vahingon kieltäminen (engl. *denial of injury*) –neutralisoimistekniikan osuus oli muuttunut, eli

toimintaa ei pidetty koulutuksen jälkeen enää niin hyväksyttävänä. Muilla tekniikoilla ei Nykäsen (2011, 260) mukaan ollut tilastollista merkittävyyttä. Li ym., (2013, 8–9) puolestaan esittävät, että kaikkiaan viisi neutralisoimistekniikkaa vahvistavat voimakkaasti työhön liittymättömän internetin käytön aikomusta.

Kuten aiemmin mainittiin, on osa aiemmista tutkimuksista (kts. esim. Barlow ym., 2013, 153; Bauer ja Bernroider, 2017, 59; Li & Cheng, 2013, 8; Cheng ym., 2014, 223–224; Siponen & Vance, 2010, 496) esittänyt, että neutralisoimistekniikat ennustavat tietoturvarikkomus aikomuksia ja ovat siten tärkeä tietoturvarikkomusten ennustaja. Kuitenkin Willison ym., (2018, 286) esittävät:

> "However, our findings indicate that techniques of neutralization increase the likelihood of employees forming computer abuse intentions only when they perceive procedural injustice not distributive injustice."(Willison ym., 2018, 286)

Eli Willison ym., (2018, 286) päätelmän mukaan neutralisointitekniikat lisäävät todennäköisyyttä sille, että työntekijät kehittävät väärinkäytös aikomuksia vain silloin, kun työntekijät havaitsevat epäoikeudenmukaisuutta resurssien jaossa noudatettaviin toiminta- ja menettelytapoihin.

4.3 Neutralisoimisteoriaa testaavat kysymykset

Kuten tässä luvussa jo aiemmin mainittiin, voi olla mahdollista, että pelkät neutralisoimistekniikat itsessään ja irrallaan neutralisoimisteorian keskeisistä väitteistä heikentävät neutralisoimisteorian selitysvoimaa. Koska aiemmat neutralisoimisteoriaa tietoturvan yhteydessä soveltaneet tutkimukset ovat pääasiassa hyödyntäneet kvantitatiivisia tutkimusmenetelmiä, tarkastellaan seuraavaksi sitä, miten teoriaa testaavat kysymykset ovat niissä mitanneet Sykes ja Matzan teorian keskeisiä olettamuksia. Aiemmat kvalitatiiviset tutkimukset, kuten Nicho ja Kamoun (2014) sekä Nykänen (2011), eivät ole sisältäneet mittauskohteisiin verrattavia mittareita, joten niitä ei käsitellä tässä yhteydessä.

Barlow ym., (2013) käyttivät tutkimuksessaan vain yhtä alkuperäisen neutralisoimisteorian neutralisoimistekniikkaa, vahingon kieltäminen. Tutkimukseen osallistujat lukivat skenaarion tilanteesta, jossa työntekijä pyytää toista työntekijää luovuttamaan salasanansa projektin määräajassa valmiiksi saattamiseksi. Tämän jälkeen osallistujat vastasivat kysymykseen, joilla tarkasteltiin heidän käsitystään kyseisestä skenaariosta. Neutralisoimistekniikan hyödyntämistä käsittelevä kysymys oli: "*How does Sam justify sharing his password in this scenario?*" Vahingon kieltämistä kuvaava vaihtoehto oli: "*He believes that no harm will result from sharing his password.*" (Barlow ym., 2013, 155.) Eli kuinka skenaariossa mainittu Sam perustelee salasanan jakamisen tuossa tilanteessa ja vastausvaihtoehto oli, ettei salasanan jakamisesta aiheudu haittaa. Edellä kerrotun kaltainen tilanne, eli salasanan luovuttaminen tietyssä tilanteessa, voisi olla realistinen selitys. Barlow ym., (2013) tutkimus ei kuitenkaan mittaa Sykes ja Matzan teorian keskeisiä oletuksia, eli syyllisyyden ja häpeän merkitystä sosiaalisesta

normista poikkeavan käyttäytymisen oikeuttamisessa. On toki mahdollista, että skenaariolla haluttiin kuvata Sykes ja Matzan esille tuomaa arvojen ja normien joustavuutta, mutta tutkimuksessa ei kuitenkaan käsitellä sitä tarkemmin.

Barlow ym., (2018) käyttivät tutkimuksessaan vain yhtä alkuperäisen neutralisoimisteorian neutralisoimistekniikkaa, vahingon kieltäminen. Tutkimusmenetelmä on hyvin samankaltainen kuin edellä esitellyssä samojen tutkijoiden aiemmassa tutkimuksessa. Tutkimukseen osallistujat lukivat skenaarion tilanteesta, jossa työntekijä pyytää toista työntekijää luovuttamaan salasanansa projektin määräajassa valmiiksi saattamiseksi. Vahingon kieltämistä tutkimuksessa käsiteltiin perusteena, ettei salasanan jakamisesta aiheudu haittaa, koska työntekijä tiesi toisen työntekijän luotettavaksi, ja koska salasanan voi vaihtaa myöhemmin toiseksi. (Barlow ym., 2018, 709.) Vaikka Barlow ym., (2018) tutkimuksessa verrataan ansiokkaasti erilaisten viestinnällisten keinojen vaikuttavuutta tietoturvapolitiikan rikkomus aikeisiin, tutkimus ei kuitenkaan mittaa Sykes ja Matzan teorian keskeisiä oletuksia, eli syyllisyyden ja häpeän merkitystä sosiaalisesta normista poikkeavan käyttäytymisen oikeuttamisessa.

Bauerin ja Bernroiderin (2017) tutkimuksessa neutralisoimisteoriaa testaavat kysymykset (taulukko 6) oli johdettu suoraan Siposen ja Vancen (2010) tutkimuksesta. Tästä syystä tulkinta siitä, kuinka näillä kysymyksillä mitataan Sykes ja Matzan teorian keskeisiä olettamuksia ja väittämiä on luettavissa myöhemmin tässä luvussa Siposen ja Vancen tutkimuksen tulkinnan yhteydessä.

TAULUKKO 6 Bauer & Bernroider (2017) artikkelin mittauskohteet

Mittauskohteet	Vapaa suomennos
Denial of responsibility: It is OK to violate the company information security policy if you don't understand it.	*Vastuun kieltäminen:* On OK rikkoa yrityksen tietoturvapolitiikkaa, jos et ymmärrä sitä.
Condemnation of the condemners: It is not as wrong to violate a company information security policy which is not reasonable	*Tuomitsijoiden tuomitseminen:* Ei ole niin väärin loukata yrityksen tietoturvapolitiikkaa, joka se ei ole järkevä.
Denial of injury: It is OK to violate the company information security policy if no damage is done to the company.	*Vahingon kieltäminen:* On OK rikkoa yrityksen tietoturvapolitiikkaa, jos se ei aiheuta vahinkoa yhtiölle.

Bauer ym., (2017) mainitsevat tutkimusaineistokseen 33 puolistrukturoitua haastattelua, joista 23 työntekijää ja 10 it-johtajaa. Bauer ym., (2017, 152) esittävät tutkimustuloksessaan, että käyttäjien kertoma suuremmaksi koettu hyöty voidaan luokitella vetoaminen korkeampiin lojaliteetteihin –neutralisoimistekniikaksi. Tutkimuksessa tai tutkimuksen liitteissä ei kuitenkaan esitellä, mitä puolistrukturoidut haastattelut mittasivat. Tästä syystä on vaikea arvioida, oliko kyse vain yksittäisistä selityksistä vai oliko niillä yhteyttä Sykes ja Matzan alkuperäiseen teoriaan.

Cheng ym., (2014) ovat soveltaneet tutkimuksessaan kaikkia Sykes ja Matzan alkuperäisen neutralisoimisteorian viittä neutralisoimis-tekniikkaan. Myös Cheng ym., (2014) hyödynsivät tutkimuksessaan joitakin Siposen ja Vancen (2010)

tutkimuksesta johdettuja niin sanottuja mittauskohteita (taulukko 7). Mitta-asteikkona Cheng ym., (2014) käyttivät: 1, täysin eri mieltä ja 7, vahvasti samaa mieltä. Tiedot oli kerätty tele- ja finanssialan organisaatioista, joissa molemmissa tietoturvapolitiikan mukaan internetin käyttö henkilökohtaisiin tarpeisiin oli kiellettyä, ja että rikkomuksesta olisi tekijälleen seuraamuksia.

TAULUKKO 7 Cheng ym., (2014) artikkelin mittauskohteet

Mittauskohteet	Vapaa suomennos
Denial of responsibility: It is OK to use the Internet access provided by the organization for personal purposes if I am not sure whether there is Internet use policy in the organization.	*Vastuun kieltäminen:* On OK käyttää organisaation tarjoamaa Internet-yhteyttä henkilökohtaisiin tarkoituksiin, jos en ole varma, onko organisaatiossa Internetin käyttöön käytäntöä.
Denial of responsibility: It is OK to use the Internet access provided by the organization for personal purpose if the Internet use policy is not explicitly advertised.	*Vastuun kieltäminen:* On OK käyttää organisaation tarjoamaa Internet-yhteyttä henkilökohtaisiin tarkoituksiin, jos Internetin käytöstä ei nimenomaisesti ilmoiteta.
Denial of responsibility: It is OK to use the Internet access provided by the organization for personal purposes if I don't understand the Internet use policy.	*Vastuun kieltäminen:* On OK käyttää organisaation tarjoamaa Internet-yhteyttä henkilökohtaisiin tarkoituksiin, jos en ymmärrä Internetin käytön käytäntöä.
Denial of injury: It is OK to use the Internet access provided by the organization for personal purposes if no harm is done	*Vahingon kieltäminen:* On OK käyttää organisaation tarjoamaa Internet-yhteyttä henkilökohtaisiin tarkoituksiin, jos ei aiheuteta mitään vahinkoa.
Denial of injury: It is OK to use the Internet access provided by the organization for personal purposes if no damage is done to the company.	*Vahingon kieltäminen:* On OK käyttää organisaation tarjoamaa Internet-yhteyttä henkilökohtaisiin tarkoituksiin, jos se ei aiheuta vahinkoa yhtiölle.
Denial of injury: It is OK to use the Internet access provided by the organization for personal purposes if no one gets hurt.	*Vahingon kieltäminen:* On OK käyttää organisaation tarjoamaa Internet-yhteyttä henkilökohtaisiin tarkoituksiin, jos kukaan ei loukkaannu.
Denial of victim: If the managers are worried about harm from personal use of the Internet they should have better online management.	*Uhrin kieltäminen:* Jos johtajat ovat huolissaan Internetin henkilökohtaisesta käytöstä aiheutuvista haitoista, heillä olisi oltava parempi online-hallinta.
Denial of victim: I don't really buy into the idea that the company loses much from personal use of the Internet.	*Uhrin kieltäminen:* En todellakaan usko ajatukseen, että yritys menettää paljon Internetin henkilökohtaisesta käytöstä.
Denial of victim: It is OK to surf the net for non-work reasons because my boss is biased and does not treat us well.	*Uhrin kieltäminen:* On OK surffata netissä muusta kuin työstä johtuvista syistä, koska pomoni on puolueellinen ja ei kohtele meitä hyvin.

Condemnation of the condemners: Managers should be more worried about other kinds of misconduct than personal use of the Internet.	*Tuomitsijoiden tuomitseminen:* Johtajien tulisi olla enemmän huolissaan muunlaisesta väärinkäytöstä kuin Internetin henkilökohtaisesta käytöstä.
Condemnation of the condemners: The Company where I work really should worry about other issues than personal use of the Internet	*Tuomitsijoiden tuomitseminen:* Yrityksen, jossa työskentelen, pitäisi huolehtia muista asioista kuin Internetin henkilökohtaisesta käytöstä.
Condemnation of the condemners: The Company has been ripping its employees off for years, so personal use of the Internet is justified.	*Tuomitsijoiden tuomitseminen:* Yhtiö on repinyt työntekijöitään vuosien ajan, joten Internetin henkilökohtainen käyttö on perusteltua.
Appeal to higher loyalties: It is OK to use the Internet access provided by the organization for personal purposes if it is somehow used to benefit an individual or a business.	*Vetoaminen korkeampiin lojaliteetteihin:* On OK käyttää organisaation tarjoamaa Internet-yhteyttä henkilökohtaisiin tarkoituksiin, jos sitä käytetään jollain tavoin hyödyksi yksilölle tai yritykselle.
Appeal to higher loyalties: It is all right to use the Internet access provided by the organization for personal purposes to get my work done more efficiently.	*Vetoaminen korkeampiin lojaliteetteihin:* On täysin oikein käyttää organisaation tarjoamaa Internet-yhteyttä henkilökohtaisiin tarkoituksiin työni tehostamiseksi.
Appeal to higher loyalties: It is OK to use the Internet access provided by the organization for personal purposes if a family member, friend, or significant other needs me to do so.	*Vetoaminen korkeampiin lojaliteetteihin:* On OK käyttää organisaation tarjoamaa Internet-yhteyttä henkilökohtaisiin tarkoituksiin, jos perheenjäsen, ystävä tai merkittävä muu vaatii minua tekemään niin.

Vaikka Cheng ym., (2014) tutkimukseen osallistuneiden organisaatioiden tietoturvapolitiikkaan sisältyi kielto internetin käytöstä henkilökohtaisiin tarpeisiin, tutkimuskysymykset eivät mittaa, uskovatko työntekijät tietoturvapolitiikkaan. Eli liittyykö tietoturvanpolitiikan noudattamiseen sama kuin lakiin, eli lakeja, joihin uskotaan, rikotaan silti, kuten Sykes ja Matza (1957, 666) esittävät. Vaikka Cheng ym., (2014) ovat koonneet varsin kattavasti erilaisia selityksiä, joita työntekijät voisivat käyttää, ei esimerkiksi vastuun kieltämiseen liittyvät kysymykset välttämättä mittaa sitä, kokeeko työntekijänä itsensä olosuhteiden uhrina tai ympäristön tuotteena, jolloin hän ei koe olevansa vastuussa tekemisistään. Kysymykset viittaavat enemmänkin selityksiin, jotka liittyvät ymmärtämättömyyteen tai tietämättömyyteen, eivätkä niinkään Sykes ja Matzan (1957, 667) esittämään: ”*...the delinquent approaches a "billiard ball" conception of himself in which he sees himself as helplessly propelled into new situations*.” Toisaalta taas vahingon kieltäminen –tekniikkaa käsittelevät kysymykset ovat hyvin realistisia, ja niihin työntekijä voisi mitä luultavimmin vastata myöntävästi. Vetoaminen korkeampiin lojaliteetteihin –tekniikka ikään kuin kokeilee, tarkoittaako tekniikka sosiaalisen siteen vai henkilökohtaisen edun asettamista niin sanotuissa arvoissa korkeammalle, mutta Cheng ym., (2014) eivät tutkimuksessaan käsittele tätä tärkeysjärjestystä tarkemmin. Cheng ym., (2014) tutkimuksen mittauskohteet eivät

myöskään suoranaisesti mittaa kokeeko työntekijä syyllisyyttä ja häpeää. Se, että tietoturvapolitiikka kieltää internetin käytön muihin kuin työtehtävien hoitamiseen, viittaisi ehdottomaan kieltoon. Cheng ym., (2014) tutkimuksen mittauskohteet eivät mittaa sitä, ovatko tietoturvarikkomukset hyväksyttyjä vai ehdottoman kiellettyjä olosuhteista riippuen. Eli onko tietoturvapolitiikka rinnastettavissa Sykes ja Matzan teoriassaan esittelemään ajatukseen, jonka mukaan sosiaalisen järjestelmän säännöt ja normit vaativat harvoin ehdotonta pakkoa.

Haag ja Eckhardt (2015) mittauskohteena (taulukko 8) käytettiin kahta alkuperäisen neutralisoimisteorian neutralisoimistekniikkaa. Mittauskohteena toimivat kysymykset ovat hyvin realistisia selityksiä, joita käyttäjät voisivat käyttää. Kuitenkaan mittauskohteet eivät välttämättä suoraan mittaa Sykes ja Matzan teorian keskeisiä väittämiä ja olettamuksia. Mittauskohteet eivät siten mittaa muun muassa sitä, uskotaanko tietoturvapolitiikkaan tai edeltääkö vai seuraako syyllisyyden ja häpeän tunteet tietoturvarikkomusta.

TAULUKKO 8 Haag & Eckhardt (2015) artikkelin mittauskohteet

Mittauskohteet	Vapaa suomennos
Denial of injury: It is OK to violate the study's code of conduct… …if no one gets hurt.	*Vastuun kieltäminen:* On OK rikkoa tutkimuksen menettelytapoja, jos kukaan ei loukkaannu.
Denial of injury: It is OK to violate the study's code of conduct… … if no harm is done.	*Tuomitsijoiden tuomitseminen:* On OK rikkoa tutkimuksen menettelytapoja, jos siitä ei ole mitään haittaa.
Denial of injury: It is OK to violate the study's code of conduct… …if no damage is done to the university.	*Vahingon kieltäminen:* On OK rikkoa tutkimuksen menettelytapoja, jos siitä ei ole yliopistolle vahinkoa.
Condemnation of the condemners 1: It is not as wrong to violate rules of conduct and usage that seem unfair to you.	*Tuomitsijoiden tuomitseminen:* Ei ole niin väärin rikkoa yrityksen tietoturvapolitiikkaa, jos se vaikuttaa epäoikeudenmukaisilta.
Condemnation of the condemners 2: It is not as wrong to violate rules of conduct and usage that seem too restrictive	*Tuomitsijoiden tuomitseminen:* Ei ole niin väärin rikkoa yrityksen tietoturvapolitiikkaa, jos ne vaikuttavat liian rajoittavilta.
Condemnation of the condemners 3: It is not as wrong to violate rules of conduct and usage that seem unjustified.	*Tuomitsijoiden tuomitseminen:* Ei ole niin väärin loukata yrityksen tietoturvapolitiikkaa, jos se vaikuttaa perusteettomilta.

Haag ym., (2015) tutkimuksissa sovellettiin yhtä Sykes ja Matzan neutralisoimistekniikkaa. Mittarina yhdestä neutralisoimistekniikasta johdetuilla kolmella kysymyksellä ei ole mahdollista tulkita Sykes ja Matzan keskeisiä väitteitä ja oletuksia. Vaikka tekijä voisi kieltää vastuunsa taulukossa 9 esitetyillä selityksillä, niillä ei välttämättä voida mitata suojeleeko tekijä näiden selitysten avulla itseään itsesyytöksiltä tai häpeän tunteilta. Kysymykset eivät myöskään mittaa, onko ohjeiden vastaisessa toiminnassa kyse sosiaalisen normin rikkomisesta.

TAULUKKO 9 Haag ym., artikkelin (2015) mittauskohteet

Mittauskohteet	Vapaa suomennos
Denial of injury: It is OK to violate the study's code of conduct… …if no one gets hurt.	*Vastuun kieltäminen:* On OK rikkoa tutkimuksen menettelytapoja, jos kukaan ei loukkaannu.
Denial of injury: It is OK to violate the study's code of conduct… … if no harm is done.	*Tuomitsijoiden tuomitseminen:* On OK rikkoa tutkimuksen menettelytapoja, jos siitä ei ole mitään haittaa.
Denial of injury: It is OK to violate the study's code of conduct… …if no damage is done to the university.	*Vahingon kieltäminen:* On OK rikkoa tutkimuksen menettelytapoja, jos siitä ei ole yliopistolle vahinkoa.

Khansa ym., (2017) tutkimuksessa sovellettiin vain yhtä Sykes ja Matzan (1957) alkuperäisen teorian neutralisoimistekniikkaa. Mittarina kysymys (taulukko 10) ei mittaa Sykes ja Matzan teorian keskeisimpiä olettamuksia.

TAULUKKO 10 Khansa ym., (2017) artikkelin mittauskohde

Mittauskohde	Vapaa suomennos
Denial of injury: It is acceptable to engage in [24]cyberloafing if no harm is done to the company.	*Vastuun kieltäminen:* Nettisurffailu on hyväksyttävää, jos yritykselle ei tehdä haittaa.

Kim ym., (2014) mainitsevat soveltaneensa neutralisoinnin mittaamisessa Siposen ja Vancen (2010) tutkimuksessa käytettyjä skenaarioita. Siposen ja Vancen (2010) tutkimuksen mittauskohteet sekä tarkastelu, miten mittauskohteet mittaavat Sykes ja Matzan teorian keskeisiä olettamuksia käsitellään myöhemmin tässä luvussa.

Li ja Cheng (2013) tutkimuksessa sovellettiin kaikkia viittä Sykes ja Matzan (1957) alkuperäisen teorian neutralisoimistekniikoita. Aiemmin esitellyn Cheng ym., (2014) tutkimuksen mittauskohteet ovat yhtä poikkeusta lukuun ottamatta samat kuin tässä Li ja Cheng (2013) tutkimuksessa. Lisäksi tietoturvarikkomuskin on sama, joten tähän kohtaan ei ole kopioitu jo aiemmin Cheng ym., (2014) tutkimuksen yhteydessä läpikäytyjä kysymyksiä ja sitä, miten teoriaa testaavat kysymykset mittasivat Sykes ja Matzan teorian keskeisiä olettamuksia. Vastuun kieltäminen –tekniikkaa mitattiin työstressin kautta. Tutkimuksessa kuitenkin tultiin siihen tulokseen, että taulukossa 11 esitetyt vastuun kieltämiseen liittyvät kysymykset eivät ennustaneet työntekijän aikomusta tietoturvarikkomukseen.

[24] Sanalle "cyberloafing"ei löydy yksittäistä suomenkielistä käännöstä, mutta termiä käytetään kuvaamaan työntekijöiden työhön kuulumatonta internetin käyttöä, kuten henkilökohtaisten sähköpostien kirjoittamista, verkko-ostoksia ja muuta niin sanottua nettisurffailua.

TAULUKKO 11 Li ja Cheng (2013) artikkelin mittauskohteet

Mittauskohteet	Vapaa suomennos
Denial of responsibility 1: It is OK to use the Internet access provided by the organization for personal purposes if …my daily tasks and job objectives is not distributed clearly.	*Vastuun kieltäminen:* On OK käyttää organisaation tarjoamaa internet-yhteyttä henkilökohtaisiin tarkoituksiin, jos päivittäiset tehtäväni ja työt eivät ole selkeitä.
Denial of responsibility 2: It is OK to use the Internet access provided by the organization for personal purposes if …the internet use policy is not explicitly advertised.	*Vastuun kieltäminen:* On OK käyttää organisaation tarjoamaa internet-yhteyttä henkilökohtaisiin tarkoituksiin, jos internetin käyttöä koskevaa käytäntöä ei nimenomaisesti ilmoiteta.
Denial of responsibility 3: It is OK to use the Internet access provided by the organization for personal purposes if …the work stress is too high	*Vastuun kieltäminen:* On OK käyttää organisaation tarjoamaa internet-yhteyttä henkilökohtaisiin tarkoituksiin, jos työstressi on liian korkea.
Denial of injury 1: It is OK to use the Internet access provided by the organization for personal purposes if …no harm is done	*Vahingon kieltäminen:* On OK käyttää organisaation tarjoamaa internet-yhteyttä henkilökohtaisiin tarkoituksiin, jos ei aiheuta vahinkoa.
Denial of injury 2: It is OK to use the Internet access provided by the organization for personal purposes if …no damage is done to the company.	*Vahingon kieltäminen:* On OK käyttää organisaation tarjoamaa internet-yhteyttä henkilökohtaisiin tarkoituksiin, jos yhtiölle ei aiheudu vahinkoa.
Denial of injury 3: It is OK to use the Internet access provided by the organization for personal purposes if …no one gets hurt.	*Vahingon kieltäminen:* On OK käyttää organisaation tarjoamaa internet-yhteyttä henkilökohtaisiin tarkoituksiin, jos kukaan ei loukkaannu.
Denial of victim 1: It is OK to use the Internet access provided by the organization for personal purposes if… if the managers are worried about harm from internet abuse they should have better online management	*Uhrin kieltäminen:* On OK käyttää organisaation tarjoamaa internet-yhteyttä henkilökohtaisiin tarkoituksiin. Jos johtajat ovat huolissaan Internetin väärinkäytöstä aiheutuvista haitoista, heillä olisi oltava parempi online-hallinta.
Denial of victim 2: It is OK to use the Internet access provided by the organization for personal purposes. I don't really buy into the idea that the company loses much from internet abuse	*Uhrin kieltäminen:* On OK käyttää organisaation tarjoamaa internet-yhteyttä henkilökohtaisiin tarkoituksiin. En todellakaan usko ajatukseen, että yritys menettää paljon Internetin väärinkäytöksistä.
Denial of victim 3: It is OK to surf the net for non-work reasons because my boss is biased and does not treat us well.	*Uhrin kieltäminen:* On OK surffata verkossa muusta kuin työstä johtuvista syistä, koska pomo on puolueellinen ja ei kohtele meitä hyvin.
Condemnation of the condemners 1: It is OK to use the Internet access provided by the organization for personal purposes if …	*Tuomitsijoiden tuomitseminen:* On OK käyttää organisaation tarjoamaa internet-yh-

Mittauskohteet	Vapaa suomennos
managers should be more worried about other kinds of misconducts than internet abuse.	teyttä henkilökohtaisiin tarkoituksiin. Johtajien tulisi olla enemmän huolissaan muunlaisista väärinkäytöksistä kuin internetin väärinkäytöstä.
Condemnation of the condemners 2: It is OK to use the Internet access provided by the organization for personal purposes if … the Company where I work really should worry about other issues than internet abuse.	*Tuomitsijoiden tuomitseminen:* On OK käyttää organisaation tarjoamaa internet-yhteyttä henkilökohtaisiin tarkoituksiin. Yritykseen, jossa työskentelen, pitäisi huolehtia muista asioista kuin internetin väärinkäytöksistä.
Condemnation of the condemners 3: It is OK to use the Internet access provided by the organization for personal purposes if … the Company has been ripping our employees off for years, so internet abuse is justified.	*Tuomitsijoiden tuomitseminen:* On OK käyttää organisaation tarjoamaa internet-yhteyttä henkilökohtaisiin tarkoituksiin. Yhtiö on repinyt työntekijöitään vuosien ajan, joten Internetin väärinkäyttö on perusteltua.
Appeal to higher loyalties 1: It is OK to use the Internet access provided by the organization for personal purposes if … If it is used to benefit an individual or a business somehow?	*Vetoaminen korkeampiin lojaliteetteihin:* On OK käyttää organisaation tarjoamaa internet-yhteyttä henkilökohtaisiin tarkoituksiin, jos sitä käytetään jollain tavoin yksilön tai yrityksen hyödyksi.
Appeal to higher loyalties 2: It is all right to use the Internet access provided by the organization for personal purposes to get my work done more efficiently	*Vetoaminen korkeampiin lojaliteetteihin:* On OK käyttää organisaation tarjoamaa internet-yhteyttä henkilökohtaisiin tarkoituksiin työn tehostamiseksi.
Appeal to higher loyalties 3: It is OK to use the Internet access provided by the organization for personal purposes if a family member, friend, or significant other needed me to do such thing.	*Vetoaminen korkeampiin lojaliteetteihin:* On OK käyttää organisaation tarjoamaa internet-yhteyttä henkilökohtaisiin tarkoituksiin, jos perheenjäsen, ystävä tai muu merkittävä vaatii minua tekemään niin.

Silic ym., (2017) mittauskohteina (taulukko 12) oli neljä Sykes ja Matzan (1957) teorian neutralisoimistekniikkaa. Vaikka Silic ym., (2017) mittauskohteet voisivat hyvinkin olla työntekijän selityksiä, ne eivät välttämättä kuitenkaan mittaa syyllisyyttä ja häpeää, jota työntekijä näillä selityksillä pyrkisi poistamaan.

TAULUKKO 12 Silic ym., (2017) artikkelin mittauskohteet

Mittauskohteet	Vapaa suomennos
Denial of responsibility: It is not my fault that my organization provides tools that are not as efficient as my cloud storage tool.	*Vastuun kieltäminen:* Ei ole minun syytäni, että organisaationi tarjoaa työkaluja, jotka eivät ole yhtä tehokkaita kuin omat pilvityökaluni.
Denial of injury: No one got hurt by my use of a zip tool I download on my own	*Vahingon kieltäminen:* Kukaan ei loukkaannu käyttämistäni zip-työkaluista, joita lataan.
Condemn the condemner: Everyone else, including you, is using software beyond the programs formally approved by the organization.	*Tuomitsijoiden tuomitseminen:* Kaikki muut, myös sinä, käyttävät ohjelmistoja, jotka ovat organisaation virallisesti hyväksymien ohjelmien ulkopuolelle.
Appeal to higher loyalty: I used an external tool to protect, or take care of, someone	*Vetoaminen korkeampiin lojaliteetteihin:* Käytin ulkopuolista työkalua suojaamaan tai hoitamaan jotakuta.

Myös Siposen ja Vancen (2010, A1 – A2) tutkimuksessa mittauskohteet oli muotoiltu kysymyksillä (taulukko 13). Koska tämän tutkimuksen rajauksena on alkuperäinen Sykes ja Matzan neutralisoimisteoria, ei tarkasteluun ole otettu mukaan myöhempiä Minorin (1981), Klockarsin (1974) tai Harrisin ja Dumasin (2009) julkaisemia neutralisoimistekniikoita, vaikka Siponen ja Vance niitä omassa tutkimuksessaan käyttivätkin. Siponen ja Vance sovelsivat tutkimuksessaan neljää Sykes ja Matzan teorian neutralisoimistekniikkaa. Lisäksi on mainittava, että Siposen ja Vancen tutkimuksessa ei keskitytty vain tietoturvarikkomusten neutralisoimiseen, vaan tutkimuksessa sovellettiin myös peloteteoriaa tutkittaessa virallisten ja epävirallisten seurausten merkitystä tietoturvarikkomuksiin. Useat tässä tutkimuksessa esitellyt aiemmat saman aihepiirin tutkimukset ovat soveltaneet näitä taulukoon 13 koottuja Siposen ja Vancen (2010) kehittämiä mittauskohteita.

TAULUKKO 13 Siponen & Vance (2010) artikkelin mittauskohteet

Mittauskohteet	Vapaa suomennos
Denial of responsibility 1: It is OK to violate the company information security policy if you aren't sure what the policy is.	*Vastuun kieltäminen:* On OK rikkoa yrityksen tietoturvapolitiikkaa, jos et ole varma, mitä politiikka on.
Denial of responsibility 2: It is OK to violate the company information security policy if the policy is not advertised.	*Vastuun kieltäminen:* On OK rikkoa yrityksen tietoturvapolitiikkaa, jos politiikkaa ei mainostettu.
Denial of responsibility 3: It is OK to violate the company information security policy if you don't understand it.	*Vastuun kieltäminen:* On OK rikkoa yrityksen tietoturvapolitiikkaa, jos et ymmärrä sitä.

Mittauskohteet	Vapaa suomennos
Denial of injury 1: It is OK to violate the company information security policy if no harm is done.	*Vahingon kieltäminen:* On OK rikkoa yrityksen tietoturvapolitiikkaa, jos ei aiheuteta vahinkoa.
Denial of injury 2: It is OK to violate the company information security policy if no damage is done to the company.	*Vahingon kieltäminen:* On OK rikkoa yrityksen tietoturvapolitiikkaa, jos se ei aiheuta vahinkoa yhtiölle.
Denial of injury 3: It is OK to violate the company information security policy if no one gets hurt.	*Vahingon kieltäminen:* On OK rikkoa yrityksen tietoturvapolitiikkaa, jos kukaan ei loukkaannu.
Condemnation of the condemners 1: It is not as wrong to violate a company information security policy that is not reasonable	*Tuomitsijoiden tuomitseminen:* Ei ole niin väärin loukata yrityksen tietoturvapolitiikkaa, joka se ei ole järkevä.
Condemnation of the condemners 2: It is not as wrong to violate a company information security policy that requires too much time to comply with.	*Tuomitsijoiden tuomitseminen:* Ei ole niin väärin loukata yrityksen tietoturvapolitiikkaa, joka vaatii liikaa aikaa noudattaa sitä.
Condemnation of the condemners 3: It is not as wrong to violate a company information security policy that is too restrictive.	*Tuomitsijoiden tuomitseminen:* Ei ole niin väärin loukata yrityksen tietoturvapolitiikkaa, joka on liian rajoittava.
Appeal to higher loyalties 1: It is all right to violate a company information security policy to get a job done.	*Vetoaminen korkeampiin lojaliteetteihin:* On aivan oikein rikkoa yrityksen tietoturvapolitiikkaa, että saa työnsä tehtyä.
Appeal to higher loyalties 2: It is all right to violate a company information security policy if you get your work done.	*Vetoaminen korkeampiin lojaliteetteihin:* On aivan oikein rikkoa yrityksen tietoturvapolitiikkaa, jos siten saa työnsä tehtyä.
Appeal to higher loyalties 3: It is all right to violate a company information security policy if you complete the task given by management.	*Vetoaminen korkeampiin lojaliteetteihin:* On oikein rikkoa yrityksen tietoturvakäytäntöä, jos suoritat johdon antaman tehtävän.

Siponen ja Vance ovat koonneet erittäin kattavasti erilaisia, yleisiä ja realistisia selityksiä tilanteista, joilla organisaation työntekijä voisi selittää tietoturvarikkomuksensa. Myös aiemmat tutkimukset (kts. esim Puhakainen, 2006; Karjalainen, 2019) ovat todenneet, kuinka esimerkiksi suuri työmäärä, kiireiset työtehtävät tai tehtävien priorisointi voivat johtaa tietoturvakäytäntöjen noudattamattomuuteen. Edellä esitellyt kysymykset eivät kuitenkaan välttämättä niin sanotusti mittaa Sykes ja Matzan neutralisoimisteorian olettamuksia.

Siposen ja Vancen (2010) tutkimuksessa esitellyt mittauskohteet eivät välttämättä suoranaisesti mittaa työntekijöiden sitoutuneisuutta tai sitä, onko tietoturvapolitiikka sosiaalinen normi, jolloin tietoturvarikkomus olisi poikkeavaa toimintaa, ja josta henkilö kokisi syyllisyyttä. Samaan tapaan kuin aiemmin käsitelty Cheng ym., (2014) tutkimus, myöskään Siposen ja Vancen (2010) kysymykset eivät mittaa sitä, uskovatko työntekijät tietoturvapolitiikkaan ja sen ohjeisiin.

Neutralisoimistekniikoista muun muassa vastuun kieltäminen –tekniikka ei välttämättä mittaa sitä, kokeeko työntekijät itsensä olosuhteiden uhrina tai että ulkopuolisiin tekijöihin vetoaminen oikeuttaisi kieltämään vastuun. Kysymykset viittaavat enemmänkin ymmärtämättömyyteen tai tietämättömyyteen liittyviin selityksiin. Vahingon kieltäminen –tekniikkaa mittaavat kysymykset saavat mitä luultavimmin työntekijän vastaamaan myöntävästi, mutta kysymykset eivät silti mittaa sitä, onko selitys silloin yleisen käytännön jatke vai normeista poikkeavaa käytöstä. Tuomitsijoiden tuomitseminen –tekniikka mittaavista kysymyksistä jää ikään kuin puuttumaan, kuka olisi se valvova taho, tai auktoriteetti, johon huomio halutaan siirtää.

Koska Siposen ja Vancen tutkimus toteutettiin Suomessa, voisivat esimerkiksi vetoaminen korkeampiin lojaliteetteihin –tekniikkaan liittyvät myönteiset vastaukset kertoa enemmän työntekijän työsopimuslaissa olevan lojaliteettivelvollisuuden noudattamisesta kuin neutralisoimisesta. Myönteiset vastaukset voisivat myös kertoa työntekijän sitoutuneisuudesta, koska myöntävät vastaukset tarkoittaisivat, että hänen lojaliteettinsa kohdistuisi organisaation toiminnan tukemiseen, eikä siten viittaisi mihinkään muuhun suurempaan lojaalisuuteen. Siinä tapauksessa kysymykset eivät välttämättä kuitenkaan vastaisi Sykes ja Matzan tarkoittamaan yleisten vallitsevien normien (engl. *the dominant normative system)* ja esimerkiksi sosiaalisten siteiden väliseen ristiriitaan, joka saa yksilön oikeuttamaan toimintaansa, ellei sosiaalinen side sitten kohdistuisi johtoon. Siponen ja Vance eivät tutkimuksessaan kuitenkaan käsitelleet tätä sosiaalista sidettä.

Siposen ym., (2020) mittauskohteet mukailevat vahvasti aiemmassa Siposen ja Vancen (2010) tutkimuksessa olleita mittauskohteita, jotka on analysoitu jo aiemmin. Tästä syystä näitä taulukon 14 mittauskohteita ei käsitellä enempää.

TAULUKKO 14 Siponen ym., (2020) artikkelin mittauskohteet

Mittauskohteet	Vapaa suomennos
Denial of responsibility 1: It is OK to use simple passwords at work if you aren't sure what the company's password guidelines are	*Vastuun kieltäminen:* On OK käyttää yksinkertaisia salasanoja, jos et ole varma, mitkä yrityksen salasanaohjeet ovat.
Denial of responsibility 2: It is OK to use simple passwords at work if the password guidelines are not advertised	*Vastuun kieltäminen:* On OK käyttää yksinkertaisia salasanoja, jos salasanaohjeita ei mainostettu.
Denial of injury 1: It is OK to use simple passwords at work if no harm is done.	*Vahingon kieltäminen:* On OK käyttää yksinkertaisia salasanoja, jos ei aiheuteta vahinkoa.
Denial of injury 2: It is OK to use simple passwords at work if no damage is done to the company.	*Vahingon kieltäminen:* On OK käyttää yksinkertaisia salasanoja, jos se ei aiheuta vahinkoa yhtiölle.
Denial of injury 3: It is OK to use simple passwords at work if no one gets hurt..	*Vahingon kieltäminen:* On OK käyttää yksinkertaisia salasanoja, jos kukaan ei loukkaannu.

Condemnation of the condemners 1: It is okay to use simple passwords at work because everyone uses simple passwords at times	*Tuomitsijoiden tuomitseminen:* On OK käyttää yksinkertaisia salasanoja, koska kaikki käyttävät toisinaan yksinkertaisia salasanoja.
Condemnation of the condemners 2: It is okay to use simple passwords at work because this is what everyone at work does.	*Tuomitsijoiden tuomitseminen:* On OK käyttää yksinkertaisia salasanoja, koska niin jokainen tekee.
Condemnation of the condemners 3: It is okay to use simple passwords at work because even the managers use simple passwords.	*Tuomitsijoiden tuomitseminen: :* On OK käyttää yksinkertaisia salasanoja, koska jopa johtajat käyttävät yksinkertaisia salasanoja.
Appeal to higher loyalties 1: It is all right to use simple passwords at work if you get your work done.	*Vetoaminen korkeampiin lojaliteetteihin:* On aivan oikein käyttää yksinkertaisia salasanoja, että saa työnsä tehtyä.
Appeal to higher loyalties 2: It is OK to use simple passwords if you carrying out an important job by your manager.	*Vetoaminen korkeampiin lojaliteetteihin:* On aivan oikein käyttää yksinkertaisia salasanoja, jos suorittaa tärkeää työtehtävää esimiehen toimesta.
Appeal to higher loyalties 3: It is all right to use simple passwords at work if it helps to get the job done.	*Vetoaminen korkeampiin lojaliteetteihin:* On aivan oikein käyttää yksinkertaisia salasanoja, jos se auttaa työn tekemisessä.
Appeal to higher loyalties 4: It is all right to use simple passwords at work if you complete the task given by management	*Vetoaminen korkeampiin lojaliteetteihin:* On aivan oikein käyttää yksinkertaisia salasanoja, jos suorittaa johdon antamaa tehtävää.

Willison ym., (2018) tutkimuksessa sovellettiin kahta Sykes ja Matzan (1957) alkuperäisen teorian neutralisoimistekniikkaa. Tutkimukseen osallistujille annettiin luettavaksi skenaarioita, joiden jälkeen heidän tuli arvioida, kuinka todennäköisesti he toimisivat samalaisissa olosuhteissa asteikolla 1 – 5, kun viisi oli ”täysin samaa mieltä” ja yksi ”täysin eri mieltä”.

Tutkimuksen vahingon kieltämiseen liittyvässä skenaariossa kuvattiin, kuinka Joe-niminen henkilö koki tulleensa kohdelluksi epäoikeudenmukaisesti jäädessään ilman korotusprosenttia. Joe ajatteli, ettei vahingoita ketään, jos hän saa tietää, kuka sai korotuksen. Joe päättää tästä syystä varastaa esimiehensä pöytälaatikosta tämän salasanan voidakseen kirjautua admin-oikeuksilla palvelimelle.

Tutkimuksen uhrin kieltämiseen liittyvässä skenaariossa Joe perusteli salaasanan varastamista sillä, että koki olevansa loukattu osapuoli.

Tutkimuksen kysymysvaihtoehdot skenaarioiden lukemisen jälkeen olivat:

- Tuntuiko Joe:sta reilulta, ettei hän saanut samaa korotusta kuin muut analyytikot?
- Tunsiko Joe, ettei ollut kovin todennäköistä, että häntä rangaistaan tietoihin pääsystä?
- Ajatteliko Joe, että hänen tekonsa eivät vahingoita ketään.

Tutkimukseen osallistujat valitsivat vielä vaihtoehdoista:

- Tällaisessa tilanteessa tekisin saman kuin Joe.
- Jos olisin Joe, olisin myös tarkastellut tietoja tällä tavalla.
- Luulen, että tekisin, miten Joe teki, jos se tapahtuisi minulle.

Willison ym., (2018) tutkimuksen skenaariot kuvailevat enemmän oikeuttamista kuin selittämistä. Salasanan varastaminen ei siten välttämättä ole enää tietoturvarikkomus, vaan kyse olisi jo rikoksesta. Willison ym., (2018) tutkimuksessa olevat kysymykset eivät kuitenkaan suoranaisesti mittaa Sykes ja Matzan (1957) teorian keskeisiä olettamuksia, kuten syyllisyyttä tai häpeää, jota henkilö kokisi tehdessään normeista poikkeavan teon.

5 TUTKIMUSMENETELMÄ, AINEISTON HANKINTA JA ANALYYSI

Tämän tutkimuksen tarkoituksena on teoreettisten lähtökohtien, aiemman tutkimustiedon, kerätyn empiirisen aineiston ja sen analysoinnin kautta löytää lisäymmärrystä työntekijöiden tietoturvarikkomuksiin. Sanotaan, ettei tutkimuksessa tärkeintä ole pelkkä tutkimustulos, vaan myös se, kuinka tulokseen on päädytty, koska tutkimustulos on riippuvainen tulokseen pääsemisen keinoista tai tavoista. Myös tapa, jolla tutkittavaa ilmiötä tai kohdetta lähestytään ohjaa niihin valintoihin (strategioihin), joita tutkimuksen aikana tehdään. Tässä luvussa tarkastellaan tämän tutkimuksen metodologiset lähtökohdat sekä esitellään ja perustellaan tähän tutkimukseen valitut aineiston keruu- ja analyysimetodit. Teoreettiset lähtökohdat ja aiemmat tutkimukset on esitelty aiemmin luvuissa kaksi ja neljä.

5.1 Metodologiset lähtökohdat

Metodioppaissa metodologia-termiin liittyy moninaista, sekä laajaa että suppeaa merkitystä (Tuomi & Sarajärvi, 2018, 13–14). Tässä tutkimuksessa metodologia-termillä myötäillään seuraavaa sitaattia:

> ”Metodologia tarkoittaa täten sääntöjä siitä, miten joitain välineitä, siis metodeja, käytetään asetetun päämäärän saavuttamiseksi. Tutkimuksen metodologia sanoo aina joitain siitä, miten ja millaisia käsitteitä on käytetty todellisuuden hahmottamiseen, jotta tulokseksi saadaan tieteellistä tietoa. Metodi siis perustelee tutkimuksessa syntyneen tiedon, mutta metodologia kysyy, onko perustelu eli käytetty menetelmä ollut järkevä.” (Tuomi & Sarajärvi, 2018, 14)

Metodologia viittaa siis ikään kuin niihin perusteisiin, joilla koko tutkimus toteutetaan. Metodologialla tarkoitetaan tässä tutkimuksessa teoriapohjan, tutkimusmenetelmän, aineistonhankintamenetelmän ja aineiston analyysimenetelmän muodostamaa kokonaisuutta. Se, mitä tutkitaan muodostaa tutkimuksen

viitekehyksen ja se, miten tutkitaan muodostaa tutkimusasetelman. Tutkimusasetelma ja valitut menetelmät ovat tässä tutkimuksessa tutkijan itsensä asettamia. Vaikka Tuomi ja Sarajärvi (2018, 14) viittaavat sääntöihin, ei sanaa ”sääntö” ole tässä tutkimuksessa tulkittu tiukkana tutkimusta hallitsevana määräyksenä. Kuten Holtkamp, Soliman ja Siponen (2018, 6280) mainitsevatkin, tutkimusmenetelmien suuntaviivat ja ohjeet eivät saisi olla tutkimuksen tekemisen esteenä vaan painopisteen tulisi olla enemmän tutkimuksen sisällössä.

Luvussa kaksi esitelty Sykes ja Matzan neutralisoimisteoria sekä tutkijan käsitys tutkittavasta ilmiöstä antoivat ikään kuin lähtökohdat koko tutkimukselle. Vahva teoriasidonnaisuus auttoi analysoimaan aiempia tutkimuksia sekä jäsentelemään empiiristä tutkimusaineistoa. Aiempaan tutkimustietoon perehtyminen puolestaan vaikutti muun muassa aiemmista tutkimuksista poikkeavan tutkimusstrategian valintaan.

5.2 Kvalitatiivisen tutkimusotteen mahdollisuudet

Tutkimuskirjallisuudessa käydään edelleen keskustelua kvantitatiivisen ja kvalitatiivisen tutkimuksen niin sanotun todistusvoiman eroista (Eskola & Suoranta, 1998, 11–13; Holtkamp ym., 2018, 6280), vaikka molempien menetelmien lähtökohtana ovat samat vaatimukset sekä teoreettisista perusteluista että arkiymmärryksen kyseenalaistamisesta (Töttö, 1997, 125). Tämän tutkimuksen tarkoituksena ei ole ottaa osaa näihin näkemyserojen keskusteluun, vaan vain esitellä ja perustella tähän tutkimukseen valittuja ratkaisuja.

Kvalitatiivisen tutkimuksen ei ole tarkoitus korvata kvantitatiivista tutkimusta, eikä päinvastoin, vaan kvalitatiivinen ja kvantitatiivinen tutkimus vastaavat vain erilaisiin kysymyksiin (Töttö, 1997, 126). Erilaisten menetelmien puolesta puhuu kuitenkin se, että niillä on mahdollista saada erityyppistä tietoa ja samankin ilmiön tutkiminen erilaisilla lähestymistavoilla ja menetelmillä voi laajentaa ja monipuolistaa ymmärrystä jonkin ilmiön luoteesta (Saaranen-Kauppinen & Puusniekka, 2006; Yin, 2014; Eisenhardt & Graebner, 2007, 28–29). Metsämuurosen (2011) mukaan kvalitatiivinen tutkimusote soveltuu hyvin silloin, kun halutaan tutkia luonnollisia tilanteita, joita ei voida järjestää kokeeksi, tai jossa kaikkia vaikuttavia tekijöitä ei voida kontrolloida.

Töttö (1997, 126–127) tarkentaa vielä, että tutkimusongelma ratkaisee sen, onko tutkimus kvalitatiivinen vai kvantitatiivinen. Jakoa ei siis tehdä aiheiden, asioiden, alojen, kohteiden tai aineistojenkaan mukaan, koska Tötön mukaan ratkaisut on tehty jo, kun aineisto hankitaan. Aiemmat neutralisoimisteoriaa tietoturvakontekstissa soveltaneet tutkimukset on enimmäkseen toteutettu kvalitatiivisin tutkimusmenetelmin, mutta kuten Maruna ja Copes (2005, 270) suosittelevat, neutralisoinnin tutkimiseen tulisi soveltaa sekä kvantitatiivisia että kvalitatiivisia lähestymistapoja. Neutralisoimisteoriaa on muilla aloilla tutkittu kvalitatiivisilla menetelmillä tutkittaessa muun muassa kuluttajien ostokäyttäytymistä, sekä niin sanottua kovan linjan rikollisuutta (kts. esim. Gruber ja Schlegelmilch,

2014; Harris ja Dumas, 2009; Topalli, 2005). Vaikka tietojärjestelmätieteessä käytetään tyypillisesti tilastollisia menetelmiä, hypoteesin testausta, matemaattisia analyyseja, kokeellista tutkimusta (Holtkamp ym., 2019, 6280), tai muita laskennalliselle logiikalle mallinnettavia menetelmiä, on kvalitatiivisen tutkimuksen monimuotoisuuden arvo tunnistettu tänä päivänä myös tietojärjestelmätieteessä (Sarker, Xiao & Beaulieu, 2013, iii; Goldkuhl, 2012, 135). Tämän tutkimuksen lähtökohtana ja pyrkimyksenä on ollut löytää mahdollisimman paljon uutta, tutkittavaa ilmiötä selittävää lisäymmärrystä. Aiemmista saman aihepiirin tutkimuksista poikkeavan lähestysmistavan, kvalitatiivisen tutkimusmenetelmän, valinta tehtiin siis jo ennen tutkimusaineiston hankintaa. Vaikka muun muassa Yinin (2014) ja Eisenhadtin (1989) mukaan kvalitatiivinen tutkimus vastaa kysymyksiin ”miksi” ja ”miten”, antaa se kuitenkin tilaa pohdiskella myös ”mitä”, ”mikä” ja ”mistä johtuu” (Töttö, 1997, 131). Kvalitatiivisen tutkimuksen valinta mahdollisti erilaisten näkökulmien tarkastelun ja oli siten luontevin valinta tutkimuksen tavoitteen saavuttamiseksi.

5.3 Tapaustutkimus

Tapaustutkimus on yleisesti käytetty kvalitatiivinen tutkimusmenetelmä (Myers & Avison, 2002, 7), vaikkei sille olekaan voitu laatia standardoitua määritelmää tai selvästi dokumentoituja toimintamalleja (Benbasat, Goldstein, & Mead, 1987, 370; Yin, 2014, 70). Tapaustutkimus soveltuu tilanteisiin, joissa tutkimus ja teoria ovat alkuvaiheessa, ikään kuin vasta muotoutuvassa vaiheessa, ja kun kyse on käytännön ongelmista, joissa toimijoiden kokemukset ovat tärkeitä ja toiminnan konteksti on kriittinen (Benbasat ym., 1987, 369). Tapaustutkimusta voidaan siis tehdä hyvin erilaista lähtökohdista ja tavoitteista (Eriksson & Koistinen, 2014, 4). Yksittäisen tapauksen puolesta puhuu esimerkiksi lähtökohta, jossa vakiintunutta teoriaa arvioidaan kriittisesti, tai tapaus on ainutlaatuinen eikä sitä voida toistaa fenomenologisista syistä, tai kun tapauksen avulla tehdään tunnetuksi jotain tai osoitetaan jotain aiemmin vaikeasti saavutettavaa (Johnston, Di Gangi, Howard & Worrell, 2019, 191). Tämän tutkimuksen voidaan todeta täyttävän tapaustutkimuksen useita lähtökohtia. Yhtenä tutkimuksen lähtökohtana ja motiivina on ollut vakiintuneen teorian kriittinen tarkastelu. Yhtenä keskeisenä lähtökohtana ja näkökulmana tarkastellaan Sykes ja Matzan neutralisoimisteorian soveltumista tietoturvarikkomuksia selittävänä teoriana. Toisena lähtökohtana voidaan lisäksi mainita, että huolimatta siitä, ettei työntekijöiden tietoturvarikkomuksia voida pitää ilmiönä uutena, silti työntekijöiden itsensä kertomana näkökulman tarkastelu ei ole helposti saavutettavissa.

Tapaustutkimusta ei tänä päivänä nähdä vain tutkimusaineiston keräämisen menetelmänä, vaan tapaustutkimus nähdään tutkimusstrategiana (Yin, 2014; Eisenhadt, 1989). Tapaustutkimus tutkii ajankohtaista reaalimaailman ilmiötä sen todellisessa ympäristössä, etenkin kun ilmiön ja kontekstin väliset rajat eivät ole selvästi ilmeisiä (Yin, 2014, 2; Laine ym., 2007,9). Eriksson ja Koistinen (2014,

7) selittävät tapaustutkimuksen kontekstuaalisuutta siten, että konteksti muodostaa tutkittavan tapauksen ympäristön. Tapaus ikään kuin liitetään reaalimaailman tehtäviin tai ongelmatilanteisiin. Järvinen ja Järvinen (2004, 82) painottavat tapaustutkimuksen mahdollisuuksista pureutua monimutkaisiin tapauksiin ja saada niistä esille uutta tietoa.

Tapaustutkimus ei ole näytteenottotutkimus (Tellis, 1997, 2; Flyvbjerg, 2006, 220; Eriksson ja Koistinen, 2014, 4), vaan empiirinen tutkimus, joka käyttää monipuolista, eri tavoilla hankittua tietoa analysoimaan tiettyä tapahtumaa tai toimintaa tietyssä rajatussa ympäristössä (Benbasat ym., 1987, 370–371). Koska yleensä kyse on useista yhdessä vaikuttavista seikoista, pyritään ilmiöstä tai aiheesta saamaan mahdollisimman kokonaisvaltainen, seikkaperäinen ja tarkka kuvaus (Benbasat ym., 1987, 370). Erona esimerkiksi kokeelliseen tutkimukseen tai kenttätutkimukseen tapaustutkimuksessa tutkijalla ei tarvitse olla ennalta omaksuttua tietoa siitä, mitä kiinnostavat muuttujat ovat ja miten niitä mitataan (Benbasat, Goldstein, & Mead, 1987, 370). Tutkija ei siis kontrolloi tapahtumia (Yin, 2014, 2).

Mikä sitten on tapaus (engl. *case*)? Vaikka tieteenalasta riippuen tapaus voidaan määritellä eri lailla, tukeudutaan tässä tutkimuksessa laadullisen tutkimuksen sanakirjan määritelmään sen yleisluontoisuuden ja selkeyden vuoksi. Schwandt (2007) selittää, että menetelmäkirjallisuudessa tapaus on esitetty erityisenä ja monimutkaisena tutkittavaksi valitun ilmiön esimerkkinä. Schwandt (2007) täsmentää, että ilmiö voi olla henkilö, prosessi, tapahtuma, ryhmä, organisaatio ja niin edelleen. Sen sijaan, että kysyttäisiin ”mikä on tapaus” tulisi ennemmin kysyä ”mistä tässä on kyse”. Tapaus on liitettävä siihen kontekstiin, jossa tapaus konkreettisesti tapahtuu, eli tapauksen tapahtumaympäristö ja sen toimijat on määriteltävä. (Eriksson ja Koistinen, 2005, 1.) Tapaus ja tutkimuskohde eivät siis tarkoita samaa asiaa, vaan tutkimuskohde viittaa enemmänkin asiaan, jota tapaus ilmentää (Eriksson ja Koistinen, 2014, 4–8; Laine ym., 2009, 10–11). Tässä tutkimuksessa sanalla ”tapaus” tarkoitetaan ilmiötä nimeltä tietoturvarikkomus. Ilmiö on kuitenkin riippuvainen tekijästä, eli kuten Crossler ym., (2013, 91) mainitsevat, monet tietoturvaa vaarantavat tekijät eivät olisi mahdollisia ilman tahallista tai tahatonta toimintaa. Erilaisten tietoturvarikkomusten kirjo on hyvin laaja, joten tässä tutkimuksessa ilmiötä tarkastellaan organisaatioympäristössä.

Tapaustutkimus ei edellytä tietynlaisten, määriteltyjen aineistojen käyttöä, vaan tapaustutkimuksessa voidaan käyttää sekä kvalitatiivista että kvantitatiivista tutkimusaineistoa (Yinin, 2014, 19). Aineisto voi myös koostua useista eri lähteistä, kuten muun muassa kirjallisista dokumenteista, arkistotiedoista ja haastatteluista (Benbasat ym., 1987, 374; Myers, 2013, 78; Eisenhardt, 1989, 535). Haastatteluiden avulla on mahdollista kerätä sellaisia tietoja, joita muista lähteistä, kuten vuosikertomuksista, sisäisistä aikakausilehdistä tai organisaation tiedotteista, ei saa tosiasiallista tai selkeää tietoa (Darken, Shanksin ja Broadbentin, 1998). Tämän tutkimuksen empiirinen osa koostuu sekä tutkimukseen osallistuneiden organisaatioiden tietoturvaan liittyvästä dokumentaatiosta että haas-

tatteluaineistosta. Kuten Keutel, Michalik ja Richter (2014, 266) esittävät, tapaustutkimusta tehtäessä tulisi olla avoin uusille lähestymistavoille, jolloin tapaustutkimuksen tarjoamat mahdollisuudet voitaisiin hyödyntää. Tapaustutkimus soveltui tämän tutkimuksen tutkimusotteeksi, koska se tarjosi joustavuutta sekä tutkimusaineiston keräämiseen että aineiston analyysiin. Tietoturvarikkomus on laaja käsite, joten ilmiön tutkiminen organisaatioympäristössä auttoi rajamaan tutkimusta. Rajaus puolestaan auttoi tarkastelemaan neutralisoimisteorian soveltumista tietoturvarikkomuksia selittävänä teoriana.

5.4 Tapaustutkimuksen kritiikki ja sen puolustus

Kaikkeen tieteen nimissä esitettyyn pitää periaatteessa suhtautua skeptisesti (Tuomi ja Sarajärvi, 2018), joten myös tapaustutkimukseen on kohdistunut monenlaista kritiikkiä. Yleinen oletus on, että esimerkiksi laajamittaiseen hypoteesien testaukseen perustuvan teorian kehittäminen olisi objektiivisempaa ja tarkempaa kuin tapaustutkimukseen perustuva (Eisenhardt ja Graebner, 2007, 26). Objektiivisuudella voidaan tarkoittaa myös sitä, ettei tutkija sekoita tai lisää omia käsityksiään, uskomuksiaan tai asenteitaan tutkimuskohteeseen (Eskola & Suoranta, 1998, 14). Jokainen tutkija joutuu omassa tutkimuksessaan käsittelemään subjektiivisuuttaan ja omia ennakkokäsityksiään (Yin, 2014), koska kuten Tuomi ja Sarajärvi (2018) esittävät, ei ole olemassa täysin puhtaasti objektiivista tietoa, vaan jokainen tutkija tekee valintoja tutkimusasetelmastaan, jolloin kaikki tieto on siinä mielessä subjektiivista. Vaikka tieteelliseen ja tutkimukselliseen ajatteluun liitetään kyseenalaistamista, systemaattisempaa tiedonkeräämistä ja erilaisten tulkintojen testaamista, silti niin sanotun arkiajattelun ja tutkimuksellinen ajattelun käynnistyminen ja eteneminen tapahtuvat samoista lähtökohdista (Hurtig, 2010, 17, 38–39). Tämän tutkimuksen tulkinnan mukaan kumpikin ajattelutapa voi olla yhtä altis virheellisille käsityksille ja tavoille lähestyä asioita. Ajattelua, niin arkista kuin tutkimuksellista, sekä rajoittavat että ohjaavat yksilön omat kokemukset, havainnot, tausta, arvot ja olemassa oleva, sen hetkinen, ymmärrys asioista. Jos ei tiedä, mitä ei tiedä, ei silloin voi myöskään ymmärtää, mikä merkitys puuttuvalla tiedolla voisi olla.

Kysymykseen, sisältääkö tapaustutkimus enemmän tutkijan subjektiivisia näkemyksiä ja ennakkokäsityksiä, Flyvbjerg (2006, 236–237) esittää näkemyksen, jonka mukaan tapaustutkimuksessa tutkija joutuu koko tutkimusprosessinsa aikana tarkentamaan näkökulmiaan. Flyvbergin mukaan tutkija joutuu hylkäämään omat ennakkokäsityksensä tuottaakseen uusia näkemyksiä (Flyvbjerg, 2006, 236–237). Tässä tutkimuksessa mahdollisten tutkijasta johtuvien oletusten, asenteiden tai uskomusten vaikutusta tutkimustulokseen pyrittiin minimoimaan valitun analyysimenetelmän avulla. Valitun analyysimenetelmän keskeinen tavoite on ohjata tutkijaa kyseenalaistamaan omat ennakkotietonsa ja ennakkoolettamuksensa.

Tapaustutkimusta on kritisoitu myös muun muassa siitä, ettei se ole tieteellisesti kontrolloitua (engl. *rigor)* (Järvinen & Järvinen, 2004, 79). Ehkä kuitenkin

yleisin kritiikki on kohdistunut yksittäisen tapauksen yleistämiseen, jolloin on katsottu, ettei yksittäistapaus voi edistää tieteellistä kehitystä (Flyvbjerg, 2006, 221). On totta, ettei tapaustutkimus sisällä samassa mielessä edustavaa otosta kuin kvantitatiiviset tutkimukset (Laine ym., 2007, 11). Flyvbjerg (2006, 229) esittää kuitenkin, kuinka usein on tärkeää selittää syvemmät syyt tiettyyn ongelmaan ja sen seurausten taakse, kuin kuvata ongelma ja selvittää sen esiintyvyys. Vaikka onkin tärkeää ymmärtää, missä määrin tietyt ilmiöt esiintyvät tietyissä ryhmissä, satunnaisotanta, joka kyllä korostaa edustettavuutta, pystyy vain harvoin tuottamaan tietoa ongelman syistä (Flyvbjerg, 2006, 241, 229). Yinin (2014, 20–21) mukaan tieteessä mikään yleistäminen harvoin perustuu yksittäisiin kokeiluihin tai testeihin (engl. *experiment*), mutta Yinin mukaan tapaustutkimukset, kuten kokeet tai testit, ovat yleistettävissä teoreettisiin ehdotuksiin eivätkä universaaleihin, yleisiin teorioihin. Tämän tutkimuksen tavoitteena ei ollut luoda universaalia teoriaa, vaan pyrkiä löytämään uutta tietoa tietoturvarikkomusten syistä. Tässä tutkimuksessa laaja edustava otos olisi ollut haasteellinen, koska eri organisaatiot ovat erilaisia, eivätkä tietoturvan standarditkaan taivu luomaan niin yhteisiä käytänteitä, että voitaisiin puhua edustavasta otoksesta.

Huolimatta kaikesta tapaustutkimukseen liittyneestä kritiikistä Keutel ym., (2014, 256) toteavat tapaustutkimuksen olevan tänä päivänä tietojärjestelmätieteessä hyväksytty menetelmä muiden menetelmien joukossa.

5.5 Teoriaa rakentava tapaustutkimus

Eisenhardtin (1989, 532) mukaan tapaustutkimuksen (engl. *case study*) avulla on mahdollista rakentaa teoria, jolloin tutkimus on iteratiivinen prosessi, ja etenee induktiivisesti[25] havaintojen pohjalta kohti teoriaan. Eisenhardtin (1989, 533) mukaan perinteisesti teorian kehittämiseen on yhdistetty aiempia kirjallisuuden havaintoja, tervettä järkeä ja kokemusta, jolloin sidos tosiasiallisiin/todellisiin (engl. *actual*) tietoihin on ollut heikko. Eisenhardtin (1989, 533) teorianmuodostusprosessissa on kaikkiaan kahdeksan vaihetta, jotka esitellään tutkimuksen tekijän vapaasti suomentamana taulukossa 15. Eisenhardtin esittämää mallia on pyritty soveltamaan tietojärjestelmätieteen tutkimuksissa (kts. esim. Urquhart & Vaast, 2012). Vaikka tässä tutkimuksessa mukaillaan Eisenhardtin teorianmuodostusprosessia, sitä ei ollut tarkoitus testata yksityiskohtaisen tarkasti, vaan teorianmuodostusprosessi auttoi etenemään tutkimuksen vaiheesta aina seuraavaan.

Eisenhard (1989, 536) esittää, kuinka aloitusvaiheessa tutkimusongelman tulisi keskittyä hyvin määriteltyyn, tiettyyn ongelmaan. Vaikka tutkimuskysymyksen ja mahdollisten käsitteiden varhainen tunnistaminen onkin hyödyllistä, Eisenhardt muistuttaa niiden olevan vasta alustavia, jolloin painopiste voi muuttua aineiston keräämisen aikana (Eisenhardt, 1989, 536). Eisenhardtin (1989, 536)

[25] Induktiivinen tulee sanasta induktio, jolla tarkoitetaan tieteenfilosofista päättelyä, joka etenee yksityiskohdista yleistyksiin. Jos esimerkiksi rakennetaan teoriaa havaintojen pohjalta, tämä tavallisesti käsitetään induktioksi. Induktio usein liitetään ns. ennalta strukturoimattomiin, pelkästään kvalitatiivisiin tutkimusmenetelmiin.

mukaan on tärkeää pyrkiä mahdollisimman lähelle tilannetta, jossa ei käsitellä mitään teoriaa eikä testattavia hypoteeseja. Vaikka tässä tutkimuksessa pyrittiin jäljittelemään tuota Eisenhardtin esittämää teoreettista joustavuutta, ei tutkimuksessa voitu täysin noudattaa ihannetilannetta. Tutkimusaineiston kerääminen aloitettiin ilman etukäteen valittuja hypoteeseja ja ennakko-odotuksia, mutta valita tutkimuksessa sovellettavasta teoriasta oli tehty jo tutkimuksen suunnitteluvaiheessa. Teoreettinen näkökulma ja aiempiin tutkimuksiin perehtyminen auttoivat käsitteiden määrittelyssä, vaikka teoriasta ei johdettu testattavia hypoteeseja. Neutralisoimisteorian keskeiset olettamukset auttoivat hahmottamaan niiden tulkintaa tietoturvan yhteydessä.

Eisenhardtin (1989, 536–537) mukaan toinen, eli tapauksen valinta on tärkeä vaihe. Valinta ei ole satunnaisotos tietystä joukosta, vaan esimerkiksi kohdealueen erityistapaus. Kolmannessa vaiheessa valitaan tiedonkeruumenetelmät. Eisenhardtin (1989, 538) mukaan tiedon kerääminen useammalla tavalla tukee vahvemman todistuspohjan muodostamisessa. Tapaustutkimus yhdistetään usein kvalitatiiviseen tutkimukseen, mutta siihen voidaan yhdistää myös kvantitatiivista tutkimusmenetelmää. Esimerkiksi kvantitatiiviset tulokset voivat auttaa erottamaan vaikeasti havaittavia riippuvuussuhteita ja siten korjata vääriä tulkintoja. (Eisenhardtin 1989, 538–539.) Tämä tutkimus myötäilee osittain Eisenhardin esittämää teorian muodostamisen prosessia. Tässä tutkimuksessa tutkimuksen teki yksi tutkija, eikä toista tutkijaa tai tutkimusryhmää ollut. Myöskään erilaisia tutkimusmenetelmiä ei tässä tutkimuksessa käytetty. Tässä kohtaa on vielä korotettava, ettei tässä tutkimuksessa sanalla ”tapaus” tarkoiteta yksittäisiä organisaatioita, vaikka empiirinen tutkimusaineisto kerättiin kahdesta organisaatiosta. Tutkimukseen osallistuneet organisaatiot esitellään myöhemmin tässä luvussa.

Eisenhardt (1989, 539–540) jatkaa, kuinka teoriaa rakentavassa tutkimuksessa aineiston kerääminen ja analysointi tehdään ainakin osittain päällekkäin ja tutkimuksen tiedonkeruuprosessia voidaan myös muuttaa. Muutoksia voidaan tehdä muun muassa tutkimuskohteiden lisäämiseen, haastattelukysymysten lisäämiseen tai tiedonkeruumenetelmiin. Näiden tarkoituksena on, että ilmiöstä kyetään saamaan mahdollisimman hyvä kokonaiskuva. Aineisto analysoidaan kohde kerrallaan. Yksittäisiin tutkimuskohteisiin perehtyminen helpottaa kohteiden vertailua. Vertailun avulla pyritään löytämään kohteita yhdistäviä malleja. Samalla voidaan löytää kohteiden erityispiirteitä ennen kuin löydettyjä yhteneväisyyksiä pyritään yleistämään. Kerätyn aineiston ja teorian vertailu tapahtuu iteroiden niin, että teoria alkaa muistuttaa läheisesti aineistoa. Vastaavuudet varmistavat empiirisesti pätevän teorian, jossa apuna käytetään kerätystä aineistosta saatua uutta, tarkempaa ymmärrystä kohdealueesta, lisäksi mitataan malleja ja todennetaan riippuvuussuhteita. Vaikka riippuvuussuhteiden havaitsemiseen hyödynnetään hypoteesien testaamista, teoriaa luotaessa kyse ei ole tilastollisesta testaamisesta siinä mielessä kuten useimmiten kvantitatiivisissa tutkimuksissa tutkimusaineistoa tarkastellaan. Erona on muun muassa se, että malli, mallin tarkkuus ja ulottuvuudet johdetaan aineiston analyysistä, eivätkä ne siten

ole etukäteen tiedossa olevia. (Eisenhardt, 1989, 540–543.) Tämän tutkimuksen empiirisen aineiston analysointiprosessi esitellään myöhemmin tässä luvussa.

Eisenhardt (1989) selittää, kuinka muotoutuvan teorian suhteuttaminen olemassa olevaan kirjallisuuteen lisää tutkimuksen sisäistä validiteettia ja yleistettävyyttä, sekä lisää teoriaa rakentavan tutkimuksen teoreettista tasoa. Suhteuttamisessa otetaan huomioon sekä tutkimuksen kanssa ristiriidassa oleva kirjallisuus, että tutkimusta tukeva kirjallisuus. Viimeinen Eisenhardtin teorianmuodostusprosessin vaihe on tutkimuksen päättäminen. Tutkimus päätetään, kun teoreettinen saturaatio on saavutettu, eikä tutkimuskohteen lisääminen lisää merkittävästi saatua uutta tietoa. Rajoitteena voivat olla myös aika ja raha. (Eisenhardt, 1989, 544–546.) Eisenhardin teorianmuodostusprosessin vaiheet on koottu taulukkoon 15.

TAULUKKO 15 Eisenhardin teorianmuodostusprosessi

Askel	Vaiheen toiminto	Perustelut
Aloitus	Tutkimuskysymysten määrittely Ei teoriaa eikä hypoteesejä	Tarkennus ytimeen Tilaa teoreettiselle joustavuudelle
Tapauksen valinta	Määrätty perusjoukko Teoreettinen otos	Tutkimuskohteen kannalta hyödylliset caset
Tiedonkeruu työtapojen ja välineiden virittely	Monet aineistonkeruu menetelmät (laadulliset ja määrälliset menetelmät, monien tutkijoiden käyttö)	Aineiston triangulaatio Erilaiset näkemykset esiin
Tutkimuskentälle meno	Yhtäaikainen aineiston keruu ja analyysi. Joustavat ja tavanomaisesta poikkeavat aineiston keruun menetelmät	Nopeuttaa analyysia ja mahdollistaa kohdistukset aineiston ominaispiirteisiin
Aineiston analyysi	Tapauksen sisäinen analyysi Tapausten välisten yhtäläisyyksien etsintä eri tekniikoiden avulla	Perehdyttää aineistoon ja alustavaan teorianmuodostukseen Pakottaa luopumaan ensivaikutelmista ja katsomaan alkuperäistä aineistoa monien linssien läpi
Hypoteesien muodostus	Kysytään todistusaineistolta miksi kysymyksiä	Terävöitetään luotujen käsitteiden validiteettia ja mitattavuutta Vahvistetaan, laajennetaan ja terävöitetään teoriaa
Aiempiin tutkimuksiin vertaus	Vertailu eriäviin tutkimustuloksiin Vertailu vahvistaviin samanlaisia tuloksia tuottaneisiin tutkimuksiin	Kohotetaan teoreettista tasoa ja terävöitetään yleistettävyyttä
Prosessin lopetus		

5.6 Tutkimuksen aineisto

Kuten jo aiemmin on mainittu, haluttiin tässä tutkimuksessa poiketa aiempien saman aihepiirin tutkimusten tutkimusmenetelmistä. Vaikka aiemmat saman aihepiirin tutkimukset ovat tuoneet esille arvokasta tietoa työntekijöiden tietoturvarikkomusten taustoista, odotettiin erilaisen lähestymistavan ja menetelmän valinnan monipuolistavan ilmiön selittämistä ja tuovan uutta tietoa. Kuten Hirsjärvi ja Hurme (2008, 48) ovat todenneet:"*On luontevaa kysyä toiselta ihmiseltä suoraan häntä itseään koskevia asioita*." Tässä tutkimuksessa työntekijöiden ääni haluttiin kuuluviin, ja antaa siten heidän itsensä kertoa kokemuksistaan, ajatuksistaan, uskomuksistaan ja tunteistaan. Tästä syystä aineistona on käytetty kahdesta organisaatiosta kerättyä haastatteluaineistoa. Lisäksi muuna aineistona on käytetty tutkimukseen osallistuneiden organisaatioiden tietoturvapolitiikan dokumentaatiota sekä muuta tietoturvaan liittyvää ohjeistusta.

5.6.1 Tutkimukseen osallistuneet organisaatiot

Molemmat organisaatiot ovat suomalaisia julkisen sektorin organisaatiota, joissa työskentelee useita satoja henkilöitä eri alojen ammateissa. Organisaatiot haluavat omasta toivomuksestaan jäädä anonyymeiksi, joten tutkimuksen raportoinnissa tätä toivetta on pyritty kunnioittamaan. Koska organisaatioiden tarkka maantieteellinen sijainti, pääasiallinen toimiala ja organisaatiorakenne eivät vaikuta tutkimustulokseen, tulevat kaikki organisaatioihin liittyvät kuvaukset jäämään yleiselle tasolle. Tietoturva-alalla tällainen käytäntö on yleinen, koska tietoturvan voi aiheena luokitella arkaluoteiseksi (Siponen ym., 2014, 220). Vaikka organisaatioiden toimialat ovat keskenään hyvin erilaiset, voidaan sanoa, että molemmat organisaatiot käsittelevät kansallisesti arvokasta tietoa. Tästä syystä tietoturvan merkitys korostuu molempien organisaatioiden päivittäisessä toiminnassa.

Molempien organisaatioiden päivittäisessä käytössä on erilaisia tietoverkkoratkaisuja[26] sekä erilaisiin käyttöympäristöihin tarkoitettuja tietojärjestelmiä[27]. Organisaatioiden tietoturvaan liittyvät periaatteet pohjautuvat sekä kansallisiin että kansainvälisiin velvoittaviin säädöksiin, ohjeisiin ja määräyksiin, jotka velvoittavat muun muassa hyvään tiedonhallinta tapaan. Vaikka organisaatioilla on

[26] Tässä tutkimuksessa tietoverkkoratkaisun määrittelyssä tukeudutaan osittain mukaillen (EY) N:o 460/2004 määritelmään. Tietoverkkoratkaisulla tarkoitetaan siirtojärjestelmiä sekä soveltuvin osin kytkentä- tai reitityslaitteistoa ja muita välineitä, joilla voidaan siirtää signaaleja johtojen välityksellä, optisesti tai muulla sähkömagneettisella tavalla, mukaan luettuina kiinteät (piiri- ja pakettikytkentäiset, mukaan luettuna Internet) ja matkaviestinnän maanpäälliset verkot.

[27] Tässä tutkimuksessa tietojärjestelmän määritelmässä tukeudutaan osittain mukaillen (EY) N:o 460/2004 määritelmään, koska se on toimialasta riippumaton. Tietojärjestelmällä tarkoitetaan tietokoneita ja sähköisen viestinnän verkkoja sekä sähköisiä tietoja, joita niissä varastoidaan tai käsitellään tai joita niillä hankitaan tai siirretään näiden järjestelmien toimintaa, käyttöä, suojausta tai ylläpitoa varten.

omista toimialoistaan johdettuja tietoturvaan liittyviä käytäntöjä, myötäilevät päivittäiset tietoturvakäytännöt yleisesti suomalaisissa julkisen sektorin organisaatiossa käytössä olevia käytänteitä. Näitä ovat muun muassa ohjeet salasanojen muodostamiseen, asiakirjojen ja muiden tietoaineistojen käsittelyyn sekä tiedon luokitteluun.

Kummallakin organisaatiolla on laadittuna ajan tasalla oleva tietoturvapolitiikka. Vaikka molemmat organisaatiot ovat suomalaisia julkisen sektorin organisaatioita, on niissä organisaatioiden erilaisuudesta johtuen erilaiset tietoturvapolitiikat. Toisessa organisaatiossa tietoturvapolitiikka on huomattavasti laajempi ja yksityiskohtaisemmin laadittu kuin toisessa. Tietoturvapolitiikan dokumentaation kokonaislaajuus ilman lainsäädännön osuutta on useita kymmeniä sivuja. Laajuuden ja yksityiskohtaisuuden perusteella on mahdollista päätellä, että tietoturva on erittäin merkittävä jokaisen työntekijän päivittäisessä työssä huomioon otettava tekijä. Laajempi tietoturvapolitiikka sisältää tietoturvaan liittyviä keskeisiä periaatteita, vastuita, vaatimuksia, toteuttamistapoja, kehittämisen tavoitteita ja riskienhallintaa. Toisen organisaation suppeampi tietoturvapolitiikka, alle kymmenen sivua, sisältää myös tietoturvaan liittyvät keskeiset periaatteet, vastuut, tavoitteet sekä joitain toteuttamistapoja, mutta tietoturvapolitiikka on kirjoitettu niin sanotusti niin ylätasoiseksi, ettei se sisällä mitään käytännön ohjeistusta. Tietoturvapolitiikan suppeus ei kuitenkaan tarkoita, etteikö tietoturva olisi toisessakin organisaatiossa tärkeä jokaisen työntekijän huomioon otettava tekijä. Molemmilla organisaatiolla on tietoturvapolitiikan lisäksi myös yksittäisiä ohjeita erilaisiin toimintoihin, joissa tietoturva tulee huomioida. Näitä ovat muun muassa ohjeet salattujen sähköpostiviestien lähettämiseen sekä erilaisten tietoaineistojen käsittelyyn ja säilyttämiseen erilaisissa ympäristöissä. Lisäksi molemmat organisaatiot järjestävät työntekijöilleen sekä pakollista että vapaaehtoista, pääasiassa sähköisessä muodossa olevaa, tietoturvakoulusta.

Julkisen sektorin organisaatioihin on Suomessa viime vuosina kohdistunut erilaisia säästötoimenpiteitä. Myöskään tutkimukseen osallistuneet organisaatiot eivät ole välttyneet erilaisista organisaatiomuutoksilta, joiden perusteena tai taustoina ovat olleet erilaiset säästösyyt. Näiden muutosten seurauksena osa organisaatioiden toiminnoista on ulkoistettu eri palveluntarjoajille, ja näillä ulkoistuksilla on ollut vaikutusta myös organisaatioiden päivittäiseen toimintaan.

5.6.2 Haastatteluaineisto

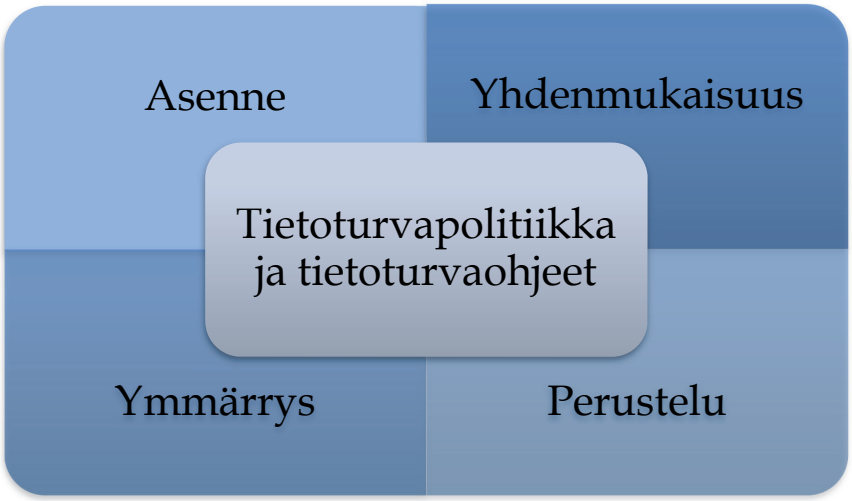
Tutkimuksen haastatteluaineisto kerättiin kolmessa osassa siten, että ensimmäiseltä organisaatiolta pyydettiin tutkimuslupaa tutkimuksen ensimmäiseen osaan lokakuussa 2016 ja myöhemmin toiseen osaan kesäkuussa 2017. Myönteiset tutkimusluvat sisälsivät sekä haastatteluiden toteutukseen että tutkimusaineiston käsittelyyn liittyviä rajoitteita, joilla ei kuitenkaan ole vaikutusta tutkimustulokseen. Tutkimuksen kolmanteen osaan, eli niin sanottuun vertailuaineistoon, pyydettiin toisesta organisaatiosta tutkimuslupaa huhtikuussa 2019. Organisaatioiden toivoman anonymiteetin vuoksi tutkimuslupahakemuksia ja niihin liittyviä päätöksiä ei ole liitetty tämän tutkimuksen liitteisiin.

Ensimmäisestä tutkimukseen osallistuneesta organisaatiosta haastateltiin joulukuun 2016 – marraskuun 2017 välisenä aikana kahtakymmentä työntekijää. Toisesta organisaatiosta haastateltiin toukokuun 2019 – heinäkuun 2019 välisenä aikana viittä työntekijää, joista yksi kieltäytyi lopulta haastatteluaineiston käytöstä. Tällä kieltäytymisellä ei kuitenkaan ole vaikutusta tutkimustulokseen. Haastatteluaineistoa kertyi siis kaikkiaan 24 haastattelua. Kukin haastattelu kesti noin tunnin ja tekstiaineistoksi purettuna haastatteluista muodostui reilut 200-sivuinen monipuolinen tekstiaineisto. Haastatteluaineistoa ei analysoitu yhtenä aineistona, vaan ensimmäisenä tutkimukseen osallistuneesta organisaatiosta kerätty aineisto muodosti yhden analysoitavan aineiston ja toisesta organisaatiosta kerätty haastatteluaineisto toimi vertailuaineistona. Seuraavaksi kerrotaan haastatteluaineiston keräämisestä.

Hirsjärvi ja Hurme (2008, 42) selittävät haastattelun muistuttavan monin tavoin keskustelutilannetta, koska molemmat perustuvat sekä kielelliseen että eikielelliseen kommunikaatioon, jonka avulla voi välittää ajatuksia, asenteita, mielipiteitä, tietoja ja tunteita. Verrattuna esimerkiksi kyselylomakkeeseen haastattelu on menetelmänä joustavampi ja tarjoaa paremmat mahdollisuudet motivoida henkilöitä osallistumaan tutkimukseen. Haastattelussa on myös mahdollista vaihdella aiheiden järjestystä, saada kuvaavia esimerkkejä ja esittää täsmentäviä kysymyksiä. (Hirsjärvi & Hurme, 2008, 36.) Tämän tutkimuksen haastattelulaji oli teemahaastattelu. Teemahaastattelu-termiä ei tiettävästi esiinny muissa kielissä, mutta se pohjautuu kohdennettu haastattelu -termiin (engl. *the focused interview*). Teemahaastattelu asettuu ikään kuin tarkasti muotoillun lomakehaastattelun ja vapaan syvähaastattelun välimaastoon. (Hirsjärvi & Hurme, 2008, 48.) Teemahaastattelussa aiempien tutkimusten ja aihepiiriin tutustumisen pohjalta suunnitellaan aihepiirit, eli teemat, ovat kaikille haastateltaville samat, vaikkakin niiden järjestys ja laajuus vaihtelevat haastattelusta toiseen. Tarkassa järjestyksessä esitettävien kysymysten sijasta haastateltavien vapaalle puheelle annetaan tilaa. (Eskola & Suoranta, 1998, 64; Saaranen-Kauppinen & Puusniekka, 2006.) Teemahaastattelu edellyttää sekä tutkittavan aihepiirin että haastateltavien tilanteen tuntemista, jotta haastattelu voidaan kohdentaa määriteltyihin teemoihin (Saaranen-Kauppinen & Puusniekka, 2006). Haastateltavien tilanteen tunteminen tarkoittaa tässä yhteydessä tietämystä siitä, että jokainen haastateltava joutui tavalla tai toisella huomioimaan tietoturvan merkityksen päivittäisissä työtehtävissään.

Teemat oli johdettu sekä Sykesin ja Matzan teoriasta että aiemmista tutkimuksista. Kuvioon 3 on pelkistetty haastatteluiden teemat. Koska kukin haastattelutilanne pyrittiin luomaan mahdollisimman keskustelunomaiseksi, ei eri teemoihin luotu tarkkoja kysymyksiä, vaan runko, jolla keskustelua ohjattiin. Vaikka kukin teema on tässä kohtaa pelkistetty yhteen sanaan, haastattelussa teemoista keskusteltiin arkisten tietoturvaan liittyvien asioiden kautta. Näitä ovat muun muassa salasanojen vaihtamiseen ja muodostamiseen liittyvät käytänteet, kalasteluviestit, tietojen siirto, tiedonluokittelu, tietoturvakoulutus ja tietoturvatietoisuus. Kaiken keskiössä on tietoturvapolitiikka ja sen noudattamisohjeet.

Kaikki teemat linkittyvät toisiinsa, eli vaikka asenteella tarkoitetaan suhtautumista tietoturvapolitiikkaan, siihen liittyy vahvasti myös se, koetaanko tietoturvapolitiikka ohjeineen ymmärrettäväksi. Ymmärryksellä tarkoitetaan myös tietämystä ohjeiden noudattamattomuuden seurauksista. Myös yhdenmukaisuus linkittyy ymmärrykseen, mutta tässä pelkistyksessä yhdenmukaisuudella tarkoitetaan myös oletusta organisaation sitoutumisen vaikutusta tietoturvakäyttäytymiseen. Perustelulla tarkoitetaan työntekijöiden kuvauksia erilaista tietoturvapolitiikan noudattamiseen liittyvistä haasteista, jotka voivat johtaa tai ovat johtaneet tietoturvarikkomukseen.



KUVIO 3 Haastatteluiden keskeiset teemat

Jokainen haastattelu aloitettiin keskustelemalla siitä, kuinka hyvin haastateltava arvio tuntevansa organisaation tietoturvapolitiikan/-politiikkoja ja kuinka merkittävä työtehtävissä huomioon otettava tekijä tietoturva hänen mielestään on. Tämä auttoi arvioimaan alustavasti, mistä teema-alueesta haastattelua jatkettiin. Haastatteluita varten oli olemassa haastattelurunko, ja vaikka teemat olivatkin jokaisessa haastattelussa samat, mahdollisti teemahaastattelu teema-alueiden järjestyksen ja laajuuden vaihtelun haastateltavan työnkuvan ja kokemuksen mukaisesti. Teemahaastattelu mahdollisti myös keskustelunomaisen vuorovaikutustilanteen, eli antoi tilaa sekä avoimille että tarkentaville kysymyksille.

5.7 Haastatteluiden haasteet ja toteutus

Eräs haastatteluihin liittyvä ongelma on haastateltavien nimettömyyden säilyvyys suhteessa jaettuihin tietoihin (DiCicco-Bloom & Crabtree, 2006, 319). Tässä tutkimuksessa haastateltaville luvattiin anonymiteetti. Tästä syystä haastateltavien henkilöllisyyteen tai ammattiin liittyviä tietoja ei tulla esittelemään. Myös-

kään haastateltavien taustatietoja (ikää, sukupuolta, ammattia, asemaa organisaatiossa tms.) ei esitetä taulukkona eikä otteita haastateltavien ilmauksista merkitä millään koodijärjestelmällä (numeroin, kirjaimin, nimimerkein tms.). Tällä pyritään varmistamaan, ettei vastausten yhdisteleminen lisäisi yksittäisen haastateltavan tunnistettavuutta. Eisenhardt ja Graebner (2007) korostavat, että haastatteluaineiston tulisi koostua organisaation eri hierarkiatasoista, yksiköistä tai ryhmistä. Tämän tutkimuksen tavoitteena oli haastatteluiden avulla kerätä työntekijöiltä mahdollisimman monipuolisia näkemyksiä, kokemuspohjaisia käsityksiä ja asenteita. Tietoturva on tutkimukseen osallistuneissa organisaatioissa jokaisen työntekijän tärkeä huomioon otettava seikka. Tämän tiedon saattoi päätellä organisaatioiden toimialoista, joten jo etukäteen oli tiedossa, että jokaisella haastateltavalla oli omakohtaista kokemusta tietoturvasta. Samalla oli oletettavaa, että sekä tutkija että haastatteluun osallistuva keskustelivat samasta aiheesta. Sitä, kuinka vahvoja haastateltavien näkemykset, kokemukset tai mielipiteet aiheesta olivat, oli mahdotonta selvittää etukäteen. Haastattelut suoritettiin haastateltavan aikataulun ja saatavuuden mukaan. Haastatteluun osallistuneet valikoituivat lopulta niin sanotulla lumipallo-otannalla, eli haastateltavat mainitsivat seuraavia mahdollisia haastateltavia, jotka työskentelivät erilaisissa työtehtävissä, ja joita tutkimukseen osallistuminen mahdollisesti kiinnosti. Yhteydenotto haastateltaviin suoritettiin ensisijaisesti sähköpostitse.

Haastateltavat eivät osallistuneet tutkimukseen palkkion tai muun korvauksen vuoksi. Se, että kummankin organisaation työntekijät joutuvat huomiomaan tietoturvan omissa päivittäisissä tehtävissään toimi erittäin vahvana motivaationa haastatteluihin osallistumisessa. Useat haastateltavat toivoivat uusia näkökulmia aiheeseen, ja jälkeen päin monet haastateltavat totesivat keskustelunomaisen haastattelutilanteen antaneen heille uutta ajateltavaa ja näkökulmia myös heidän omaan työhönsä.

Yhtä poikkeusta lukuun ottamatta kaikilla haastateltavilla on takanaan useamman vuoden työkokemus omassa organisaatiossaan ja siten hyvä organisaatiotuntemus. Haastateltavat ovat eri-ikäisiä, heidän vastuullaan on erilaisia työtehtäviä organisaation eri hierarkiatasoilla ja organisaatioiden eri yksiköissä. Muutamien haastateltavien työnkuvaan sisältyy tietoturvarikkomusten selvittämistä sekä tietoturvaratkaisujen suunnittelua ja kehittämistä. Ensimmäisestä tutkimukseen osallistuneesta organisaatiosta haastattelut suoritettiin yksilöhaastatteluina työympäristön ulkopuolella. Tällä ratkaisulla pyrittiin mahdollistamaan, etteivät haastateltavat keskenään tienneet keitä muita organisaation työntekijöitä tutkimukseen osallistui. Toisesta tutkimukseen osallistuneesta, niin sanotusta vertailuorganisaatiosta, haastattelut suoritettiin haastateltavien työympäristössä, kuitenkin siten, etteivät haastatteluun osallistuneet keskenään tienneet, keitä haastatteluun osallistui. Koska on kuitenkin täysin mahdollista, että haastateltavat ovat keskustelleet osallistumisestaan tutkimukseen, ei haastateltavien ilmauksien yhteyteen merkitä haastatteluiden ajankohtia eikä mitään, mikä mahdollisesti lisäisi henkilöiden tunnistettavuutta. Jokaista haastattelua varten varattiin rauhallinen ja häiriötön paikka. Tällä pyrittiin minimoimaan mahdollisia haastatteluympäristöstä aiheutuvia häiriötekijöitä.

Jokaisella haastateltavalla oli mahdollisuus tutustua tutkimussuunnitelmaan, joten he tiesivät, millaiseen tutkimukseen haastatteluaineistoa tullaan käyttämään. Lisäksi tutkija kävi jokaisen haastattelun alussa läpi, mikä tutkimuksen tarkoitus on. Haastatteluihin osallistuminen oli vapaaehtoista. Jokaiselle haastattelulle oli varattu runsaasti aikaa ja kukin haastattelu kesti noin tunnin. Kahta poikkeusta lukuun ottamatta haastattelut nauhoitettiin haastateltavan luvalla. Yksi haastateltava koki nauhoituksen liian epämiellyttävänä ja toinen nauhoittamatta jäänyt haastattelu törmäsi teknisiin ongelmiin, joten haastatteluista koottiin muistiinpanot. Tekstimuotoon purettu haastattelu lähetettiin jokaiselle haastatellulle mahdollisia korjauksia tai tarkennuksia varten ennen analysointia. Yksi haastateltava kieltäytyi lopulta antamasta haastatteluaineistoa tutkimuksen käyttöön, yksi haastateltava korjasi yhtä lausetta ja yksi haastateltava tarkensi oman organisaationsa yhtä toimintatapaa.

Tietoturva-alan tutkimusten yhtenä haasteena on se, että tutkimukseen osallistuvat vastaavat siten, miten olettavat olevan sosiaalisesti hyväksyttävää vastata (Barlow ym., 2018, 698). Tässä tutkimuksessa haastatteluiden alussa jokaiselle haastateltavalle selitettiin, ettei haastattelussa keskitytä organisaation toimintatapojen tai teknisten ratkaisujen tarkkoihin yksityiskohtiin. Haastatteluissa tärkeintä oli haastateltavan omat näkemykset, kokemukset ja mielipiteet tutkimusaiheesta, koska ilman niin sanottujen loppukäyttäjien (peruskäyttäjien) näkemysten huomioimista ei tietoturvaakaan ole mahdollista kehittää kokonaisvaltaisesti. Tutkija ei ollut siinä asemassa, että hänen tehtävänään olisi ollut syyllistää mistään toiminnasta, tai tuomita ketään. Haastateltaville luvatun anonymiteetin vuoksi tutkija suoritti itse kaikkien haastattelunauhoitusten litteroinnin. Jotta jokainen haastattelutilanne muodostui mahdollisimman luontevaksi ja keskustelunomaiseksi, on haastatteluiden litteroinnissa harkinnanvaraisesti jätetty haastateltavan mainitsemia yksityiskohtia, kuten paikannimiä, järjestelmien nimiä, työvälineiden ja henkilöiden nimiä joko kokonaan litteroimatta tai muotoiltu ne tunnistamattomaksi. Haastateltavien ilmaisut on raportoinnissa muutettu kirjakielelle, jolloin mahdolliset murreilmaisut eivät yksilöi ketään haastateltavaa.

Laadullisten tutkimusten objektiivisuutta on usein kritisoitu siitä, etteivät haastattelut säily samanlaisina eikä tutkimuskohdetta tarkastella puolueettoman päältäkatsojan näkökulmasta (Eskola & Suoranta, 1998, 14). Tässä tutkimuksessa jo yksinomaan haastateltavien erilaisuus ei olisi mahdollistanut kaikkien haastatteluiden toistettavuutta täysin identtisinä. Jotta haastatteluissa kyettiin tavoittamaan edes pieni pala kunkin haastateltavan sosiaalista todellisuutta, merkitysmaailmaa, sivuttiin haastatteluissa muun muassa haastateltavien käsityksiä organisaatiokulttuurista sekä heidän näkemyksiään, miksi tiettyjä toimintatapoja on muodostunut.

5.8 Aineiston analysointi

Tutkimusaineiston analysointi vaikuttaa tutkimuksen luotettavuuteen eli reliabiliteettiin, jolla tarkoitetaan, ettei tutkimustulos ole sattumanvarainen. Tapaustutkimuksen arviointimittarina on perinteisesti pidetty triangulaatiota. (Laine, 2007, 23.) Triangulaatio sanalla tarkoittaa erityyppisten aineistojen, erilaisten teorioiden ja menetelmien tai useiden tutkijoiden käyttöä samassa tutkimuksessa (Eskola & Suoranta, 1998, 51–52; Eriksson & Koistinen, 2014, 46). Tapaustutkimuksessa on mahdollista käyttää myös erilaisia aineiston analyysimenetelmiä (Eriksson & Koistinen, 2014, 46). Tämän tutkimuksen triangulaatio muodostui aineiston analyysimenetelmien yhdistelmänä, jolloin tutkimusaineistosta oli mahdollista saada esille useita eri näkökulmia. Seuraavaksi esitellään tätä analyysimenetelmien yhdistelmää.

Eisenhardt (1989, 539–540) toteaa haastatteluaineistolle olevan tyypillistä, että keräys ja analysointi tapahtuvat rinnakkain. Koska Sykes ja Matzan neutralisoimisteoria toimi koko tutkimuksen niin sanottuna tukirankana, toimi teoria myös apuvälineenä analysoinnissa etenemisessä. Kuten jo aiemmin tässä luvussa mainittiin, sekä neutralisoimisteoria että aiemmat tutkimukset auttoivat määrittelemään tutkimuksen käsitteitä. Teorian osuus tämän tutkimuksen analyysissa liittyy neutralisoimisteorian keskeisiin olettamuksiin. Tällaisesta analyysin muodosta käytetään suomeksi nimeä teoriaohjaava tai teoriasidonnainen analyysi. Saaranen-Kauppinen ja Puusniekka (2006) selittävät, ettei teoriaohjaava (engl. *theory-driven analysis*) aineiston analyysi perustu suoraan teoriaan, vaikkakin kytkennät teoriaan on havaittavissa. Sykes ja Matzan (1957) neutralisoimisteoria keskittyi nuorisorikollisiin ja siihen, kuinka rikollinen oikeuttaa normeista poikkeavan käyttäytymisensä. Vaikka tämä tutkimus ei tutki rikollisuutta, voitiin neutralisoimisteoriasta silti tuoda käsitteitä, joita verrattiin tietoturvarikkomuksiin. Tuomi ja Sarajärvi (2018, 81–82) selittävät, kuinka teoriaohjaavassa analyysissä aikaisemman tiedon merkitys on kyllä tunnistettavissa, mutta analyysi ei silti ole teoriaa testaavaa. Pikemminkin aikaisempi tieto voi avata uusia ajatuspolkuja. Aineistolähtöisyys ja valmiit mallit vaihtelevat ajatusprosessin aikana. (Tuomi & Sarajärvi, 2018, 81–82.)

Analyysin ensimmäisessä vaiheessa haastatteluaineistoa analysoitiin yhtä aikaa aineiston keräämisen kanssa, jolloin aineistoa verrattiin teemoittelun kautta. Käytännössä tämä tarkoitti, että jo haastattelutilanteessa haastateltavan kertomaa verrattiin, ainakin osittain, taustateoriaan. Kun kaikki ensimmäisenä tutkimukseen osallistuneen organisaation haastatteluaineisto oli kerätty, haastatteluaineisto luettiin läpi useaan kertaan. Aineistosta poimittiin tietoturvakäyttäytymiseen ja tietoturvapolitiikkaan liittyviä teemoja, joita sovitettiin Sykes ja Matzan (1957) teorian keskeisiin oletuksiin sekä neutralisoimistekniikoihin. Tämä tarkastelu käydään tarkemmin läpi luvussa kuusi.

Eisenhardtin (1989) teorianmuodostusprosessissa kehotetaan luopumaan ensivaikutelmasta ja tarkastelemaan aineistoa ”monien linssien läpi”. Eisenhardt (1989, 534) viittaa Sutton ja Callahan (1987) tutkimukseen, jossa sovellettiin niin

sanottua paholaisen asianajajaa. Sutton ja Callahan (1987, 411) selittävät hyödyntäneensä teorianmuodostusprosessissaan kolmatta tutkijaa, jonka tehtävä oli havaita tutkimuksen puutteita ja auttaa paljastamaan vaihtoehtoisia oletuksia. Eli useamman tutkijan avulla tarkasteltiin, perustuvatko tulokset aineistoon, voisiko tulos muuttua vai pitäisikö tietty tulos hylätä kokonaan. Tässä tutkimuksessa tutkimusaineiston hankinnan ja analyysin suoritti yksi tutkija. Tästä syystä tämän tutkimuksen analysoinnissa tukeuduttiin osittain kilpailevien hypoteesien analyysi –menetelmää (engl. *Analysis of competing hypotheses*). Kilpailevien hypoteesien analyysi, josta käytetään myöhemmin sen lyhennettä ACH, on menetelmä, jonka tavoitteena on tutkia tai testata vaihtoehtoisia selityksiä, jolloin johtopäätöksiä kyetään harkitsemaan syvällisesti (Heuer, 1999). Tässä tutkimuksessa ACH toimi kriittisen ajattelun tukena ja tarjosi ajattelumallia aineiston ”monien linssien läpi” tarkasteluun.

Eisenhardtin (1989) teorianmuodostusprosessissa on myös tarkoitus muodostaa hypoteeseja. Eisenhardtin (1989, 541–544) kuvaamassa hypoteesin muodostusprosessissa määritellään rakenteet ja aineiston perusteella rakennetta mitataan. Hypoteesin muodostuksessa varmistetaan, että rakenteiden väliset suhteet sopivat todisteisiin. Vahvistavat suhteet tarjoavat mahdollisuuden tarkentaa ja laajentaa teoriaa.

Ihminen pyrkii usein muun muassa etsimään todisteita tai tietoja, jotka vahvistavat hänen olettamuksiaan, uskomuksiaan ja ajatuksiaan. Esimerkiksi hypoteeseihin ei tästä syystä välttämättä etsitä vaihtoehtoisia selityksiä, vaan huomio rajoitetaan tietoihin, jotka tukevat hypoteesia. (Nickerson, 1998, 177; Heuer, 1999, xxiii.) Heuerin (1999, 41) mukaan pelkkä tieto ei voi puhua itsestään. Vasta tutkijan analyysi luo tiedolle merkityksen, mutta tutkijan tulisi tiedostaa omia ennakko-oletuksiaan, koska ennakkokäsitykset ovat ratkaisevan tärkeitä päätettäessä siitä, mitä pidetään merkityksellisenä ja miten tietoja tulkitaan. Heuer (1999, 41–42) lisää vielä, että toisaalta tilanteessa, jossa tutkija pyrkisi torjumaan tai poistamaan omat subjektiiviset lähtökohtansa ja näkemyksensä, tutkimukselle annettava panos voi heikentyä. Sitä vastoin tunnistamalla omat ennakko-oletuksensa, niitä on mahdollisuus haastaa (Heuer, 1999, 41–42). Tässä tutkimuksessa omien ennakko-oletusten ja –asenteiden lähtökohta huomioitiin jo tutkimuksen alkuvaiheessa. Kuitenkaan tutkijan työkokemukseen perustuvia näkemyksiä, kokemuksia ja havaintoja ei pyritty torjumaan tai poistamaan, vaan nimenomaan haastamaan niitä. Ilman tutkijan tietoturvaan liittyvää työkokemusta, tutkimukselle annettu panos olisi mitä luultavimmin heikentynyt. Ilman kiinnostusta aihepiiriin, eli ihmettelyä siitä, miksi järkevä aikuinen ihminen toimii vastoin ohjeita, ei koko tutkimustakaan tuskin koskaan olisi edes tehty.

ACH-menetelmässä on kahdeksan vaihetta (liite 1) hypoteesien muodostamiseen tilanteessa, jossa aineiston kerääminen on jo osittain tai kokonaan suoritettu. Heuerin (1999, 103–105) mukaan ACH-menetelmän keskeinen lähtökohta on se, ettei asetettuja hypoteeseja keskitytä vahvistamaan tiedoilla, jotka tukevat kyseessä olevia hypoteeseja, vaan päinvastoin pyritään painottamaan niihin tietoihin (tai löytämään niitä tietoja), jotka heikentävät hypoteesia. (Heuer, 1999,

103–105.) ACH-menetelmässä termiä ”hypoteesi” käytetään laajassa merkityksessä, jolloin se on mahdollinen selitys tai päätelmä, jota testataan keräämällä ja esittämällä todisteita (Heuer, 1999, 32). Vaikka ACH-menetelmässä hypoteesia ei olisi johdettu aiemmasta teoriasta tai aiemmista tutkimuksista, se ei Heuerin (1999, 34–35, 42, 117) mukaan tarkoita, etteikö hypoteesia voisi johtaa teoreettisista lähtökohdista. Jokin taustateoria voi auttaa tunnistamaan muun muassa tietyn ongelman keskeisiä elementtejä, käsitteellisiä malleja, yksityiskohtia ja kehityksen suuntia. Teorian on siis oltava sovellettavissa reaalimaailman ongelmiin, ja siten abstraktikin teoria voi tarjota ajattelun työkaluja ilman ajattelua rajoittavaa luovuutta. (Heuer, 1999.) Tässä tutkimuksessa analyysin keskeisiä elementtejä on tunnistettu neutralisoimisteoriasta ja kehityksen suuntia ovat puolestaan näyttäneet aiemmat saman aihepiirin tutkimukset.

Tämän tutkimuksen lähtökohtana on monipuolistaa tietoturvatutkimusta, jonka vuoksi tutkimuksen aineiston hankinta toteutettiin aiemmista saman aihepiirin tutkimuksista poikkeavalla tavalla. Haastatteluista muodostui rikas, monipuolinen tekstiaineisto, joka jakaminen ja rajaaminen määrällisesti mitattavaan muotoon olisi mitä luultavimmin rajannut myös ilmiöstä löydettyjä havaintoja. Tämä tutkimus sisältää lukuisia käsitteitä, joten ACH auttoi hahmottamaan eri käsitteiden välistä yhteyttä. Samalla se tarjosi järjestelmällisen tavan tutkia hypoteeseja sekä palautti tarkastelemaan asetettuja väitteitä uudelleen ja tarkastelemaan erilaisia vaihtoehtoja.

6 NEUTRALISOIMISTEORIAN TULKINTA TIETOTURVAKONTEKSTISSA

Tässä luvussa neutralisoimisteoriaa, sen keskeisiä oletuksia sekä neutralisoimistekniikoita tarkastellaan tietoturvan näkökulmasta. Alkuperäisen neutralisoimisteorian sisältö käsitteli (nuoriso)rikollisuutta, joten kaikkia teoriassa esiteltyjä oletuksia ei täysin sellaisenaan ole mahdollista siirtää tietoturvakontekstiin. Tämän tutkimuksen keskeisenä oletuksena on, etteivät yksittäiset neutralisoimistekniikat välttämättä itsessään selitä toimintaan ryhtymisen syitä. Koska Sykes ja Matzan teorian neutralisoimistekniikat muodostavat keskeisen sisällön koko teoriasta, keskitytään tässä luvussa vertaamaan eri neutralisoimistekniikoita tietoturvakontekstissa. Samalla luvussa tarkastellaan myös sitä, liittyykö tietoturvaan uskomusten/asenteiden ja käyttäytymisen välistä ristiriitaa samaan tapaan kuin Sykes ja Matzan teoriassa. Pääluvun loppuosa keskittyy tietoturvarikkomusten selontekoihin. Koska tutkimusaineiston analysoinnissa eri organisaatioista koottu aineisto analysoitiin erillään, on tässä kohtaa selvyyden vuoksi mainittava, että myös haastateltavien ilmaisuissa käytetään tätä jaottelua. Toisesta organisaatiosta käytetään siten ilmaisua vertailuorganisaatio.

6.1 Yhdenmukaisuuden vaatimus

Sykes ja Matzan (1957, 665) väitteen mukaan (nuoriso)rikollinen on ainakin osittain sitoutunut yhteiskuntaan eikä yksilö ole täysin immuuni yhdenmukaisuuden (engl. *conformity*) vaatimukselle. Yhdenmukaisuudella viitataan käyttäytymiseen tai käyttäytymisen muutoksen siten, että toiminta sovitetaan yhteen toisten ihmisten kanssa (Cialdini & Goldstein, 2004, 606). Tutkimusaineistona käytettyjen dokumenttien perusteella tietoturva koskee jokaista organisaation järjestelmiin ja laitteisiin käyttöoikeuden omaavaa henkilöä. Vaatimus tarkoittaa, että tietoturvapolitiikan mukaiset ohjeet, säännöt, määräykset, kiellot ja käskyt koskevat kattavasti koko henkilöstöä. Tietoturvaan voidaan siten olettaa liittyvän organisaatioiden asettama yhdenmukaisuuden vaatimus.

Tietoturvakontekstissa neutralisointiprosessin sosiaalista osuutta tarkastellaan tässä tutkimuksessa työntekijän organisaatioon sitoutumisen kautta. Sitoutumisesta muodostettiin ensin hypoteeseja ja tutkimusaineiston analyysin avulla etsittiin viittauksia (osoittimia), kuinka työntekijät kuvailivat sitoutumistaan organisaatioon ja sen toimintatapoihin. Jotta voidaan tarkastella, mikä merkitys tietoturvapolitiikalla työntekijälle on, on tutkimusaineistosta tarkasteltu myös sitä, miten hyvin tietoturvapolitiikka ohjeineen tunnetaan. Eli tietääkö ja ymmärtääkö työntekijä edellä mainitun yhdenmukaisuuden tavoitteen sekä sen, mihin hän on sitoutunut?

6.1.1 Sitoutuminen

Yksi tämän tutkimuksen olettamuksista on, että työhönsä sitoutuneelle työntekijälle työ tarjoaa myös rahallista korvausta (tai etuja) arvokkaampia elementtejä, kuten merkityksellisen ja kiinnostavan työn tai mahdollisuuden omien kykyjensä käyttämiseen. Myöskään työstä saatavaa arvostusta ei voi unohtaa. Toisaalta sitoutumiseen voi liittyä rationaalisen sitoutumisen lisäksi myös tunnepohjaista sitoutumista, kuten yhteinen arvomaailma tai yksilön identiteetin rakentuminen voi nojautua osittain organisaatioon.

Organisaatioon sitoutumiseen vaikuttavat tekijät eivät ole suoraviivaisen yksiselitteisiä, joten tässä tutkimuksessa aineiston analysoinnissa on tukeuduttu Allen ja Meyer (1990, 3) määrittelemään kolmen komponentin malliin, jonka osia ovat affektiivinen (engl. *affective component*), jatkuva (laskelmoiva) (engl. *continuance component*) ja normatiivinen (engl. *normative component*) sitoutuminen. Lisäksi tarkastelussa huomioidaan myös Steersin (1977) esittämiä sitoutumiseen vaikuttavia tekijöitä. Steers (1977, 47) jakaa organisaatioon sitoutumisen tekijät kolmenlaisiin asioihin, joita ovat henkilökohtaiset ominaisuudet (saavutusten tarpeet, ikä ja koulutus), työn ominaisuudet (tehtävän identiteetti, omavalintaisuus, vuorovaikutus, työstä saatava palaute) ja työkokemus (ryhmän asenteet, organisaation luotettavuus ja henkilökohtainen tärkeys). On siis oletettavaa, että työntekijöillä, jotka ovat vahvasti organisaation tavoitteisiin sitoutuneita, heillä on todennäköisesti myös vahva halu työskennellä organisaatiossa ja edistää sen tavoitteiden saavuttamista.

Allen ja Meyersin (1990, 2) mukaan työntekijät, joiden sitoutuminen on voimakkaasti affektiivinen, pysyvät organisaatiossa, koska he *haluavat* pysyä sen jäseninä. Heidän sitoutumisensa on tunnepohjainen ja he nauttivat organisaation jäsenyydestä, hyväksyvät organisaation arvot ja samaistuvat niihin. Allen ja Meyersin (1990, 4) mukaan vahva jatkuva (laskelmoiva) organisaatioon sitoutuminen viittaa tilanteeseen, jossa työntekijä pysyy organisaatiossa, koska hänellä on taloudellinen tai muu "*pakottava*" tarve. Työntekijä ikään kuin laskee sijoituksensa tuottavuutta, tai sitä, millaisia kustannukset olisivat, mikäli hän lähtisi organisaatiosta. Jos työntekijä kokee sijoittaneensa paljon aikaa ja energiaa hallitakseen tiettyjä työtaitoja, joita ei kuitenkaan voisi helposti siirtää muihin organisaatioihin, työllisyysvaihtoehtojen puute voi saada hänet jäämään organisaatioon. Meyerin ja Allen (1997, 25) mukaan voimakas normatiivinen sitoutuminen puolestaan pohjautuu vastuullisuuden ja *velvollisuuden* tunteisiin. Tällaiset tunteet

motivoivat yleensä yksilöitä käyttäytymään asianmukaisesti ja toimimaan siten, mikä on organisaation kannalta soveliasta ja asiaankuuluvaa. Meyerin ja Allen (1997, 25) kuitenkin jatkavat, ettei normatiiviseen sitoutumiseen liity samankaltaista innostusta ja osallistumista kuin affektiiviseen sitoutumiseen. Työntekijät, jotka pysyvät organisaatiossa pääasiassa vahvan normatiivisen sitoutumisen vuoksi, saattavat vastustaa velvoitteitaan, ja vaikka tämä vastustus ei estä heitä suorittamasta tehtäviään, se voi vaikuttaa siihen, kuinka vapaaehtoisesti tai vastahakoisesti he tehtävänsä suorittavat. Jyrkältä vaikuttavasta rajauksesta huolimatta, Meyer ja Allen (1997, 13) selittävät, ettei työntekijän suhde organisaatioon välttämättä heijastele vain yhtä komponenttia, vaan eriasteisesti kaikkia kolmea. Työntekijä voi siten aidosti nauttia työskentelystään organisaatiossa, mutta myöntää taloudellisen näkökulman organisaatiossa pysymiseen.

Haastateltavat olivat työskennelleet organisaatiossa useita vuosia, osa jopa vuosikymmeniä. Haastateltavat mainitsivat työsuhteiden pituudesta muun muassa seuraavasti:

> ”Puhun koko työhistoriastani, koska olen ollut [paikan nimi] ja sitä kautta käsitellyt luottamuksellista tietoa, kun elettiin sitä aikaa, ettei ollut sitä tietotekniikkaa laajasti, vaan pelattiin papereilla.”

> ”Olen ollut 15 vuotta tässä organisaatiossa.”

> ”...kun on kuitenkin tehnyt tätä työtä jo 20 vuotta.”

Vaikka haastateltavat eivät ilmaisseetkaan suoranaista halukkuutta huomattaviin ponnistuksiin organisaation puolesta, voidaan haastateltavien kertomat pitkät työsuhteet tulkita vähintäänkin kohtalaisena haluna pysyä organisaation jäsenenä sekä sitoutuneisuudesta organisaation tavoitteisiin. Vaikka pitkä työsuhde voi kertoa myös yksilön mukavuudenhalusta, on silti oletettavaa, että työ organisaatiossa on koettu niin mielekkäänä, etteivät henkilöt olleet (haastattelu hetkeen mennessä) irtisanoutuneet tehtävästään.

Olisi epäuskottavaa edes olettaa, etteivät pitkään samassa organisaatiossa työskennelleet myös kritisoisi organisaation toimintaa. Haastateltavat mainitsivat:

> ”Mutta kun nyt on menty siihen, että osa organisaation toiminnoista on myyty ulkopuolisille ja sen jälkeen, kun ne on myyty ulkopuolisille, se kenelle ne on myyty, on pilkkonut oman yhtiönsä ja myynyt ne edelleen ulkopuoliselle, jolloin ei enää ole tosi asiallista tietoa, missä ihan oikeasti mennään. Ja silloin tullaan tähän kaupallisuuteen. [instanssin nimi] on halunnut näin, että yrityksiä myydään, mutta se tietoturva unohdetaan niistä täysin.”

> ”Koska palvelut ulkoistetaan, ei ole sitä lähitukea, niin käyttäjällehän jää väistämättä sitten enemmän kaikenlaista pientä juttua, mitä sen pitää hanskata ja pitää ymmärtää muuttaa joitain polkuja ja mitä niitä nyt onkaan. Niin se tietoturva on vaan yksi siellä niitten kaikkien joukossa.”

> ”Sopimuksessa lukee, että ne saa olla tietyn verran pois käytöstä ja sitten se todellakin on näin.”

> ”En usko, että meidän organisaatio on varsinkaan vielä tajunnut sitä, kuinka paljon nämä ovat menneet eteenpäin nämä tietojärjestelmät, ja kaikkihan nykyään tehdään tietojärjestelmillä. Tämä on vain minun oma näkemys.”

Se, etteivät tutkimukseen osallistuneen organisaation työntekijöiden sitoutumista kuvaavat näkemykset olleet täysin yhteneväisiä, ei kuitenkaan antanut ymmärtää, ettei muun muassa organisaation toiminnan turvaaminen tai muu organisaation olemassa oloon liittyvä merkitsisi riittävästi motivoimaan työskentelyä organisaatiossa. On toki mahdollista, että haastateltavat olisivat kertoneet motivaatiostaan toisin, jos tutkimuksen pääasiallisena tarkoituksena olisi ollut organisaation sitoutumiseen suuntaava tutkimus. Kokemusten ja näkemysten erilaisuutta ei pidä kuitenkaan nähdä negatiivisena asiana. Liiallinen näkemysten yhteneväisyys ei välttämättä pitkällä tähtäimellä toimisi edes organisaation tavoitteiden saavuttamisessa. Haastatteluista saa kaiken kaikkiaan vaikutelman, että työntekijöiden sitoutumisaste työhönsä organisaatiossa on varsin korkea. Se, että tutkimukseen osallistuneet organisaatiot ovat julkisen sektorin organisaatiota, merkitsee samalla sitä, että Suomessa julkisen sektorin organisaatiot eivät pysty kilpailemaan palkoissa yksityisen sektorin kanssa, vaan sitoutumiseen vaaditaan muitakin tekijöitä. Kuten eräs vertailuorganisaation haastateltavista mainitsi:

> ”Palkka ei niin suuri tässä talossa ole, vaikka kuinka ylitöitä tekisi, että rahan takia tekisi. Jos rahan takia tekisin, olisin jo vuosia sitten lähtenyt kävelemään.”

Vertailuorganisaatiossa sitoutuneisuus ei kuitenkaan välttämättä kohdistunut suoraan organisaatioon itsessään, kuten eräs haastateltava muotoilee:

> ”No en koe, että minulla olisi varsinaisesti mitään velvollisuuksia tätä organisaatiota kohtaan, se on vain työnantaja, vaan se on enemmän Suomelle hyödyllistä. Altruismi on tässä ehkä vähän liikaa sanoa, mutta näen, että muille tästä on enemmän hyötyä, että edes yritän vähän. Jos olisi jostain muusta järjestelmästä kyse, niin en tiedä, kiinnostaisiko minua oikeestaan ollenkaan.”

6.1.2 Tietoturvapolitiikan merkitys

Tietoturvapolitiikan tarkoituksena on ohjata ja tukea organisaation tietoturvaan asetettuja tavoitteita. Tietoturvatietoisuuteen puolestaan liittyy työntekijän tietämys näistä tavoitteista. Kuinka hyvin työntekijä sitten on selvillä näistä tietoturvapolitiikan asettamista tavoitteista?

Haastatteluiden mukaan organisaatioissa järjestetään sekä pakollista että vapaaehtoista tietoturvakoulutusta. Lisäksi molemmissa organisaatioissa koko henkilöstön on kyettävä kirjallisella dokumentaatiolla osoittamaan henkilökohtainen, organisaation asettama, riittävän hyvä tietoturvatietoisuuden taso. Haastateltavien tehtävänkuvat organisaatioissa olivat erilaisia, joten jokaisen kanssa keskusteltiin, miten hyvin haastateltava arvio tuntevansa oman organisaation

tietoturvapolitiikan ja siihen liittyviä ohjeita. Haastateltavien ilmaisut eivät suoraan kertoneet heidän tutustuneen varsinaiseen organisaation tietoturvapolitiikan dokumentaatioon, ainakaan kokonaisuudessaan. Käsitteenä sana ”tietoturvapolitiikka” ei haastatteluissa merkinnyt täysin yhtäläistä asiaa. Haastateltavat mainitsivat muun muassa:

> ”Varmasti olen lukenut siihen liittyviä määräyksiä, mutta en syvällisesti, koska se ei kuulu suoraan minun toimialaani. Kyllä minä ne perusasiat olen käyny läpi, mitä pitää käydä läpi.”

> ”Pätkiä olen lukenut, mutten kannesta kanteen.”

Vertailuorganisaation haastateltaville organisaation tietoturvapolitiikka ei ollut täysin tuttu ja haastateltavat mainitsivatkin muun muassa näin:

> ”En tunne oikeestaan ollenkaan. Olen minä kyllä siitä kuullut, että on niitä jotain tiettyjä linjauksia, mutta en ole koskaan missään ikinä nähnyt virallista dokumenttia, mitä voisi selata läpi.”

> ”Aika huonosti. En usko, että olen sitä koskaan edes nähnyt. Olen kyllä tehnyt ne kaksi testiä.”

Osa haastateltavista rinnasti tietoturvapolitiikan tuntemuksen organisaation niin sanotun tietoturvatestin suorittamiseen. Eräs haastateltava selitti:

> ”Aika hyvin mielestäni. Ei tästä nyt niin hirveen kauaa ole, kun tein sen tietoturvajutun. Se on tavallaan tietoturvan verkkokurssi, joka pitää suorittaa ja siinä käydään dokumentteja läpi ja siihen on tentti päälle.”

Se, ettei yksittäinen käsite tarkoita samaa asiaa, ei vaikuttanut tarkoittavan, etteivätkö haastateltavat silti olisi kokeneet ymmärtävänsä, mitä tietoturva organisaation toiminnalle merkitsee. Organisaatioiden tietoturvatesti toimii myös ikään kuin valvontaan liittyvänä elementtinä, ja vaikka testin yksityiskohtaisesta sisällöstä ei haastatteluissa keskusteltu, toivat haastateltavat sekä myönteisiä että kielteisiä ajatuksia siitä, miten testi osoittaa tietoturvan tärkeyden ja miten työntekijät voivat hahmottaa testin avulla tietoturvaan liittyviä tavoitteita.

> ”Mutta se niissä testeissä häiritsi, että joissakin kysyttiin, että mitä ymmärretään tällä ja tällä politiikalla tai systeemillä, se oli siis joku termi, jota nyt en muista ulkoa, niin haettiin minun mielestäni liikaa tällaista teoriaa. Miksi pitää tietää tämmösiä teorioita normaalin käyttäjän, kun se fokus pitäsi olla juuri siinä ihan käytännön klikkailussa.”

> ”Helposti ymmärrettävä, mutta ei liity omaan työtehtävääni ehkä kovin paljoa. Se oli mielestäni itsestään selvää. Olisin selvinnyt siitä testistä lukematta niitä alustuksia ja menemällä suoraan tekemään sen tehtäväosion.”

> ”En koe testiä kuormittavana tai epämielekkäänä, mutta haasteellisempia ne saisi olla ja nimenomaan laajentaa sitä näkökulmaa myös sinne henkilökohtaiseenkin elämään, koska minä voin tehdä sielläkin tietoturvarikkeen, joka voisi vaikuttaa, vaikken tekisi sitä organisaation nimissä. Voisi ajatella

ehkä jotain muuta, kuin että luet dokumentin ja vastaat joihinkin monivalintakysymyksiin. Se ei välttämättä ole nykypäivänä se tehokkain tapa oppia."

Vertailuorganisaatiossakin kaikki haastateltavat olivat suorittaneet oman organisaationsa pakollisen niin sanotun tietoturvatestin, mutta eivät kokeneet, että se olisi suoranaisesti lisännyt tietoturvatietoisuutta. Kuten haastateltavat mainitsivat:

"Se testi ei lisännyt tietoturvatietoisuutta. Se oli sellaista pakkopullakertausta."

"Ei missään nimessä. Se on niin ympäripyöreä. Hyvä, että edes sellainen on, mutta olisi kiva, kun olisi jotain parempaa."

Myönteisenä haastateltavat kokivat sen, että tietoturvatesti oli niin sanotulla maalaisjärjellä tehtävissä. Huolimatta siitä, että tietoturvaan liittyvä opiskelumateriaali oli haastateltaville tuttua, ja niin sanottu tietoturvatesti pakollinen osa organisaation tietoturvakoulutusta, suhtautuminen siihen oli kuitenkin pääasiassa myönteistä. Haastateltavien ilmaisut voisivat kuvastaa sitä, että haastateltavat olisivat sisäistäneet tietoturvan merkityksen vähintäänkin riittävän hyvälle tasolle. Vai voisivatko sittenkään? Miten määritellä riittävän hyvä taso organisaation tietoturvaan liittyvien tavoitteiden saavuttamiseksi? Vaikka ymmärtää "mitä", se ei välttämättä tarkoita, että ymmärtää "miksi" ja "miten".

Eräs haastateltava kuvailee:

"Vaikka on käynyt sen tietoturvatestin, tietää pintaraapaisun, mutta ei tiedä sitä kokonaisuutta, miten se pelaa. Ja mitä enemmän tiedät asioista, ja mitä enemmän tiedät kokonaisuutta, sen enemmän ymmärrät niistä ja osaat toimia oikein. Se, että saat tunnin tai kaksi tietoturvakoulutusta, niin paljonko se auttaa? Sinulle vaan annetaan pelisäännöt, toimia näin, näin ja näin, ja se ei yksinkertaisesti nykypäivänä riitä noihin järjestelmiin. Minkä vuoksi sitten tarvitsee käydä kouluja monta vuotta, että olet atk-nikkari? Eikös sen pitäsi riittää, että sinulla on reipasta mieltä ja tietokone, niin sinähän osaat sen jo!?

Ja sitä kautta tulee sitä tietoturvatietous? Höpö höpö. Ei sillä oo mitään tekemistä sen kanssa, vaan se vaatii pitkäjänteistä koulutusta. Se on yksi työkalu, mitä pitää kouluttaa, mutta kun siihen ei ole työnantajilla aikaa ja sen takia tapahtuu kaikennäköisiä."

Haastateltavien ilmaisut "määräykset" ja "pelisäännöt" kertovat, että tietoturvapolitiikan voidaan tulkita ainakin pyrkivän ohjaamaan tietoturvakäyttäytymistä. Vaikkei haastatteluissa mainittu testi voisikaan suoraan mitata, miten hyvin tietoturvaan liittyvät tavoitteet ymmärretään, mainitsee eräs haastateltava kuitenkin:

"Se välitön palaute käyttäjälle, ja malli, miten tulee toimia, se on mielestäni ihan toimiva."

Vaikka ilmaisu ”ei kuulu minun toimialaani” voisi jossain yhteydessä tarkoittaa välinpitämättömyyttä, tässä yhteydessä haastateltavan kuvaus kertoi pikemminkin siitä, että organisaatiossa on taho, jossa tietoturvapolitiikkaan liittyvät ohjeet, määräykset ja säännöt laaditaan. Kuten eräs haastateltava mainitseekin:

> ”...koska joku niitä kirjottaessaan ei voi tietää kaikkia tilanteita...”

Tietoturvan pelisääntöjä ei luoda yhdessä, vaan ne annetaan työntekijälle. Tietoturvapolitiikka on siis kirjallinen dokumentti tai kokoelma erilaisia tietoturvaan liittyviä dokumentteja. Haastateltavat kuvailivat tietoturvaan liittyvää dokumentaatiota:

> ”Työnantajan taholtahan tulee ohjeita ja infoa tästä tietoturvasta, miten pitää käyttäytyä, niin niitähän tulee paperikaupalla. Eri asia on sitten se, miten ihmiset niihin megalomaanisiin pumaskoihin viitsii ja jaksaa perehtyä ja käytetäänkö niissä sellaista terminologiaa, että normaali käyttäjä väsyy lukemaan sitä, että se meni vähän niinkuin täältä.” (haastateltava heilautti kättään päälaen yli)

> ”Pystyn kyllä ne omiin työtehtäviin liittämään, mutta kun ne tehdään ikään kuin asiakirjamuodossa, niin siitä se ei aukea se asia. Ne pitäsi olla enemmän sellaisia ihan peruskäyttäjälle olevia ohjeistuksia. Referoida se ehkä jollain lailla, eli jalkauttaa se kapulakieli.”

> ”Siis kaiken maailman ohjeitahan tulee ihan älyttömästi, mutta onko se tietoturvaohje sen paremmin sisäistetty kuin mikä tahansa muu ohje, niin en osaa sanoa sitä.”

> Haastateltava kertoo uuden järjestelmän käyttööotosta: ”Ja tässä on sitten sekin kääntöpuoli, että vaikka se olisikin valmis se järjestelmä, niin siellä on niin valtavasti tietoa, että miten löydät sen sieltä sitten, että miten se on järjestetty. Ainakin nyt tuntuu sille, miten se oli vanhassakin, että se on sellanen hornan kattila, että löydänkö minä sen ”tietopankista” vai mistä minä löydän sen.”

Myöskään vertailuorganisaatiossa tietoturvapolitiikan dokumentaatio ei käsitteenä vaikuttanut olevan täysin tuttu eikä siten vaikuttanut välttämättä palvelevan tarkoitustaan täysin. Haastateltavat kuvailevat muun muassa näin:

> ”Täällähän ei ole ikinä ollut sellaista niin kuin itse koen sen, että on sellainen julkinen dokumentti ja sen lisäksi on paksu opus, missä on kaikki ne jutut, että tehdään juuri näin ja kaikki ohjeet, miten ne menevät. Ja se ei ole julkinen. Mutta täällä ei ikinä ole minun mielestä ollut sellaista. Puhun nyt vähän menneisyydestä, mutta ei minun mielestä ole ollut sellaista, minkä kokisin tietoturvapolitiikaksi ja tietoturvaohjeistukseksi.”

> ”Siis oletan, että sellainen tietoturvapolitiikka on olemassa, mutta en minä tiedä onko. Tiedän vaan niitä vaatimuksia, mitä tietyillä palveluilla on tietoturvan suhteen.”

> ”Intrasta on vaikea löytää jonkin toimintatavan tai tiedon ajantasaisuutta. Jonkin tiedon tai toimintatavan voimassaoloaikaa ei näy, eikä voi siten tietää, mikä on hyväksyttyä, eikä ole selvää, koskeeko jokin asia kaikkia.”

Molemmissa tutkimukseen osallistuneissa organisaatioissa työntekijöiden sitoutumisaste työhönsä organisaatiossa vaikuttaisi olevan varsin korkea. Organisaatioiden tietoturvapolitiikka ohjeineen ei välttämättä haastateltavien kertomana vaikuttanut suoranaisesti sitouttavan heitä organisaation tietoturvan tavoitteisiin eikä siten välttämättä toimivan yhdenmukaisuutta edistävänä.

6.2 Asenne

Sykes ja Matza (1957, 664–665) esittivät neljä väitettä, jotka esiteltiin luvussa kaksi. Vaikka kaikki neljä väitettä eivät täysin istu tietoturvakontekstiin, mahdollisti haastatteluiden keskustelunomaisuus sen, että haastatteluista saattoi tarkastella haastateltavien tietoturvaa kohtaan liittyvää asennetta sekä hahmottaa sitä, miten työntekijät tietoturvan kokivat.

Tietoturvan merkittävyydestä haastateltavat kuvailivat muun muassa näin:

> ”Erittäin tärkeänä. Kyllä se on niin kuin itsestäänselvyys.”

> ”Onhan se tietyissä asioissa koko ajan läsnä, että sen joutuu ottamaan huomioon.”

> ”Se tietoturvatietämys niistä vaatimuksista ja ohjeistusta tulee niin monelta eri taholta, eli henkilölle tulee niin paljon syötteitä siitä, että organisaatio ottaa tietoturvallisuuden huomioon.”

> ”Minulle kaikki tietoturva-asiat ovat selkeitä, mutta sellaiselle henkilölle, joka ei ole niin perehtynyt, ne voivat olla hankalia.”

> ”Minä veikkaan, että se pulju, missä olen, niin se asenne on aika hyvä. Mutta kun mennään alaspäin, niin tietysti käyttöoikeudet ja käyttötasot on matalampia, kun mennään tavallaan ruohojuuritasolle ja siellä on nuorempaa porukkaa, niin se asenne ei välttämättä ole sillä tasolla kuin mitä se on esim täällä missä olen töissä. Uskon, että valtaosa porukasta on omaksunut sen tietoturvan tärkeyden.”

> ”Meillä on aika pitkä perinne tietoturvasta, jo ennen tietojärjestelmiä.”

> ”Se on tärkeää. Puhun koko työhistoriastani, koska olen työssäni käsitellyt myös ihmisten terveystietoja yms, kun elettiin sitä aikaa, että ei ollut sitä atk:ta laajasti, niin kyllä minä näen, että se tietoturva on hyvin tärkeätä.”

Myös vertailuorganisaatiossa tietoturva koettiin tärkeäksi:

> ”Tietoturva on todella tärkeä. Se on tavallaan iso osa siinä mielessä, että työskentelee vähän niin kuin sillä alalla ja sen lisäksi, miten itse hoitaa asioita ja työskentelee, niin se on kumpaankin tosi tärkeetä.”

Jos tietoturva, sen merkitys sekä suhtautuminen siihen on tärkeää, voidaan kysyä, mistä tuota asennetta ja tietämystä sitten ammennetaan, koska organisaa-

tioiden tietoturvapolitiikan dokumentaatio ei haastateltavien kertomana vaikuttanut täysin ohjaavan ja tukevan tietoturvan toteutusta. Haastateltavat mainitsivat omaksuneensa tietoa organisaation intrasta löytyvistä kehotuksista valppauteen (heads-up ilmoitukset), organisaation sisäisistä tapahtumista, itseoppimalla sekä yleisestä uutisoinnista.

Vertailuorganisaatiossa tietoturvatietoisuus oli haastatteluiden perusteella omaksuttu muun muassa aikaisemman työhistorian ja opintojen myötä organisaation ulkopuolelta. Eräs haasteltava kertoo:

> ”Ulkopuolelta. Ei todellakaan sisäpuolelta. Olen yrittänyt tuoda sitä ulkoa sisälle, mutta hyvin rajallisesti kuitenkin, että se on ollu sellasta, että tehdään tällaisia ja tehdään estoja ja rajauksia, mutta ei niitä ole mihinkään kirjattu, että nämä ovat talon linjauksen mukaisia. Että oman perstuntuman kautta tehdään. ”

Sykes ja Matza (1957, 665) toisen väitteen mukaan nuorisorikollinen saattaa tuntea arvostusta ja kunnioituksensa lainkuuliasta henkilöä kohtaan, ja kykenee siten itse tuntemaan paheksuntaa laitonta toimintaa kohtaan. Vaikka haastatteluiden perusteella ei voinut päätellä, että tietoturvaohjeita noudattavia kohtaan osoitettaisiin suoranaista arvostusta tai kunnioitusta, kuvastivat haastateltavien ilmaisut jonkinasteista, jos nyt ei suoranaista paheksuntaa, niin kritiikkiä kuitenkin.

> ”Kun henkilö kokee olevansa riittävän korkeassa asemassa, hän oikeuttaa itsensä tekemään asioita eri tavalla kuin muut ja helpommin. Se on jännä, että joku haluaisi oikeuttaa itselleen, ettei hänen tarvitse näitä ja näitä noudattaa ihan vaan sen takia, että on täällä riittävän ylhäällä.”

> ”Mutta loppupelissä koko organisaation ylin johto vastaa tietoturvatietoisuudesta. Joten myös siellä päässä se tietoturvallisuuden taso ei välttämättä ole niin hyvällä mallilla kuin se pitäisi olla.”

> ”Alkaa olla jo klisee se johdon sitoutuminen turvallisuuteen.”

> ”Mutta kun mennään johdossa ylöspäin, niin se ymmärrys on, etteivät he välttämättä tiedä, että heidänkin pitäsi käydä niitä kursseja. He vetoavat siihen, ettei tunnu siltä, että pitäisi mennä istumaan niihin, vaikka niiden pitäisi mennä.”

Vaikka asenne olisi hyvä ja tietoturvakin koettaisiin tärkeänä, silti haastatteluissa toistuvat ilmaisut viittasivat siihen, ettei tietoturvaan liittyviä ”miksi” ja ”miten” ymmärretä täysin yhtäläisesti. Seuraavassa alaluvussa keskitytään tarkemmin tähän aiheeseen.

6.3 Perustelu

Jos tarkastellaan tietoturvaa suhteessa Sykes ja Matzan teoriaan, siitä on löydettävissä yhtäläisyyksiä, kuten muun muassa se, että tietoturvakulttuuri heijastelee

organisaatiokulttuuria, eli ei ole olemassa vahvasti erillisiä alakulttuureita. Mitä eroa sitten on rikollisessa ja työntekijässä? Ei välttämättä mitään. Kumpikin voi yhtä lailla oppia vastuun väistelyä. Sanotaanhan, että joka tahtoo, löytää keinot, se joka ei tahdo, löytää selitykset.

Sykes ja Matza (1957, 667) mainitsevat: "*It is by learning these techniques that the juvenile becomes delinquent, rather than by learning moral imperatives, values or attitudes standing in direct contradiction to those of the dominant society*." Kuitenkaan Sykes ja Matza eivät teoriassaan tuo selkeästi esille sitä, missä nuo poikkeavan käyttäytymisen mahdollistamat neutralisoimistekniikat opitaan, eli miten poikkeavuuden oikeutus toimii rikollisuuden mahdollistajana.

Seuraavaksi käydään läpi neutralisoimisteorian niin sanottu opintosisältö, eli neutralisoimistekniikat, sekä verrataan niitä tietoturvakontekstissa. Voisiko organisaatio itse tarjota valmiita selitystapoja? Eli vaikka organisaation tietoturvapolitiikka ei haluaisi suosia tietoturvarikkomuksia, se siltikin tahattomasti tarjoaisi siihen sopivia selitystapoja? Entä voisiko tietoturvapolitiikka jopa heikentämään työntekijän motivaatiota noudattaa sitä?

6.3.1 Vastuun kieltäminen *("En tarkoittanut sitä")*

Aiemmissa tietoturvatutkimuksissa Sykes ja Matza (1957) teorian vastuun kieltäminen –neutralisoimistekniikkaa on mitattu väitteillä, ettei työntekijä ymmärrä tietoturvapolitiikkaa tai ole varma sen sisällöstä (Cheng ym., 2014; Siponen & Vance, 2010, A1). Mittauskohteina ovat myös olleet päivittäisten työtehtävien epäselvyys ja liiallinen työstressi (Li & Cheng, 2013).

Sykes ja Matza (1957) puolestaan viittasivat teoriassaan siihen, kuinka rikollinen väittää tai kokee olevansa ikään kuin olosuhteiden uhri tai vallitsevan ympäristön tuote.

Haastateltavat käyttivät ilmaisuja ”peruskäyttäjä”, ”normaalikäyttäjä” ja ”loppukäyttäjä”. Jo nuo ilmaisut kuvastavat sitä, ettei suurin osa organisaation työntekijöistä kehitä tai hallinnoi erilaisia järjestelmiä. Se, etteivät työntekijät voi vaikuttaa siihen, millaisia teknisiä tietoturvaratkaisuja organisaatioissa käytetään, tai miten tietoturvapolitiikka ohjeineen on laadittu, voi varmastikin saada yksilön kokemaan itsensä ikään kuin olosuhteiden uhriksi, joka ajelehtii räätälöidyistä virheilmoituksista tai yhteysongelmista aina seuraavaan, tai etsii tietoa tietämättä, mistä sitä etsii, ja tiedon löydettyään, se ei sittenkään vastaa sitä, mihin hän tietoa olisi tarvinnut.

Haastateltavat havainnollistivat esimerkkien kautta räätälöityjä virheilmoituksia ja muita ongelmia:

> ”Että oven saranat ei toimi tai ovi on takalukossa, että sehän se on se ongelma. Ja se tuli tässä nyt, kun tuli joku päivitys, niin se meni vähän pieleen ja minä olen sen nyt kolme kertaa nollauttanut sen salasanan ja nyt sieltä tuli, että sinne pitäisi kirjautua riittävän monta kertaa väärin ja että se blokkaa sen koko systeemin pois ja sitten mennä taas mistä lie lataamaan sen uudelleen.”

> ”Kun tuli joku järjestelmäpäivitys ja nyt se ei toimi, tai siis toimii aina kun nollaa sen salasanan, pääsen siihen uudelleen, kun syötän siihen salasanan,

mutta kun kirjaudun ulos, niin se ei enää muista sitä salasanaa, vaikka se on ihan varmasti oikein."

"Osassa meidän laitteista se on ominaisuus, että se kaatuu, mutta osassa jos käyttäjä ei tule oikeilla stepeillä siitä laitteesta ulos ja sitten kun seuraava käyttäjä menee siihen, se kaatuu sen takia."

"Ei voida tehdä mitään. Jos ollaan organisaation tietokannoissa, niin odotetaan niin kauan, että homma pelaa, paiskotaan laitteita ja koputellaan niitä."

"Jos ajattelee esim toimenpidettä, että sinulla on järjestelmä auki ja siirrät sieltä yhden tiedoston toiseen paikkaan, siinä menee aikaa joitakin sekunteja, mutta jos sinulla menee siihen aikaa esim kolme tuntia, kun yrität erehdyksen kautta, että ei mene, ei mene, koitat kaikki vaihtoehdot, sammutat, käynnistät uudelleen ja tällaisen prosessin kautta, niin jossakin vaiheessa ihminen turhautuu, että ei tästä tule mitään."

"Jos sanon, että missä tehdään tietoturvarikkeitä, niin se on yksinkertaisesti paikoissa, joissa ei ole muuta tapaa toimia."

Edellä kerrotut ikään kuin räätälöidyt virheilmoitukset tai ongelmatilanteet voivat hyvinkin todennäköisesti aiheuttaa työntekijälle tunteen, että hän ajelehtii olosuhteiden uhrina tietoteknisestä ongelmasta toiseen ymmärtämättä, tai edes haluamatta ymmärtää, miksi asentaa, käynnistää, säätää tai asettaa käyttäjätuen tai ohjeen antamia määrityksiä. Työntekijä ei välttämättä aidosti ymmärrä, miksi juuri hän sai räätälöidyn virheen, vaikka asennusohje on yhtäläinen kaikille käyttäjälle. Vaikka työntekijä saattaa itse omalla toiminnallaan aiheuttaa laitteen tai ohjelman toimimattomuuden, aiheuttaa tietoturvarikkomuksen tai vaarantaa tietoturvaa, hänen päällimmäinen tunne ei ole syyllisyys ja häpeä, vaan enemmänkin eri asteinen ärtymys.

Kuten luvussa viisi mainittiin, haastateltavien kanssa keskusteltiin tietoturvaan liittyvistä arkipäiväisistä teemoista, joista yhtenä teemana oli salasanakäytänteet. Tässä kohtaa on mainittava, että erilaisista tietoverkkoratkaisuista ja erilaisiin käyttöympäristöihin tarkoitetuista tietojärjestelmistä johtuen työntekijällä saattaa olla päivittäisessä käytössään jopa 20 salasanaa, tai salasanan ja pin-koodin yhdistelmää. Tietoturvapolitiikan mukaisesti, osassa järjestelmiä vaaditaan yli 16 merkkiä pitkiä salasanoja. Salasanojen tulee olla vahvoja ja eri järjestelmissä tulee käyttää erilaisia salasanoja.

Se, että yksilö kieltää tietoturvan yhteydessä vastuun eikä siten koe olevansa vastuussa siitä, mihin tilanteeseen on joutunut tai mitä tekee, saattaa olla opittua. Oikeutuksen käyttäminen edellyttäisi kuitenkin yksilön sisäistä keskustelua, joka etukäteen tai jälkikäteen. Kuten eräs haastateltava spontaanisti kertoi:

"Ei ihminen pysty siihen, että ne olisi päässä. Ei, vaikka käytät hyviä käytäntöjä, että on joku asia ja sitten toinen asia ja sitten siinä välissä muuttaa, vaikka numeroita. Ja miten ihminen perustelee sitä, että se ei vaihda sitä salasanaa? Ei se tietoisesti perustele sitä mitenkään. Tärkeintä on se, että pystyy käyttämään järjestelmiä sujuvasti."

Sykes ja Matzan (1957) teorian mukaan tahallinen teko ikään kuin naamioidaan näyttämään tahattomalle, ja siten torjutaan sekä syytökset sosiaalisten normien rikkomisesta että syytöksistä seuranneet häpeän tai syyllisyyden tunteet tai oletetut häpeän tai syyllisyyden tunteet. Kun salasanoihin liittyvistä käytänteistä keskusteli haastateltavien kanssa, jolloin he joutuivat tietoisesti pohtimaan asiaa, ei haastateltavissa ollut havaittavissa merkkejä syyllisyydestä tai häpeästä:

> ”Salasanoissa on meidän organisaatiossa muutenkin semmoinen ongelma, että jos kaunis ajatus on, että niitä ei saa kirjoittaa mihinkään muistiin, niin se systeemi ei toimi.”

> ”Jokainen tietää, että jokaisessa järjestelmässä pitää olla eri salasana, mutta että miksi näitä on niin pirun paljon. Ja kyllähän se ärsyttää.”

> ”Juuri tämä salasanojen säilyttämiseen liittyvä juttu. Se on mahdotonta, että ne pitää olla vaan korvien välissä, että ei saa mihinkään kirjottaa ylös. Ja mihinkään ei saa käyttää samaa salasanaa.”

> ”Juuri kirosin, kun se järjestelmä vaati sitä. Minun mielestä on todella iso virhe tehdä niistä niin vaikeita. Että kun tehdään niin vaikea salasanavaatimus, että erikoismerkkejä, numeroita, kirjaimia, välilyönti, piste, pilkku ja isot kirjaimet ja muut, että siitä salasanasta tulee niin vaikea, että se laitetaan paperille ylös. Taikka, että salasanassa tulee olla 18 merkkiä. Koska nytkin minulla on oltava niin pitkä salasana, että se on oltava paperilla ylhäällä. En minä pysty muistamaan niitä ja kun sitä ei tarvitse vielä koko ajan.”

> ”Salasana vaihdetaan, vasta kun järjestelmä pakottaa, ainakin minulla on se tilanne. Ja kun järjestelmä pakottaa, niin siinäkin vaiheessa minä kiroan ja koska se pelaa täällä muistipuolella, että pienellä muutoksella, että se menisi tänne muistiin. Ja kun olen [akuutti ja kriittinen työtehtävä] ja tarviin päästä nettiin ja siinä on pikkusen paljon ajateltavaa, sen pitää olla yhden napin takana, että se aukee. Koska siinä vaiheessa 16 merkkinen salasana, niin ei tule mitään. Siinä kiire on tilanteen luomaa.”

Vertailuorganisaation haastatteluissa mainittiin esimerkiksi:

> ”No kun pitää 16-merkkisiä salasanoja keksiä, niin ei ne pysy mielessä. Tai niin kuin minulla on yli 20-merkkinen salasana, ja olen sen oppinut, niin sitten pitää opetella uusi niin eihän se mitenkään onnistu”

Vertailuorganisaatiossa haastateltavilta kysyttäessä heidän syyllisyyden ja häpeän tunteitaan, kuvaili eräs haastateteltava muun muassa näin:

> ”En yhtään, en pätkääkään. Se, että pitää keksiä joku pitkä salasana, niin se on minun mielestäni vain näennäistä tietoturvaa.”

Jo se, että haastateltavat ylipäätään toivat esille salasanoihin liittyviä ongelmia ja haasteita, kertoi siitä, että kenenkään tarvinnut suojella itseään itsesyytöksiltä. Kuten eräs haastateltava mainitsee:

> ”No siis minä en voi tietää, koska en minä tiedä toisten ihmisten salasanoja.”

Vaikka toimisi tietoturvapolitiikan vastaisesti, valvonta ei ulotu salasanan vaihtamattomuuteen, jos järjestelmä ei pakota, tai salaamattoman sähköpostin lähettämiseen, vaikka tieto olisi pitänyt salata, tai jos järjestelmä ei automaattisesti tunnista heikkoa salasanaa, käyttäjä voi valita heikon, mutta helposti muistettavan salasanan. Eräs haastateltava mainitsi tästä näin:

> ”Jos ei ohjeessa ole mitään pakottavaa, niin ei sen noudattamista voi mitenkään tarkistaa. Miten sen tarkistaa? Ei mitenkään.”

Se, ettei työntekijä koe olevansa vastuussa, voisi toki tarkoittaa, että työntekijä on niin vieraantunut itsestään, ettei koe olevansa vastuussa elämästään eikä silloin myöskään tietoturvapolitiikan noudattamisesta. Se, mikä tekee tämänkaltaisesta vastuun kieltämisestä ristiriitaisen, on se, että työntekijä huolehtii päivittäiset työtehtävänsä vastuullisesti ja aikataulussaan, ja on sitoutunut organisaation toimintaan. Työntekijät eivät tunne syyllisyyttä ja häpeää siitä, että joutuvat kirjoittamaan salasanoja ylös muistin tueksi, tai etteivät muuta olemassa olevaa salasanaa täysin toisenlaiseen kuin aikaisempi oli, vaikka nämä ovat tietoturvapolitiikan vastaista toimintaa.

6.3.2 Vahingon kieltäminen *(”En vahingoittanut ketään”)*

Aiemmissa tietoturvatutkimuksissa vahingonkieltäminen –neutralisoimistekniikkaa on mitattu muun muassa väitteillä, voiko tietoturvapolitiikkaa rikkoa, jos sillä ei aiheuta vahinkoa tai kukaan ei loukkaannu (Li & Cheng, 2013; Silic ym., 2017; Siponen & Vance, 2010).

Sykes ja Matza (1957) esittävät teoriassaan näkemyksen, jonka mukaan rikollinen arvio tekonsa vakavuuden ja seurausten välistä yhteyttä. Neutralisoimisteorian mukaan yksilö tekee siis ikään kuin perustellun ja tietoisen päätöksen, joten hänellä on oltava vähintäänkin arvio seurauksista.

Tietoturvan yhteydessä työntekijän tulisi siis ensinnäkin tietää, millaisen rangaistuksen hän saisi. Työntekijän tulisi myös tietää, mitkä seuraukset hänen teollaan voisi olla. Tällä tarkoitetaan sitä, että työntekijän olisi kyettävä arvioimaan, aiheuttaako jokin teko esimerkiksi tiedon hallinnan menetyksen, tai voiko tiedon luottamuksellisuus vaarantua. Jos työntekijä siis oikeuttaisi itsensä kieltämään vahingon, hänen voisi olettaa myös ymmärtävän joko etukäteen tai jälkikäteen, mitä hän teki ja miksi. Haastateltavat kuvailivat tätä tietämystä:

> ”Tiedon menettämisen haaste on se, että se on erittäin vaikeasti mitattavissa, että mitä se vaikuttaa. Mikä tahansa organisaatio, joka tuottaisi x euroa ja sen euromääräiset tuottotarpeet on jotakin ja se tuottaa tiettyä palvelua tai tuotetta tai mitä tahansa, niin jos joku tieto menetetään, ei pystytä näkemään sitä, monenko euron tappio siitä juuri sillä hetkellä tuli tai vaikuttaa vähän ajan päästä. Koska joku joka on mahdollisesti saanut tiedon käsiinsä, joka ei hänelle kuulu, niin millon se sitä käyttää ja miten se käyttää sitä hyödykseen, sitä ei välttämättä tiedä.”

> ”Miten arvioitat tiedon? Kuinka kallista se tieto on? Sille ei voida laittaa euromäärästä hintaa, mutta palvelinkoneelle, sille voidaan määrätä hinta. Jos

esimerkiksi ajattelee koko elämän valokuvakokoelmaa, se ei ole minkään arvoinen toiselle, mutta toiselle mittaamattoman arvokas.”

”Minä en tuossa tilanteessa tietoisesti tee sitä virhettä, näin sanoisin. Ja minä en tässäkään tilanteessa tiedä olenko tehnyt väärin vai oikein. En edes tiedä tai ole varma, toiminko oikein vai en, mutta se on ainoa keino, minkä minä tiedän.”

”Kun olen maallikko käyttäjä, niin minä en tiedä, kuinka paljon tämmöisessä tiedonsiirrossa tulee jotain, mikä aiheuttaa tietoturvauhkaa. Kait siinä pystyy siirtämään harmittomana tiedostona myös jotain haittatietoja. Varmaan meidän suojausohjelmat haistelevat niitä koko ajan, minä en tiedä sitä mekanismia, mutta riskihän on tässä, että käyttäjä on se suurin riski ja kun sinulla on hyvin suojattu ja oma, niin näiden kahden välissä on se suurin riski.”

”Jos sähköpostiketjussa on parikymmentä, ja vastauksia pallotellaan siellä, välitetään eteenpäin ja muuta. Kai se on inhimillistä, ettei huomannut, kun painoikin vastaa kaikille, ja siellä onkin yksi, jolle asia ei kuulu millään lailla.”

”Yleensä perustellaan vaan sillä: tietoturva syistä –termillä. Tietoturva syistä, sinun pitää menetellä näin ja näin. Mutta en minä muista, että olisi koskaan laajasti avattu, että mitä tapahtuu, jos et toimi näin, että joku lamaantuu tai jotain. Työasema menee ehkä lukkoon, mutta mitä muuta tapahtuu, niin se on mysteeri.”

”Jos puhutaan tietoturvasta, niin ihminen ei täysin aina pysty ymmärtämään, mitä hän aiheuttaa järjestelmille, kun ei sitä ole koulutettu sille. Joitakin asioita ei kannatakaan kouluttaa, kuten jos teet näin, näin ja näin, niin pystyt kaataa koko järjestelmän. Mutta jos jätät tuon tekemättä, se voi vaikuttaa siihen, että kaadat tämän järjestelmän. Tietämättään. Se on pakko kertoa.”

”Tietoturva on aika hankala aihepiiri niille, jotka kokevat sen liittyvän vain salasanoihin tai että pääseekö joku murtautumaan sähköpostiin, eikä ymmärrä esimerkiksi sitä, että tietoturvallisuutta on tiedon käytettävyys tai että sen tulee olla eheää jne, ja ei siten koe välttämättä tietoturvaongelmaksi, jos tiedonsiirtoyhteys vähän pätkii, niin ei ymmärrä sitä kuin käytettävyys ongelmaksi, eikä näe yhteyttä siinä, että se on myös tietoturvallisuuteen liittyvä haaste.”

Neutralisoimisteoriaan liittyy oletus siitä, että yksilö kykenee tekemään arvioita omasta käyttäytymisestään ja sen seurauksista. Yksilö kykenee siis lähes varmasti ymmärtämään tekojensa seuraukset, ja hyödyntää erilaisia neutralisoimistekniikoita tekoon liittyvän syyllisyyden ja häpeän poistamiseen. Työntekijällä tätä varmuutta ei välttämättä oikeasti ole. Työntekijä ainoastaan käyttää järjestelmää, mutta ei varsinaisesti ole kehittämässä sitä, eikä hallinnoi sitä mitenkään, joten työntekijällä ei välttämättä ole edes mahdollisuuksia arvioida, mitä jokin teko tai tekemättä jättäminen lopulta aiheuttaa, koska passiivisuuskin voi vaarantaa tietoturvan. Teknologian arkipäiväisyydestä huolimatta tietoturvaan liittyvät riskit ovat usein niin moniuloitteisia, ettei asiantuntija saati loppukäyttäjä voi välttämättä arvioida oman käyttäytymisensä lopullisia seurauksia.

Haastatteluissa tietoturvarikkomuksen rangaistus ei ollut täysin selvää, vaikkakin arvioita haastateltavat mainitsivat useita.

”Ei ole tullut vastaan, ja suoraan sanottuna, en tiedä.”

”Et oikeasti saa mitään, jollet osoita sitä, että siitä on tullut isompaa haittaa. Jotain tehnyt, niin sitä pidetään moitittavana käyttäytymisenä ja sitten ohjataan oikeaan suuntaan, mutta ei siitä tule mitään oikeudellisia juttuja tai rangaistuksia.”

”Tuohon en osaa vastata mitään, että mikä se on loppupelissä sitten se rangaistus.”

”Mutta mikä on sitten rangaistus, se voi olla puhuttelu, huomautus, varoitus, mitä näitä nyt on. En tiedä miten näitä juttuja on edennyt, siis meidän organisaatiossa.”

Myöskään vertailuorganisaatiossa tietoturvarikkomuksiin liittyvät rangaistukset eivät haastatteluiden perusteella niin selkeitä. Haastateltavat kertoivat muun muassa näin:

”En tiedä, onko edes olemassa keinoa rangaista. Tietoturvaohjeiden rikkomista ei rangaista tai ne eivät ole kenenkään vastuulla. Vaikkapa [ammattinimike] ei edes ymmärrä, mistä on vastuussa.”

”En ole ikinä kaivanut, missä sanoittaisi tarkemmin, mitä voi tapahtua, jos tahallaan väärinkäyttää jotain.”

Vertailuorganisaation haastateltavat kuvailivat myös sitä, ettei käyttäjä välttämättä edes tiedä tehneensä mitään väärää, eikä siten välttämättä ymmärrä pelätä mitään rangaistusta toiminnastaan, muttei myöskään ymmärrä ilmoittaa tekemistään vääristä toimista. Esimerkiksi jokin haittaohjelma ei välttämättä latautuessaan näyttäydy käyttäjälle mitenkään.

Kuten luvussa kaksi esiteltiin, Sykes ja Matza (1957) esittävät vahingon kieltämisen –neutralisoimistekniikan yhteydessä termit ”*mala in se*” ja ”*mala prohibita*”. Yksilön täytyy siis tietää ne selitysmallit, jotka kulloisessakin kulttuurissa tekevät eron, onko rikos tai poikkeava teko väärin, koska se on kiellettyä, vai onko rikos tai poikkeava teko väärin, koska se rikkoo esimerkiksi moraalin periaatteita. Tutkimusaineistona olleista tietoturvapolitiikan dokumenteista ei ollut selkeästi löydettävissä, milloin sitä ei sovellettaisi, eli ei mainittu erillisiä määräyksiä tai ohjeita esimerkiksi poikkeustilanteisiin, jolloin tietoturvapolitiikka ei olisi voimassa.

6.3.3 Uhrin kieltäminen *(”Siitäs saivat”)*

Aiemmissa tietoturvatutkimuksissa uhrin kieltäminen –neutralisoimis-tekniikkaa on mitattu muun muassa sillä, että tietoturvapolitiikkaa voi rikkoa, jos esimies on puolueellinen, tai organisaatio ei menetä paljoakaan, jos tieto-turvapolitiikkaa rikkoo (Li & Cheng, 2013; Cheng ym., 2014). Willison ym., (2018) tutkivat myös uhrin kieltämisen –neutralisoimistekniikkaa tilanteessa, jossa työntekijä olisi kokenut tulleensa kohdelluksi epäoikeudenmukaisesti.

Sykes ja Matza (1957) selittävät teoriassaan tätä neutralisoimistekniikkaa ikään kuin kahdessa osassa. Ensimmäinen osa liittyy siihen, kuinka rikollinen

myöntää olevansa vastuussa, mutta teko on pikemminkin laillinen kosto tai rangaistus. Kuten jo luvussa kaksi esiteltiin, tähän tekniikkaan liittyy myös tilanne, jossa rikollinen kokee olevansa hyväntekijä eikä rikollinen. Toinen osa taas liittyy tilanteisiin, joissa tieto uhrin olemassa olosta sivuutetaan.

Tietoturvan yhteydessä on hankala määritellä ensinnäkin se, kenelle halutaan kostaa tai ketä halutaan rangaista. Onko se joku organisaation jäsen, jokin organisaation osasto tai yksikkö, vai koko organisaatio? Toisaalta organisaatio ympäristössä on vaikea määritellä, kuka tai mikä olisi tuntematon uhri, jonka olemassa olon voisi sivuuttaa, koska työntekijä on itse organisaation sisällä. Tietoturvatutkimuksissa on tutkittu niin sanottujen sisäpiiriläisten tekemiä väärinkäytöksiä, kuten tahallista tietojen hävittämistä, tietomurtoa, petosta, kiristystä, kavallusta, tietojen myymistä ja luovuttamista. Muun muassa Willison ja Warkentin (2013) sekä Nicho ja Kamoun (2014) mainitsevat tutkimuksessaan näistä sisäpiirin tekemistä väärinkäytöksistä. Li ja Cheng (2013) sekä Cheng (2014) olivat tutkimuksessaan tulkinneet muun muassa "pomon" uhriksi, jota rangaistaan puolueellisuudesta, sekä organisaatio oli ikään kuin tuntematon uhri, joka ei menettäisi paljoakaan työntekijöiden henkilökohtaisesta internetin käytöstä.

Haastatteluaineistosta ei voinut päätellä kenenkään kostonhalua tai halua rangaista ketään henkilöä, organisaation osaa tai koko organisaatiota. Haastatteluiden mukaan kosto jotakuta henkilöä kohtaan, vaikuttaisi lähes väistämättä koko organisaatioon. Vaikka haastateltavat eivät ilmaisseet kostonhalustaan tai halustaan ottaa oikeutta omiin käsiinsä, se ei tarkoita, etteikö joku haastateltavista voisi näin joskus toimia. Mikäli näin kävisi, silloin kyse ei välttämättä enää olisi rikkomuksesta, vaan kyse saattaisi olla rikoksesta. Suomalaisen lainsäädännön mukaan muun muassa tietomurto tai tietojärjestelmän häirintä tai niiden yritys voivat olla rikoslain mukaisesti tuomittavia tekoja (Finlex, 2007).

6.3.4 Tuomitsijoiden tuomitseminen *("Kaikki kiusaavat minua")*

Aiemmissa tietoturvatutkimuksissa tuomitsijoiden tuomitseminen –neutralisoimistekniikkaa on mitattu väitteillä, että tietoturvapolitiikka ei ole järkevä, se on liian rajoittava tai tietoturvapolitiikan noudattaminen vie liikaa aikaa (Siponen & Vance, 2010). Tekniikkaa on mitattu lisäksi väitteillä, että kaikki käyttävät organisaation hyväksymättömiä ohjelmistoja (Silic ym., 2017), tai että organisaation tulisi huolehtia muista asioista, kun työhön liittymättömästä internetin käytöstä (Li & Cheng, 2013).

Sykes ja Matza (1957, 668) esittävät teoriassaan, että rikollinen ikään kuin hyökkää niitä vastaan, jotka joko valvovat normien ja lakien noudattamista, tai eivät hyväksy rikollista toimintaa.

Tietoturvakontekstissa tietoturvapolitiikan on rinnastettu edustavan normien ja lakien noudattamista valvovaa tahoa. Kuten jo aiemmin tässä luvussa mainittiin, tutkimusaineistona olleista tietoturvapolitiikan dokumenteista ei ollut selkeästi löydettävissä, milloin sitä ei sovellettaisi, eli mainintoja poikkeustilanteisiin, jolloin tietoturvapolitiikka ei olisi voimassa, ei löydy.

Tänä päivänä on mahdollista erilaisin teknisin välinein valvoa organisaation toimintaa esimerkiksi valvontakameroilla, kulunvalvonnalla ja tietoverkon

käytön valvonnalla (lokitiedot, välitystiedot). Vaikka tekninen valvonta olisikin tänä päivänä osa normin noudattamiseen liittyvää kontrollia, tämän tutkimuksen rajauksessa Sykes ja Matzan teoriaa verrataan vain tietoturvapolitiikkaan, eli sen toimii ikään kuin auktoriteetin tai valvojan asemassa. Tekninen valvonta ei pysty ulottumaan kaiken kattavasti siihen, noudatetaanko tietoturvapolitiikassa annettuja linjauksia, määräyksiä, ohjeita, tavoitteita ja toimintatapoja, vaan niin sanotun loppukäyttäjän ratkaistavaksi jää, miten hän lopulta eri tilanteissa toimii. Miten loppukäyttäjä sitten suhtautuu tähän niin sanottuun auktoriteettiin? Vaikka aiemmin käsiteltiin jo sitä, miten tietoturvaan ja tietoturvapolitiikkaan suhtaudutaan, tässä kohtaa tietoturvapolitiikkaa tarkastellaan enemmän siitä näkökulmasta, miten noudattamisen velvollisuuteen suhtaudutaan, onko tietoturvapolitiikka oikeudenmukainen, tasapuolinen vai onko tietoturvapolitiikassa esimerkiksi ylilyöntejä. Tietoturvapolitiikkaan liittyvää joustamattomuutta kuvailtiin esimerkiksi:

> ”Kyllähän niitä pitää noudattaa ja ne ovat aika tiukasti rajattuja, mutta elävä elämähän on sitten...”

> ”Jos ohjeissa on jotain, se on lähtökohtaisesti kiellettyä, mutta kun sellainen ei ole käytännön elämää.”

> ”Kyllä monessa tilanteessa ohjeita joudutaan soveltamaan. Mutta se ei ole lähtökohta.”

> ”Kyllähän me monessa tietoturva-asiassa sanotaan, että asian tekeminen täysin meidän organisaation ohjeiden mukaan aiheuttaa sen, että sieltä tulee loppukäyttäjä sen tehtävän tehneenä verisenä ja hakattuna ulos.”

Myöskään vertailuorganisaation tietoturvapolitiikasta ei löydy mainintaa, milloin sitä ei noudettaisi. Eräs haastateltava mainitsee osallistuneensa tietoturvaan liittyvään koulutukseen ja kuvailee koulutuksen jälkeistä tuntemusta:

> ”Silti päällimmäiseksi jäi tunne, että tietoturvapolitiikan noudattaminen perustuu vapaaehtoisuuteen.”

Jos tietoturvapolitiikkaa verrataan edelleen ikään kuin auktoriteettiin, se joutuu myös kilpailemaan asemastaan, kuten haastateltavat selittivät:

> ”Pitää muistaa, että tietoturva, tietysti tärkeä asia, niin se on vaan yksi työntekijän kaikista niistä ohjeista, jota tulvii joka puolelta ja nykyisillä tietojärjestelmillä koko ajan tulee: pitää kirjautua ulos tänään, kun on huoltokatko, kaikkea mitä pitää itse tehdä määrityksiä, jotta pääset internettiin. Niitä tulee koko ajan. Sekin on niin, että jotenkin se pitää priorisoida, mikä on oikeasti tärkeätä ja mikä ei oo niin tärkeetä. Se tietotulva ja ne vaatimukset, mitä pitää tehdä ja mitä ei pidä, niitä on hirveästi.”

> ”Mutta täytyy miettiä mikä on itseistarkoitus. Eli mitä me tehdään ja mihinkä me halutaan sitä tietoa. Itseistarkoitus ei ole tiedon turvaaminen, vaan sen käyttäminen ja tiedon tuottaminen, ja sitä kautta tehdään analyysi ja päätökset. Se vain varastoidaan johonkin turvallisesti.”

Se, että työntekijät mainitsevat työelämän realiteeteista, ei kuitenkaan suoraan ilmaise tietoturvapolitiikan ja tietoturvan kunnioittamisen tai arvostamisen puutteesta. Moniammatilliseen organisaatioon liittyviä työelämän realiteetteja tuli myös haastatteluissa esille.

> ”(Koulutus)taustalla on vaikutusta siihen, mitkä ovat intressit ja mihin kiinnittää huomiota ja mihin keskittyy ja mitkä kokevat, että tämä kuuluu nyt minulle ja että tämä on nyt minustakin kiinni tämä toiminta, että minulla on myös oma roolini hoitaa tämä kunnolla. Ehkä siinä tavallaan tulee niitä eroja, kun joku kokee, että tämä minun toiminta nyt tähän vaikuta.”

> ”Suurimpana näen sen, että tekniikka menee niin hurjasti eteenpäin, että käyttäjät ei ehkä pysy siinä kärryillä, että mitä työvälineitä on käytössä. Esimerkiksi normaali niin sanottu peruskäyttäjä ei tiedä, millä voi liitetiedoston salata ja mikä nyt on se oikea menettelytapa lähettää, kun niin yksityiskohtaisia asioita ei tietoturvaohjeessa voi olla. Koska jos vaikka [organisaatio Y] muuttaa jonkun salaustuotteen käyttöä, se on tänään voimassa, muttei enää huomenna, vaan se muuttuu välittömästi.”

> ”Tämä nyt hyppää vähän isompaan kuvaan, mutta minun mielestä ala kärsii siitä, että normaalit peruskäyttäjät ja monesti organisaatiossa vähän ylemmälläkin olevat ihmiset ajattelevat, että se turvallisuus on niiden turvallisuus-ihmisten heiniä, että tehkää te, tehkää meille ohje, kertokaa, miten se tehdään.”

> ”Tietoturvassa on se, että jos ei asia ole tullut vastaan, ei sitä ole osannut ottaa oikein edes huomioon. Tietoturvaan pätee ainoastaan koulutus ja koulutus siihen on suhteellisen pitkä. Olen ottanut esimerkkinä sähkömiehen, koska se on tekemisissä sähkön kanssa ja sitten on aivokirurgi ja sekin on tekemisissä sähkön kanssa, mutta se on aivoissa. Mutta voiko ne vaihtaa tehtäviänsä? Sähkön kanssa kumpikin on tekemisissä. Voi vaihtaa. (ironisesti) Eli kun yleistetään asioita, sähkö kun sähkö, tietoturva kun tietoturva... kyllä se siitä.”

Vertailuorganisaatiossa aihetta pohdittiin muun muassa:

> ”Tekniikka on mennyt organisaatiosta ohi. Ei ole ajateltu tulevaisuuteen, vaan ajateltu, että se mikä on tehty, on hyvä. Tehdään hirveä työ toimintamalleista, mutta tuon taivaallista kukaan ei noudata niitä. Kukaan ei valvo niiden noudattamista. Uudet asiat eivät istu toimintaan. Jatkuva kehitys, mutta toiminta ei muutu.”

> ”Käyttäjät, jotka suurin piirtein tietävät, mitä haittaohjelmalla tarkoitetaan, niin ne saattavat osata vähän pelätäkin, mutta iso osa henkilöstöstä ei ymmärrä niistä mitään.”

> ”En tiedä ajatellaanko eri yksiköissä asiaa ollenkaan. Luulen, että tietoturvan näkyminen on hyvin yksikkökohtasta, it-puolella se on huomattavasti enemmän mielessä kuin tuolla jossakin muualla.”

Vaikka tietoturva siis koskettaa kaikkia, silti koulutus, työtehtävät ja asema organisaatiossa vaikuttavat niin asenteisiin kuin käytännön toimintatapoihin. Schein (1991, 54–55) toi jo yli kolme vuosikymmentä sitten, eli vuonna 1985 julkaistussa teoksessaan, esille, kuinka tietojenkäsittelytekniikan veljeskunnalla on

omat sanastonsa, omat norminsa, omat perinteensä, oma näkemys merkityksestään ja oma käsityksensä siitä, miten tekniikkaa tulisi käyttää, ja on täysin mahdollista, ettei mikään näistä sovi yhteen järjestelmiä käyttävien kielessä, tarkastelutavoissa tai edes normien kanssa. Jollain tapaa tilanne ei ole vuosikymmenissä vieläkään muuttunut riittävästi. Da Veiga ja Martins (2017, 88) toteavat tuoreessa tutkimuksessaan organisaatioiden pitävän sisällään ikään kuin kahta alakulttuuria. Informaation teknologian parissa työskentelevät työntekijät, jotka suhtautuvat tietoturvaan myönteisesti ja työntekijät, jotka eivät työskentele informaation teknologian parissa, ja jotka eivät suhtaudu tietoturvaan yhtä myönteisesti (Da-Veiga & Martins, 2017, 85).

6.3.5 Vetoaminen korkeampiin lojaliteetteihin *("En tehnyt sitä itseni vuoksi")*

Aiemmissa tietoturvatutkimuksissa vetoaminen korkeampiin lojaliteetteihin – neutralisoimistekniikkaa on mitattu esimerkiksi sillä, että työhön kuulumaton internetin käyttö hyödyttää joko yksilöä itseään tai organisaatiota, tai työhön kuulumaton internetin käyttö tehostaa työn tekemistä, tai perheenjäsen, ystävä tai muu merkittävä henkilö vaati tekemään niin (Cheng ym., 2014; Li & Cheng, 2013). Silic ym., (2017) tulkitsivat menetelmän käyttöä siten, että muun kuin työnantajan tarjoama työväline hoitaa tai suojaa jotakuta. Siponen ja Vance (2010) mittasivat neutralisoimistekniikkaa sillä, että yksilö perustelisi saavansa työnsä tehtyä tai suorittavansa johdon antamaan tehtävää.

Sykes ja Matza (1957, 669) esittivät teoriassaan, että rikollisesti tai poikkeavasti käyttäytyvä ei kiistä vallitsevan normatiivisen järjestelmän vaatimuksia, vaan ikään kuin sivuuttaa ne suuremman lojaliteetin vuoksi. Sykes ja Matza (1957, 669) viittaavat sosiaalisiin siteisiin, kuten sisaruksiin, jengiin ja ystävyyssuhteisiin, mutta eivät teoriassaan esittele, mikä tietyssä tilanteessa aiheuttaa vaatimusten priorisoinnin, eli missä tilanteessa esimerkiksi lain tai normin rikkominen hyödyttää hänen vahvaa sosiaalista sidettään enemmän kuin lain tai normin mukainen käyttäytyminen.

Kuten edellä mainittiin, tietoturvatutkimuksissa tuota arvojen niin sanottua priorisointia on tutkittu henkilökohtaisen edun, organisaation toiminnan turvaamisen ja sosiaalisten suhteiden kautta. Sanana lojaalius, lojaalisuus ja lojaliteetti voivat tarkoittaa lainkuuliaisuutta, mutta myös luotettavuutta, uskollisuutta ja rehtiyttä (Turtia, 2010, 320). Kuten Sykes ja Matza (1957, 669) esittävät, normatiivisen järjestelmän vaatimuksia ei noudateta, vaan ne sivuutetaan pienempien sosiaalisten ryhmien (engl. *smaller social groups*) vuoksi. Tämän tutkimuksen tulkinnan mukaan Sykes ja Matza tarkoittivat vetoaminen korkeampiin lojaliteetteihin selityksellä -"En tehnyt sitä itseni vuoksi"- sitä, että teko tehdään jonkun toisen (ihmisen tai asian) vuoksi.

Tämän tutkimuksen yhtenä olettamuksena oli, että mikäli tietoturvarikkomuksen tekisi jonkun toisen vuoksi, se edellyttäisi erittäin vahvaa sosiaalista sidettä. Rikkomuksen tekijän tulisi arvottaa sosiaalinen side vahvemmaksi kuin mitä rangaistuksen seuraukset olisivat. Tuollaista äärimmäistä tilannetta ei haastatteluissa tullut esiin. Sykes ja Matza (1957) teoria ei täysin sellaisenaan istu tietoturvakontekstiin, joten tämän neutralisoimistekniikan yhteydessä tarkasteltiin,

voisiko lojaliteetti kohdistua johonkin arvoon tai periaatteeseen, joka nousisi korkeammalle prioriteetille tai jotain asiaa kohtaan olisi suurempi lojaliteetti kuin tietoturvapolitiikan noudattaminen. Haastateltavat kuvailivat tilanteita, joissa tietoturvapolitiikan noudattaminen ei välttämättä ohjaa toimintaa.

> ”Lähinnä olen nähnyt sen niin, että on kiire. On asioita, jotka on hoidettava ja kun järjestelmät eivät toimi hyvin, se aiheuttaa lisää kiirettä ja silloin saatetaan tehdä jotain, mitä ei ole sallittua tehdä.”

> ”Ehkä turhautumista, ja sitten kiire taas. En tiedä tuleeko se kiire siitä, että asioita ei saa tehtyä, kun se on niin kankee se järjestelmä. Mutta ongelmia se aiheuttaa kyllä.”

> ”Kun jotain on pakko tehdä kiireellä, niin se on pakko tehdä, vaikka tietoisesti tietoturvan kustannuksella.”

> ”Yksi on semmoinen, että on kiire. En tiedä sitten, onko se oikeata kiirettä vai tehtyä kiirettä, mutta välillä on kiire eli periaatteessa siinä kohtaa pitää aina katsoa, että huoneessa ei ole mitään muille kuulumatonta tietoa.”

> ”Joskus on sellanen tilanne, että oikein tekeminen tavallaan ei mahdollista sitä maaliin pääsyä siinä aikaikkunassa, eli riski on otettava. Kyllä se on niin, että kiire ajaa siihen pisteeseen, eli jos työ tehdään ohjeen mukaisesti, se ei ehdi siihen aikamääreeseen. Se on organisaation etu, että pääsee suorittamaan sen tehtävän. Oma henkilökohtainen kiire ei ole se motivaattori siinä.”

> ”Katson, että organisaation etu, koska sama ihminen minä olen, teen minä sen työn vai en, autanko minä siinä vai en, mutta minä katson aina sitä kokonaisuutta, että mihin se ratkeaa.”

Kysymykseen, voiko kiire olla aitoa vai opittua, haastateltavat selittävät:

> ”En tiedä, onko kiire opittua, mutta kun nykyisellä työrytmillä tehdään asioita ja tehtävänannot tulee siten, että huomenna on oltava valmis, niin tämä on ongelma meillä.”

> ”No tänä päivänä monelle organisaatiolle tuttu, eli tekniikka on mahdollistanut valtavan informaatiomäärän ja sitä kautta kyselyjä, tietopyyntöjä, lukuisia samanaikaisia tehtäviä ja yksilö niin sanotusti tukehtuu siihen massaan ja siinä se kiire sitten tietenkin tulee.”

> ”Kyllä se voi olla ihan aito tarve saada nopeesti se tieto. Ehkä aina ei ole näin, mutta jos ryhdyt sitä yhtä asiaa selvittämään, tai annat sen jollekin muulle, kun olet siinä asiassa kiinni ja on monta muuta asiaa siinä päällä ja sen jälkeen se saattaa unohtua tai jää johonkin vaiheeseen, että jääkö se sinne ja kun haluaisi kuitenkin sen asian loppuun kerralla, kun kerran on sen aloittanut. Keskeytykset ovat aina ikäviä ja siitä ehkä tulee se paine sitten.”

> ”Ei se voi todellinen olla. Missään ei lue, että vähän voi rikkoa lakia, jos on kiire. Kiire ei oikeasti voi olla semmoinen syy, mutta sillä perustellaan monesti sitä. Varsinkin silloin, jos tapahtuu poikkeama. Joku pieni tietoturvarikkomus voi johtua kiireestä, aikataulu painaa päälle ja pitää tehdä. Pidempi aikaista taas ei voi perustella kiireellä.”

> ”Jos tulee oikein kiire, niin pannaan se tietokone vähäksi aikaa kiinni, niin se kiire menee ohi.”

”Ehkä se on omalla tavalla tehtyä kiirettä. Tuolla tulee kyllä nopeita juttuja, mutta sillä kiireellä myös selitetään, että ei ole aikaa, sillä selitetään kanssa hirveen paljon. Se on olevinaan hienoa, että on kiire, vaikka välttämättä ei oikeasti olekaan.”

”Sekä että. Toiminnan jatkuvuuden kannalta, voi kiire olla ihan todellinen ja näen sen ihan ymmärrettävänä perusteluna sille yksilölle, mutta sen yksilön pitäisi myös muistaa se annettu koulutus, että on olemassa myös muita keinoja toimia.”

Moniammatillisessa organisaatiossa työtehtävät voivat vaihdella paljonkin, joten toisille kiire voi tietyssä tilanteessa olla todellinen kiire, kun taas toiselle, työtehtävät eivät ole yhtä kiireisiä. Olipa kiire sitten todellinen tai epätodellinen, haastateltavien puheissa työtehtävästä suoriutuminen nousi korkeammalle prioriteetille kuin tietoturvapolitiikan noudattaminen. Kuitenkin tässä neutralisoimistekniikassa nimenomaan vedotaan siihen, ettei tekijä tehnyt tekoa itsensä vuoksi, vaan jonkin korkeamman lojaliteetin vuoksi. Poistaisiko työntekijä siis omantunnontuskia, itsesyytöksiä, syyllisyyttä ja häpeää siitä, että oikeuttaa itsensä toimimaan vastoin tietoturvapolitiikkaa organisaation toiminnan jatkuvuuden hyväksi? Työstä johtuva kiire ja töiden priorisointi voivat toki aiheuttaa itsesyytöksiä, ja on täysin mahdollista, että työntekijä voisi järkeistää, että jos teko nyt ei niin oikein ollutkaan, se on silti hyväksyttävää. Ristiriitaisuuden tässä kohtaa tekee se, kuten jo aiemmin tuli esille: tietoturvapolitiikan laatii joku, joka ei voi ottaa ohjeita, määräyksiä ja sääntöjä laatiessaan huomioon kaikkia tilanteita. Toisaalta voidaan kysyä, millaisen rangaistuksen työntekijä saa, jos yksittäisellä teolla turvaa organisaation toiminnan jatkuvuutta? Se, että jättäisi jotain tekemättä kiireeseen vedoten, voidaan olettaa aiheuttavan organisaatiossa enemmän paheksuntaa, kuin se, että tekee jotain vedoten kiireeseen.

Myös vertailuorganisaation haastatteluissa arvojen tai periaatteiden priorisointia käsiteltiin. Haastateltavat selittivät näkemyksiään näin:

”Se voisi olla joku sellainen tilanne, jossa joku asia pitää vain saada aikaseksi. Tekemättä jättämisen seuraukset ovat suuremmat kuin sen rikkeen. Että se asia painaa enemmän vaakakupissa, tai käy vielä huonommin jollekin yksittäiselle ihmiselle tai meidän organisaatiolle, jos sitä rikettä ei tee, niin silloin rikkeen todennäköisesti voisi tulla tehdyksi. Jos mennään johonkin ihmisen henkeä uhkaaviin asioihin, niin ei sen ihmisen tarvitse hirveästi merkitä. Jos henkeä tai terveyttä uhkaavaa tai tämmöistä, niin hyvin helposti saattaisi tehdä väärin (rikkomuksen).”

”No varmaan siinä on se, että pääosin täällä ei ole oikeesti aikaa ja toinen syy on sitten ihan vaan laiskuus, enkä tarkoita, että ihmiset ovat laiskoja, vaan siitä tulee vaan niin paljon monimutkaisempi ylläpitää versus se aika mitä on käytettävissä, niin se on käytännössä mahdoton tehdä sitä, miten ehkä haluisi tehdä.”

”No henkilökohtaisesti olen sitä mieltä, että eihän näissä koskaan pitäsi olla niin kiire. Kun omalta kannaltakin tätä miettii, niin eihän tätä näin pitäisi tehdä. Ei voi olla niin kiire jollakin asialla, että pitää häslätä, mutta jotenkin tuntuu, että kun ylemmälle tasolle mennään niin, ei sillä niin ole väliä, kunhan se vaan nyt jotenkin tapahtuu. Että jos jotain pitää tehdä nopeasti, niin ei haittaa, vaikka se rikkoisikin jotain.”

6.3.6 Oppiminen

Sykes ja Matza (1957, 664) mainitsevat:

> "It is now largely agreed that delinquent behavior, like most social behavior, is learned and that it is learned in the process of social interaction".

On siis laajasti hyväksytty ajatus siitä, että rikollinen käyttäytyminen opitaan. Aiemmat neutralisoimisteoriaa tietoturvakontekstissa soveltaneet tutkimukset eivät ole käsitelleet tätä kriminologian keskeistä olettamusta.

Neutralisoimisteoriassa yhdistyvät ikään kuin sekä oppimisteoria että kontrolliteoria, koska yksilön pitää oppia neutralisoimistekniikat, mutta hänen täytyy ikään kuin peilata omaa käyttäytymistään sosiaaliseen kontrolliin ja/tai sosiaalisiin siteisiin. Jos kyse olisi vain oppimisteoriasta, silloin teorian voisi olettaa sisältävän esimerkiksi mallioppimista. Sykes ja Matza (1957, 667) mainitsevat alaviitteessä:

> "A number of observers have wryly noted that many delinquents seem to show a surprising awareness of sociological and psychological explanations for their behavior and are quick to point out the causal role of their poor environment."

Tämä Sykesin ja Matzan esittämä näkemys ikään kuin vahvistaa sitä, että tekijä on tietoinen, millaiset selitykset ovat yleisesti hyväksyttyjä. Mitä ilmeisimmin Sykes ja Matza päättelivät, että koska rikokseen oppimisprosessia oli käsitelty riittävästi, he keskittyivät vain opintosisältöön, eli neutralisoimistekniikoihin ja siihen, mitä ne pitävät sisällään. Ihminen ei oletettavasti ole muuttunut 1900–luvulta niin paljoa, etteikö hän edelleen oppisi asioita sosiaalisen vuorovaikutuksen ja vastavuoroisuuden kautta. Jos siis tietoturvarikkomuksia neutralisoidaan, voidaan olettaa, että tietoturvapolitiikan vastainen asenne, tekniikat ja motivaatio opitaan työyhteisön sisällä. Vaikka rikkomuksen tekeminen olisi sikäli subjektiivinen päätös, että yksilö käy itsensä kanssa ikään kuin sisäisen keskustelun, hänen on silti tiedettävä, mitkä selitykset olisivat yleisen käytännön jatkeita (engl. *an extension of common practice)* eivätkä niinkään niiden vastakohtia, jolloin selityksen hyväksyttävyys olisi todennäköisempää.

Kuten aiemmin alaluvussa 6.2 mainittiin, tietoturvan olemassa olon merkitys vaikuttaisi olleen haastateltaville ymmärrettävä, vaikka tietoturvapolitiikka itsessään ei välttämättä tukisi käytännön työn tekemistä. Jo se tosiasia, että organisaatioissa on tänä päivänä tietoteknisiltä taidoiltaan erilaisia työntekijöitä, saa kysymään, opitaanko tietoturvarikkomusten tekninen toteutus vuorovaikutuksen kautta? Entä tapahtuuko myös tietoturvarikkomuksille myönteisen asenteen oppiminen opettamalla? Haastateltavat selittävät, kuinka haasteena voi olla myös tavoista poisoppiminen.

> ”Kun mainitsit kysymyksen, minkä takia ihminen toimii vastoin ohjeita. Tässä on monta kertaa huomannut, että esimerkiksi sitä tietoturvaohjetta ei tunneta, sitä ei ole edes luettu, sitä ei ole löydetty, vaan oletetaan, on oletamus. Jotenkin tuntuu, että lukkiudutaan tekemään asioita, siten kuin on kerran opittu tekemään joku juttu, niin lähdetään painamaan sillä. Ja odo-

> tetaan, että syöte tulee turvallisuuden puolelta, että kyllä joku tulee ottamaan minua kädestä kiinni ja sanoo, että ei, et voi tehdä, et voi salata tällä, et voi lähettää tätä näin tai tuolla tavalla. Poisoppiminen on turva-asioissa..."

> "Koska ihminen toimii, siten miten se on oppinut toimimaan ja osaa tehdä sen hyvin, juuri niin kuin se on oppinut tekemään, mutta se ei välttämättä ole oikein täällä työelämässä."

> "Se on vähän niin sanotusti opittu se tapa jossakin muualla, että kun näin onnistuu kotona helposti."

Vertailuorganisaatiossa oppimista haastateltava kuvaili näin:

> "Henkilökohtaisesti se tapahtui niin, että työhuoneessa kirosin, että taas pitää keksiä uusi salasana, jossa on viissataamiljoonaa merkkiä, niin sermin takaa kuului, että minä käytän siellä lopussa sellaista juoksevaa numerointia. Johon totesin, että ai no tämähän toimii, otanpa itsekin käyttöön. Eli se on opittu juttu kyllä. Joku on sen kokeillut, ja se toimii, ja elämä on mukavaa taas."

Haastateltavat kertoivat myös, kuinka oikeat toimintatavat voi sisäistää.

> "Se ei pääsääntöisesti tule kyllä opettamalla, vaan koen, että se on tullut sisäistämällä sieltä alusta asti. Muistan kyllä, kuinka ensimmäisinä päivinä silloisella osastolla päällikkö otti huoneeseensa ja kävi läpi muutamia organisaation toimintaan siihen maailman aikaan liittyviä asioita, että kyllä se on lähtenyt minulla ainakin ensimmäisistä päivistä sillon, että tietyt asiat menevät tietyllä tavalla ja tietyt asiat on otettava toiminnassa huomioon. Ei mitään yksittäisiä koulutusketjuja, vaan aina jollain tavalla näitä tietoturva-asioita on tuotu esiin."

Haastateltavat eivät osanneet selittää tai havainnollistaa, miten oikeiden toimintatapojen sisäistäminen konkreettisesti tapahtuu. Kuten Schein (1991, 32) esittää, organisaatiokulttuuri pitää sisällään ikään kuin perusoletuksia, jotka ovat alitajuisia, näkymättömiä ja itsestäänselvyyksiksi muodostuneita. On siis mahdollista, etteivät haastateltavat kyenneet selittämään ulkopuoliselle näitä heille itsestäänselvyyksiä.

Vaikka haastateltavat eivät kyenneet täysin selkeästi selittämään, mitä, missä ja miten oppiminen tapahtuu, vaikuttaisi sille, että edelleen tänä päivänä oppimiseen liittyy edes jonkinasteinen vuorovaikutteisuus. Se, että oppii yksittäisen tavan kiertää tietoturvan teknisen ratkaisun, ei kuitenkaan välttämättä tarkoita, että oppii tietoturvarikkomuksia suosivan asenteen ja motivaation.

6.3.7 Ennen vai jälkeen oikeuttaminen

Sykes ja Matza (1957, 666) esittävät teoriassaan:

> "They are viewed as following deviant behavior and as protecting the individual from self-blame and the blame of others after the act. But there is also reason to believe that they precede deviant behavior and make deviant behavior possible."

Kuten jo luvussa kaksi mainittiin, tähän Sykes ja Matzan teoriaan kohtaan, oikeutetaanko rikollinen tai poikkeava teko ennen vai jälkeen teon, on kohdistunut

paljonkin arvostelua. Maruna ja Copes (2005, 231) tulkinnan mukaan Sykes ja Matza (1957) teoriassa esitetty ajatus ”neutralisoinnit edeltävät poikkeavaa käyttäytymistä” tarkoittaisi sitä, että pitämällä rikollisia avuttomina olosuhteiden uhreina, edistettäisiin neutralisointiin liittyvien tekosyiden sisäistämistä. Kuitenkin Topalli (2005, 826) ja Maruna ja Copes (2005, 227) toteavat olevan vaikeaa ennustaa aikooko yksilö neutralisoida jotain vai kertooko hän jälkikäteen selityksiä toiminnastaan.

Tietoturvakontekstissa etukäteen oikeuttaminen saattaisi tarkoittaa, että huolimatta siitä, että työntekijä olisi sisäistänyt organisaation tietoturvapolitiikan mukaiset ohjeet, säännöt, vaatimukset ja lait esimerkiksi asiakirjojen ja/tai henkilötietojen käsittelyyn, salasanakäytäntöihin, sähköpostikäytäntöihin ja lokien keräämiseen, hän haluisi silti rikkoa niitä, ja joko tietäisi tulevansa kokemaan syyllisyyttä ja häpeää tai kokisi syyllisyyttä ja häpeää jo ennen kuin olisi ryhtynyt tietoturvarikkomukseen. Työntekijän tulisi ennen tuota aiottua toimenpidettä pohtiessaan tietää erilaisia vaihtoehtoja, joilla selittää itselleen, ettei ole vastuussa siitä, mitä tulee tekemään, tai ettei mitään vahinkoa tule tapahtumaan, tai että rikkomus on itseasiassa laillinen kosto, tai ettei tietoturvapolitiikka ole ketään ohjeistamaan tai valvomaan. Vasta sopivan oikeutuksen löytäminen aktivoisi työntekijän tietoturvarikkomuksen. Jälkikäteen oikeuttaminen puolestaan tarkoittaisi sitä, että työntekijä tekisi ensin tietoturvarikkomuksen. Työntekijän kokisi teostaan omantunnontuskaa, syyllisyyttä, häpeää ja itsekunnioituksen menetystä, ja säilyttääkseen eheän minäkuvan, hän joko syyttäisi teosta muita tai kaivaisi muistinsa kätköistä edellä mainitut selitysmallit, jotka hän on oppinut sosiaalisen vuorovaikutuksen kautta. Tutkimusaineistosta ei kuitenkaan ollut löydettävissä edellä esitetyn kaltaista yksilön käymää sisäistä keskustelua.

Vaikka haastateltavat mainitsivat salasanojen mieleen painamisen vaikeudesta, kiireestä, erilaisista tietojärjestelmän tai laitteen käyttöön liittyvistä ongelmista, ymmärtämättömyydestä tai tietämättömyydestä, on näiden perusteella vaikea ennustaa, aikooko työntekijä käyttää näitä selityksiä jatkossa etukäteen. Haastattelutilanteessahan haastateltavat kertoivat tapahtumista, jotka olivat tapahtuneet ennen haastattelua.

Vaikka haastatteluista saa vaikutelman, ettei tietoturvapolitiikan noudattamattomuuden tai sääntörikkomusten taustalla välttämättä ole oman edun tavoittelu, pahantahtoisuus, välinpitämättömyys, sosiaalinen paine, se ei kuitenkaan tarkoita, etteikö työntekijä voisi selittää myös tulevaisuudessa, ettei osaa, ymmärrä, tiedä tai ehdi. Näihin selityksiin, ja siihen tapahtuuko selittäminen etukäteen vai jälkikäteen tai missä tilanteissa selitys tapahtuisi etukäteen ja missä jälkikäteen, palataan myöhemmin tämän luvun lopussa.

6.3.8 Uskomukset vs toiminta

Sykes ja Matzan (1957, 667) teorian keskeinen lähtökohta on se, että sosiaaliset kontrollit pyritään tekemään tehottomiksi, jolloin sisäistettyihin normeihin liittyvät uskomukset eivät vastaa todellista toimintaa. Kuten Sykes ja Matza (1957, 667) esittävät:”*In this sense, the delinquent both has his cake and eats it too…”* Myös suomen kielessä käytetään vastaavaa sanontaan kuvaamaan tilannetta, jossa henkilö

haluaa kahta asiaa, mutta jotka kumoavat toisensa. Onko tietoturvapolitiikan noudattamattomuudessa samaan tapaan kyse uskomusten ja toiminnan välisestä ristiriidasta kuin Sykes ja Matzan teoriassa?

Kuten luvussa kolme käsitteiden määrittelyssä esiteltiin, tietoturvatutkimusten yhteydessä sosiaalista normia on tutkittu verrattain vähän. Tässä tutkimuksessa tietoturvapolitiikan rinnastusta sosiaaliseen normiin tarkasteltaessa asetettiin muutamia olettamuksia, joita olivat: 1) Työntekijälle ei olettamuksen mukaan tarvitse selittää, mikä merkitys tietoturvapolitiikalla on, eli kun joku asia on itsestään selvä normi, sen merkitystä ei tarvitse selittää. 2) Jos tietoturvarikkomus on sosiaalisesta normista poikkeamista, rikkomuksen seurauksena tekijää vähintäänkin paheksutaan. 3) Normin olemassa oloa vahvistetaan ja säilytetään sillä, että tietoturvarikkomuksiin puututaan välittömästi. 4) Tietoturvapolitiikan noudattaminen hyödyttää työyhteisön jäseniä, jolloin tietoturvapolitiikan noudattaminen tekee työyhteisön jäsenten käyttäytymisestä ennustettavaa. Sosiaalista normia ei siten tämän tutkimuksen tulkinnan mukaan ylläpidetä vain palkkioiden ja rangaistusten avulla. Haastatteluiden perusteella tietoturvapolitiikka ohjeineen määrittelee kyllä vaatimukset, muttei välttämättä ole rinnastettavissa luvussa kolme esiteltyyn sosiaaliseen normiin. Tietoturvakäyttäytymisestä saattaa puuttua kuvailevaan normiin liittyvä ”mitä useimmat muut ihmiset tekevät” sekä velvoittavaan normiin liittyvä ”millainen käyttäytyminen on sosiaalisesti hyväksyttävää ja arvokasta”. Pelkkä tietoisuus vaatimuksista ei välttämättä toimi riittävänä kimmokkeena, vaan saattaa olla, että tarvittaisiin tunne, jolla käyttäytymiseen vaikutetaan. Sosiaalinen normi ei siis vaikuttaisi syntyvän yksinomaan sillä, että esitetään dokumentteja, tai muita muodollisia asioiden käsittelytapoja.

Haastatteluiden perusteella vaikuttaisi sille, ettei tietoturva ole vielä saavuttanut sosiaalisen normin asemaa jota ylläpidettäisiin sosiaalisen kontrollin avulla. Sosiaaliseen järjestykseen liittyvä poikkeavan teon paheksunta niitä kohtaan, jotka eivät noudata hyväksyttäviä tapoja, on tietoturvarikkomusten yhteydessä hankala osoittaa. Tietoturvarikkomusta ei ensinnäkään välttämättä havaita, ja toisaalta rikkomuksen tekijästä saattavat tietää vain pieni, rajattu joukko. Vaikka tuo pieni joukko toimisikin ikään kuin yleisönä, joka arvio tai tuomitsee yksilön toiminnan, tietoturvapolitiikan noudattamattomuuteen ei välttämättä liity suoranaista sosiaalista hylkäämistä tai paheksuntaa. Haastateltavien kohdistama kritiikki organisaation johdon tietoturvakäyttäytymiseen ei yksinään vielä kuvasta sosiaaliseen normiin liittyvää sosiaalista hyljeksyntää ja paheksuntaa. Vaikka tietoturvapolitiikka asettaisikin pakottein tuettavan käyttäytymissäännön, kuten Allardt ja Littunen (1984, 21) sosiaalisen normin määrittelevät, viittaa jo sana sosiaalinen siihen, ettei sosiaalista normia voida asettaa yksittäisellä päätöksellä.

Haastatteluaineiston perusteella säännöt tai ulkoinen paine eivät yksinomaan ohjaa työntekijää. Jos kaikki kielletään, joko kirjallisilla ohjeilla, tai teknisillä rajoitteilla ja valvonnalla, saadaan kyllä luotua pelotteita, ja vaikka muun muassa Hirschin (1969, 291) mukaan voimakkain tunne, joka estää ihmisiä rikkomasta lakeja, on pelko, silti haastateltavien mukaan työn tekemiseen tarvittavien, täysin tavanomaisten asioiden hoitaminen sitoo työntekijän siten, ettei

hänellä ole välttämättä edes aikaa pohtia, onko hän poikkeava, jos ei valitse vahvaa salasanaa ja mitä muut ajattelevat, jos hän jättää salasanan vaihtamatta.

Tietoturvapolitiikka ohjeineen ei välttämättä muodosta uskomusta samassa merkityksessä kuten Sykesin ja Matzan teoriassa esitetty ajatus sisäistettyihin normeihin liittyvästä uskomuksesta. Työntekijä on harvoin vaikuttamassa niihin tietoteknisiin ratkaisuihin, joita käyttää, joten hän ei välttämättä osaa jälkikäteenkään selittää, mitä teki ja miksi. Käyttäjän näkökulmasta esimerkiksi vaihtoehtoisen tavan löytäminen voi olla vain tapa hoitaa työtehtävä loppuun, kuten eräs haastateltava selittää.

> ”Mutta vaihtoehtoinen reitti voi olla yksi tapa, kun en ole tunnistanut mikä muu voisi olla keino. En ole sitä muistaakseni mistään ohjeesta lukenut ja en sitä ohjeistusta niin tarkkaan hallitse, että olisin heti keksinyt, että miten tämä lähtee.”

Tietoturvaohjeet eivät voi olla niin kattavia, että ne pitäisivät sisällään kaikki mahdolliset variaatiot, mitä saa tehdä ja mitä ei saa tehdä, kuten eräs haastateltava tästä mainitsee:

> ”Eihän se olisi edes mahdollista, että joka homma olisi kiellettyä, mitään ei saa tehdä, koska aina tulee joku uusi juttu ja muuta. Mutta onhan joissain ohjeissa varmaan puutteita, ei niihin voi tyhjentävästi laittaa kaikkea, mitä saa tehdä ja mitä ei saa tehdä. Ja joissain saattaa olla mainintoja, että harkinnan perusteella. Että vähän kuitenkin tapauskohtaisesti jotain asioita joutuu tekemään.”

Yhteiskuntaan, yhteisöön tai instituutioon sitoutuminen, vaikka vain osittainenkin, edellyttää silti jonkinasteista kontrollia, joka voi olla virallinen, mutta myös kirjoittamattomat säännöt vaikuttavat käyttäytymiseen. Sykes ja Matzan neutralisoimisteorian mukainen neutralisointi on siis prosessina sekä sosiaalinen että psykologinen (Copes, 2003, 121–124; Topalli, 2018). Yksilö neutralisoi tai järkeistää tekojaan, koska hän on sitoutunut yhteiskuntaan tai sosiaaliseen järjestykseen ja uskoo sen sääntöihin. Psykologisen neutralisoinnista tekee se, että yksilön täytyy ikään kuin käydä sisäistä keskustelua itsensä kanssa päästäkseen eroon häpeästään ja syyllisyydestään tai sääntörikkomuksesta seuranneesta pelosta. (Topalli, 2018.) Yksilön sitoutumisasteen oletetaan vaikuttavan neutralisoinnin määrään ja laatuun siten (Topalli, 2018; 2005, 800), että ilman tavanomaisiin uskomuksiin tai yhteiskunnallisiin normeihin sitoutumista tai seurausten pelkoa, yksilöllä ei ole edes tarvetta neutralisoida mitään (Agnew, 1994; Topalli, 2005, 804). Toisaalta Topallin (2018; 2005, 800) mukaan heikosti sitoutuneet pyrkivät säilyttämään myönteisen minäkuvan yhdenmukaisen ympäristön arvoihin, eivätkä välttämättä heikentääkseen ennakoitua syyllisyyden välttämistä perinteisiä arvoja vastaan. Topallin (2005, 823) mukaan niille, jotka ovat sitoutuneet perinteiseen (sovinnaiseen) yhteiskuntaan, neutralointi antaa heille mahdollisuuden rikkomuksiin luopumatta silti hyvästä (myönteisestä/positiivisesta) minäkuvastaan. Hirschi (1969, 295–296) puolestaan kyseenalaistaa koko neutralisoinnin perusajatuksen, jossa yksilö muodostaisi järkeistämisjärjestelmän tai jon-

kinlaisen ajatusrakennelman perustellakseen tekoja, joihin haluaa sitoutua. Topallin (2018) mukaan heikossa sitoutumisessa neutralisointi toimii, kun taas vahvassa sitoutumisessa neutralisointi ei toimi. Työntekijöiden sitoutuneisuutta kuvaillaan muun muassa näin:

> ”Kyllä se on sen organisaation olemassa olon tarkoitus ja se toimintaympäristö. Sieltä se lähtee.”

> ”Minun mielestä, ja tämä voi kuulostaa kornille, kyse on siitä, mikä on koko organisaation olemassaolon tarkoitus ja siihen liittyvät jutut.”

Eli koko organisaation olemassa olo on erittäin merkittävä motivaattori tietoturvan huomioimiseen. Silti työntekijä voi jättää noudattamatta tietoturvapolitiikassa mainitun salasanakäytänteen, ja kuten eräs haastateltava mainitsi: ”Mutta ei siitä yöunet mene. ”

Topalli (2005, 807) mainitsee, kuinka rikolliset saattavat tuntea suoranaista ylpeyttä toiminnastaan ja taidoistaan. Voiko työntekijä kokea samaan tapaan olevansa nokkela ja kekseliäs osatessaan kiertää tietoturvaratkaisut? Eli syyllisyyden ja häpeän tilalla onkin päinvastainen tunne? Työntekijöiden uteliaisuutta, kekseliäisyyttä ja nokkeluutta kuvastavat haastateltavien mainitsemat ”vaihtoehtoinen reitti” tai ”tämähän toimii”. Nuo muutamat ilmaisut kertovat, että työntekijät etsivät ja usein myös löytävät erilaisia ja vaihtoehtoisia tapoja jonkin asian toteuttamiseksi. Vaikka työntekijät voivatkin kokea ylpeyttä oivaltaessaan, kuinka jonkin tietoturvaratkaisun voi joko kiertää tai sivuuttaa täysin, ei haastatteluista voinut päätellä suoranaista ylpeyttä, vaan enemmänkin vaihtoehtoisen tavan löytäminen oli vain toteamus. Välttämättä se, joka teknisen ratkaisun kehittää, ei tule edes ajatelleeksi sille vaihtoehtoista toimintatapaa. Ihminen on ollut kekseliäs kautta aikojen, ja ilman tuota kekseliäisyyttä, moni tämän päivän arkinen teknologia olisi jäänyt keksimättä.

Topalli (2005, 806–807) esittää ajatuksen, jonka mukaan yksilöllä, jolla on vain vähän yhteyttä muodolliseen valvontaan ja tavanomaisiin normeihin, kuten Topalli mainitsee niin sanotuilla hardcore-rikollisilla olevan, ei yksilölle myöskään synny syyllisyyden ja häpeän tunteita. Tietoturvan yhteydessä tämä tarkoittaisi sitä, että koska työntekijällä on vain vähän mahdollisuuksia vaikuttaa tietoturvaratkaisuihin ja tietoturvapolitiikkaan, sekä yhteyttä siihen, miten valvontaa suoritetaan, tietoturvapolitiikasta ei muodostu normia, eikä työntekijä välttämättä koe syyllisyyttä ja häpeää tekemisistään.

6.4 Selonteot

Sykes ja Matza (1957, 666) viittaavat teoriassaan Robin Williamsiin esittäessään ajatukseen siitä, kuinka normatiivisen järjestelmän joustavuus antaa yksilölle mahdollisuuden sekä moraalisen syyllisyyden että yhteiskunnan asettamien ran-

gaistusten välttämiseen, mikäli tekijä pystyy osoittamaan, että teosta puuttui rikollinen tarkoitus[28]. Suomen kielissä sanat rikos ja rikkomus eivät tarkoita samaa asiaa. Työntekijän tekemästä tietoturvarikkomuksesta saattaa jo lähtökohtaisestikin puuttua rikollinen tarkoitus, tai työntekijä ei ainakaan koe tekevänsä varsinaista rikollista toimintaa rikkoessaan tietoturvapolitiikan mukaisia ohjeita.

Useat organisaatioiden tietoturvapolitiikan mukaiset tietoturvaratkaisut edellyttävät ehdottomuutta. Ehdottomuudella tarkoitetaan tässä yhteydessä sitä, ettei tietoturvapolitiikasta löydy erillisiä mainintoja, määräyksiä tai ohjeita esimerkiksi poikkeustilanteisiin, jolloin tietoturvapolitiikka ei olisi voimassa. Toisaalta tietoturvapolitiikasta ei myöskään löydy rikkomukseen liittyviä lievennysperusteita samaan tapaan kuin esimerkiksi rikoslaissa[29]. Tietoturvapolitiikka ei usein myöskään sisällä Sykes ja Matzan (1957, 667) teoriassa viittaamia tekojen erotteluja ”*mala in se*” ja ”*mala prohibita*”. Vaikka organisaation arvot ja normit ohjaavat työntekijöiden toimintaa, tietoturvan yhteydessä niiden ei useinkaan voi katsoa rajoittuneen sovellettavaksi tiettyyn aikaan, paikkaan, henkilöön tai sosiaaliseen tilanteeseen samaan tapaan kuin Sykes ja Matza (1957, 666) teoriassaan esittävät.

Verrattuna rikollisuuteen, kuten varkauteen, pahoinpitelyyn tai petokseen, tietoturvan yhteydessä työntekijä ei välttämättä koe olevansa henkilökohtaisessa vastuussa siitä, mitä tietojenkäsittely-ympäristössä tapahtuu (ei hyvässä eikä pahassa), koska hän työntekijänä on harvoin päättämässä niistä tietoturvaratkaisuista, joita käyttää. Toisaalta työntekijällä ei myöskään välttämättä ole kykyä arvoida tekojensa seurauksia ja rangaistuksen todennäköisyyttä samaan tapaan kuin yksilö esimerkiksi peloteteorian (engl. *deterrence theory*) keskeisen ajatuksen mukaan toimii.

Kokeeko työntekijä itsensä poikkeavana tai leimataanko hänet poikkeavana, jos hän tekee tietoturvarikkomuksen? Eli hyväksyykö työntekijä ikään kuin sen, että häntä pidetään poikkeavana, mutta hän kieltää täyden vastuun ja esittää puolustuksia vai oikeuttaako työntekijä tietoturvarikkomuksen, jolloin teosta otetaan vastuu, mutta samaan aikaan torjutaan ja vähätellään teon halveksittavaa merkitystä, eli pyritään kieltämään leimautuminen poikkeavaksi? Hirschin (1969, 295) mukaan poikkeavan teon tekeminen tarvitsee vähintään yhtä tehokkaan motivaation kuin moraalisten esteiden antama vastus. Vaikka luvussa neljä esitellyissä aiemmissa tutkimuksissa (Siponen & Vance, 2010; Bauer & Bernroider,

---

[28] ”The normative system of a society, then, is marked by what Williams has termed flexibility; it does not consist of a body of rules held to be binding under all conditions. This flexibility is, in fact, an integral part of the criminal law in that measures for "defenses to crimes" are provided in pleas such such as nonage, necessity, insanity) drunkenness, compulsion, self-defense, and so on. The individual can avoid moral culpability for his criminal action-and thus avoid the negative sanctions of society-if he can prove that criminal intent was lacking. It is our argument that much delinquency is based on what is essentially an unrecognized extension of defenses to crimes, in the form of justifications for deviance that are seen as valid by the delinquent but not by the legal system or society at large.” (Sykes ja Matza, 1957, 666)

[29] ”2) rikokseen johtanut voimakas inhimillinen myötätunto taikka poikkeuksellinen ja äkkiarvaamaton houkutus tai muu vastaava seikka, joka on ollut omiaan heikentämään tekijän kykyä noudattaa lakia;” (Finlex, rikoslaki 13.6.2003/515)

2017; Silic ym., 2017) viitataan neutralisoimisteorian tulkinnoissa siihen, että tietoturvarikkomusten yhteydessä neutralisointi tarkoittaa moraalittoman teon oikeutusta, on Siponen (2001, 309) kuitenkin esittänyt varhaisemmassa julkaisussaan, ettei niin sanottu peruskäyttäjä useinkaan kykene käymään laajaa moraalista pohdintaa tilanteissa, joissa asiaan liittyy tietokone. Terminä moraali ei ole erityisen yksiselitteinen, eikä tämän tutkimuksen tarkoituksena ole ottaa osaa etiikan tutkimusalan erilaisten moraalifilosofian näkökulmien keskusteluun, vaan verrata Sykes ja Matzan teoriassa käyttämiä käsitteitä tietoturvakontekstiin. Moraali kuvastaa niitä jokaisessa yhteiskunnassa olevia sääntöjä, mitä ihmisen tulisi tai ei tulisi erilaisissa tilanteissa tehdä (Quinn, 2015, 79). Muun muassa Mason, Mason ja Culnan (1995, 161) korostivat jo yli 20 vuotta sitten sitä, kuinka tietojenkäsittelyssä työskentelevien on syytä pohtia eettisyyttä suhteessa työnantajiin, asiakkaisiin ja muiden ihmisten oikeuksiin. Eli pohdinnan tarve kohdistettiin enemmän tietojenkäsittelyn ammattilaisiin, eikä niinkään loppukäyttäjiin. Huolimatta siitä, että ihmisen moraalilla on merkitystä myös organisaation tietoturvalle, puuttuu tietoturvakirjallisuudesta edelleenkin teoreettinen perusta yksilön etiikan ja moraalin merkityksestä turvallisuudelle (Siponen, 2001, 312–313). Onkin siis täysin mahdollista, ettei työntekijä välttämättä koe olevansa poikkeava eikä häntä välttämättä leimata poikkeavaksi tilanteessa, jossa hän rikkoo tietoturvapolitiikan ohjeita, määräyksiä ja sääntöjä. Työntekijä ei siis välttämättä koe tekevänsä mitään moraalitonta.

Tietoturvaan liittyvä käyttäytyminen ei välttämättä vielä tänä päivänä ole rinnastettavissa sosiaalisen järjestyksen ja sosiaalisen kontrollin avulla ylläpidettävään sosiaaliseen normiin. Vaikkei työntekijä välttämättä kokisi olevansa poikkeava, eikä ympäristökään leimaisi tietoturvapolitiikkaa rikkovaa työntekijää poikkeavaksi, vaikuttaisi sille, kuten aiemmatkin tietoturvatutkimukset ovat osoittaneet, että tietoturvapolitiikan vastaisia tekoja silti selitetään. Seuraavaksi tarkastellaan näitä, tässä tutkimuksessa selonteoiksi ja perusteluiksi nimettyjä keinoja tehdä omaa tai toisten toimintaa ymmärrettäväksi.

6.4.1 Miten?

Alaluvuissa 6.3.1 – 6.3.5 alkuperäisen neutralisoimisteorian viittä neutralisoimistekniikka verrattiin tietoturvakontekstiin. Alle on poimittu keskeisimmät haastatteluaineistossa esiintyneet perustelut:

- muistin rajallisuus (kykenemättömyys)
- tietämättömyys
- ymmärtämättömyys
- osaamattomuus
- kiire

Edellä esitellyt perustelut häilyvät ikään kuin yleisesti hyväksyttyinä selityksinä tai hyväksyttyjen selitysten jatkeena. Niitä ei tarvitse suoranaisesti oikeuttaa, eikä niitä välttämättä tarvitse edes opettaa, koska niihin liittyy jollain

tapaa inhimillisyys. Esimerkiksi kiireessä ja paineessa ihminen saattaa toimia luontevammin totuttujen tapojensa mukaisesti eikä välttämättä kykene kriittiseen ajatteluun, vaikka toimiikin niin sanotusti tietoisesti. Tällaista psykologista estettä kutsutaan esimerkiksi saatavuusharhaksi, jolloin tutut keinot pysyvät käytössä, eli valintaa ohjaavat tutut elementit. (Mills, Durepos & Wiebe, 2009, 158–159.)

Tietoturvarikkomusten yhteydessä yksilö ei välttämättä perustele toimintaansa sillä, että hänellä on oikeus tehdä jotain, koska hän ei osaa, ymmärrä tai tiedä. Eli hän ei oikeuta toimintaansa. Vaikka neutralisoimisteorian mukaan rikolliset tai poikkeavasti käyttäytyvät tuntevat syyllisyyttä rikkoessaan sosiaalisia normeja vastaan, syyllisyys ja häpeä eivät välttämättä ole hallitsevia tunteita tietoturvapolitiikan noudattamattomuudessa. Neutralisoimisteoriassa yksilö tarkastelee enemmän sitä, mitä on oppinut neutralisoimaan, ja sitä millainen teko on neutralisoitavissa, eikä niinkään sitä, millainen selitys olisi sosiaalisesti hyväksyttävää. Edellä mainitut selitykset eivät kuitenkaan ole täysin ristiriidassa Sykes ja Matzan teoriasta. Kuten Sykes ja Matza (1957, 669) esittävät: "*These "definitions of the situation" represent tangential or glancing blows at the dominant normative system rather than the creation of an opposing ideology; and they are extensions of patterns of thought prevalent in society rather than something created de novo.*" Neutralisoinnit ovat vallitsevan yhteiskunnan ajattelutapoja, eivätkä irrallaan niistä. Yhtä lailla tietoturvarikkomusten perustelut tai selitykset eivät ole irrallaan siitä ympäristöstä, missä niitä tapahtuu. Organisaation viralliset ja epäviralliset normit, säännöt ja menettelytavat määritellään organisaation sisällä. Samassa paikassa määritellään myös, millainen käyttäytyminen on poikkeavaa.

Perusteluna tai selontekona tietämättömyys, ymmärtämättömyys, osaamattomuus, kykenemättömyys tai kiire vaikuttaisivat myötäilevän enemmän Scottin ja Lymanin (1968) esittämää ajatusta ennakoimattoman tai yllättävän käyttäytymisen syistä, jotka ovat sosiaalisesti hyväksyttävämpiä selityksiä kuin Sykes ja Matzan (1957) väite poikkeavuuden oikeutuksesta. Teon rangaistavuus jostain vahinkoa aiheuttavasta teosta siis lievenee tai lievittyy (ainakin suomalaisessa kulttuurissa) pahoittelevilla selityksillä kuten esimerkiksi ”En tiennyt”, ”En ymmärtänyt”, ”En osannut”, ”En muistanut” tai ”En ehtinyt”. Kuten luvussa kolme mainitaan, Scott ja Lyman (1968, 47) jakavat omassa artikkelissaan selonteot oikeuttaviin ja pahoitteleviin. Siinä missä neutralisointi toimii selitysmallina sille, mitä yksilö on oppinut neutralisoimaan tai järkeistämään, pahoittelevassa selonteossa painotus on enemmän siinä, mikä on sosiaalisesti hyväksyttävää. Kuten luvussa kolme viitattiin Suonisen (1997) näkemykseen, selonteko tai perustelu ei välttämättä tarkoita jonkin asia olevan selvä, vaikka tekoon liitetään ikään kuin järjellinen selitys ja vastuun lieventäminen. Edellä mainittuihin selontekoihin liittyy pyrkimys osoittaa, että teosta puuttuu tarkoituksellisuus ja suunnitelmallisuus.

Vaikka esimerkiksi salasanojen muistamattomuus voisikin olla organisaatiossa opittu selitys, muistin rajallisuuden syyksi on hankala osoittaa ulkopuolista, itsestä riippumatonta tekijää. Sykes ja Matzan (1957, 666) teoriassa mai-

nittu ”*the blame of others after the act*” ei siten välttämättä liity tietoturvarikkomuksiin samaan tapaan kuin rikoksiin. Huolimatta siitä, että tietoturvapolitiikan joustamattomuus voisi toimia Sykes ja Matzan teoriaan rinnastettavana selityksenä siitä, että ulkopuoliset tekijät vaikuttivat tekoon, silti selontekona kykenemättömyys tai muistin rajallisuus vaikuttaisivat myötäilevän enemmän Scottin ja Lymanin (1968, 48) esittämää ajatusta, jonka mukaan yksilö vetoaa johonkin mentaaliseen tekijään. Haastatteluissa näitä ilmaisuja olivat esimerkiksi ”ei pysy mielessä” tai ”ei ihminen pysty siihen”. Vastuun ja vahingon vähättelemiseen voidaan Scottin ja Lymanin (1968, 48) esittämän mukaan käyttää puolustusta esimerkiksi puutteellisista tiedoista. Henkilö välttelee vastuuta sillä, että tiettyjä tietoja ei ollut saatavilla, jotta hän olisi voinut muuttaa käyttäytymistään. Toisaalta teon vakavuutta on mahdollista vähätellä sekä tietämättömyyteen, ymmärtämättömyyteen että osaamattomuuteen vedoten, eli henkilö voi käyttää selitystä siitä, ettei tiennyt tai osannut edes ajatella aiheuttavansa mitään vakavaa. Haastatteluissa näitä kuvaavia ilmaisuja olivat esimerkiksi ”kun olen maallikko käyttäjä” tai ”en edes tiedä tai ole varma”.

Sykesin ja Matzan (1957, 669) teorian vetoaminen korkeampiin lojaliteetteihin –neutralisoimistekniikka tuo kyllä esille sen, että tietyssä tilanteessa yksilö priorisoi lojaliteettiaan, muttei tarkemmin käsittele sitä, mikä tietyssä tilanteessa saa aikaan tuon priorisoinnin. Tutkimusaineisto antaisi viitteitä siitä, että yksilön priorisointi olisi sidonnainen selontekoon ”kiire”. Kiireisen tilanteen johdosta tehdyssä tietoturvarikkomuksessa vaikuttaisi olevan mahdollista käyttää myös selontekoa ”kykenemättömyys”. Haastatteluissa näitä kuvaavia ilmaisuja olivat esimerkiksi ”tukehtuu siihen massaan” ja ”nykyisellä työrytmillä tehdään asioita”. Nämä kuvastavat kykenemättömyyttä joko omaksua jotain asiaa tai ennättää tehdä jotain asiaa. Kaikki edellä esitellyt haastatteluista nousseet selonteot, eli kykenemättömyys, tietämättömyys, ymmärtämättömyys ja osaamattomuus, saattavat esiintyä itsenäisenä selontekona. Yksilön selonteko kuvastaa sitä, että häneltä ikään kuin puuttuu kyky hallita tilannetta. Tällaiseen selontekoon voi liittyä edellä mainittu ”*the blame of others after the act*”, vaikkei sillä voitaisikaan osoittaa ketään yksittäistä henkilöä tai ryhmää, vaan syytös suuntautuu tilanteeseen. Sykes ja Matzan (1957, 666) teoriassa mainitut yksilön käyttämät perustelut ”välttämättömyys” ja ”pakko” esiintyivät haastatteluissa. Haastatteluaineistossa edellä mainitut ilmaisut esiintyivät kuvailtaessa kiireistä tilannetta, joihin ei liittynyt syyllisyyden ja häpeän tunteita. Siten kumpikaan perustelu irrallaan muista neutralisoimisteorian olettamuksista ei välttämättä viittaa oikeuttamiseen.

Sekä Topalli (2018) että Copes (2003, 121–124) ovat esittäneet neutralisoinnin olevan prosessina psykologinen siten, että yksilön on käytävä ikään kuin sisäinen keskustelu itsensä kanssa päästäkseen eroon häpeästään ja syyllisyydestään tai sääntörikkomuksesta seuranneesta pelosta. Se, että yksilö oikeuttaa itsensä tekemään jotain, edellyttää jollain tapaa tietoista pohdintaa, joka voi, kuten Sykes ja Matza (1957, 666) esittävät, tapahtua joko ennen tai jälkeen teon. Tietoturvarikkomuksen yhteydessä tuota teon suunnitelmallisuutta ja sisäistä keskus-

telua ei välttämättä käydä. Työntekijä ei siis välttämättä käy itsensä kanssa keskustelua, jossa selittää itselleen, ettei ymmärrä, pysty, osaa tai ehdi. Teon oikeutuksessa perustelu suuntautuu itsestä poispäin ("*the blame of others after the act*"), ja vaikka selonteossakin perustelu vaikuttaisi seuraavan tekoa, silti perustelu vaikuttaisi suuntautuvan enemmän tekijään itseensä kuin itsestä poispäin. Tekoon ei välttämättä liity samaan tapaan ennakointia kuin Sykes ja Matzan (1957) teoriassa, jossa neutralisointi voi edeltää tekoa.

Scott ja Lyman (1968, 47) ovat esittäneet oikeuttavien ja pahoittelevien selontekojen tai selitysten eroksi myös sen, että oikeuttavassa selonteossa henkilö myöntää olevansa vastuussa, mutta kiistää teon halveksuttavuuden. Kuten Sykes ja Matza (1957, 667) teoriassaan esittelevät, tekijä kokee, että jos teko ei nyt niin oikein ollutkaan, se on silti hyväksyttävää. Pahoittelevassa selonteossa tekijä puolestaan myöntää teon olleen väärä tai epäasianmukainen, mutta kiistää täyden vastuun teosta (Scott & Lyman, 1968, 47). Haastatteluiden perusteella työntekijät eivät koe olevansa täysin yksin (henkilökohtaisessa) vastuussa siitä, jos eivät osaa, tiedä, ymmärrä, muista tai ehdi.

6.4.2 Miksi?

Sykes ja Matzan teoria luotiin sekä erilaiseen ympäristöön että myös erilaiseen ajanjaksoon kuin tämän päivän sosiotekninen ympäristö. Kuten Maruna ja Copes (2005, 224) sekä Topalli (2005, 824) esittävät, muun muassa suhtautuminen auktoriteetteihin on muuttuneet siitä, kun ensimmäinen neutralisoimisteoria hahmoteltiin. Vaikuttaisi sille, ettei tietoturvapolitiikka yhdessä tietoturvan kanssa ole, tärkeydestään huolimatta, saavuttanut samankaltaista auktoriteetin asemaa kuin mitä Sykes ja Matza teoriassaan kuvailevat, eli lakeja, joihin uskotaan, rikotaan silti. Myös muun muassa Dhillonin ym., (2016) mainitsema sosiotekninen ympäristö, jossa ihminen ja teknologia muovaavat toisiaan, on ympäristönä muuttunut paljon Sykes ja Matzan teorian luomisen ajasta. Tuo muutos on osaltaan muokannut myös selontekoja. Tietoturvan näkökulmasta sosioteknisen ympäristön muutos näyttäytyy siten, että tietoturvarikkomuksissa tai –loukkauksissa sekä organisaation tekninen infrastruktuuri ympäristöineen että sosiaalinen ympäristö muodostavat yhdessä huomioon otettavan, mutta monimutkaisen kokonaisuuden (Dhillon ym., 2016).

Tietoturvapolitiikka ja tietoturvakulttuuri luovat käyttäytymismalleja siitä, miten tulisi toimia. Vaikka edellä esiteltiin tietoturvarikkomusten pahoittelevia selontekoja, joiden tarkoitus viittaisi enemmän sosiaalisesti hyväksyttävään selitykseen kuin oikeutukseen, vaikuttaisi silti sille, ettei tietoturvakäyttäytymiseen välttämättä liity täysin samankaltaista sosiaalisesta ympäristöstä haettavaa hyväksyntää kuin esimerkiksi perustellun toiminnan teorian tai suunnitelmallisen käyttäytymisen teorian mukaisesti esitetään.

Ausubel (1955) on artikkelissaan esittänyt sekä syyllisyyteen että häpeään liittyviä määritelmiä. Syyllisyys viittaa käsitteenä yksilön kokemaan negatiiviseen tunteeseen siitä, että hänen käyttäytymisensä on ristiriidassa moraalisten arvojen kanssa, joita hän kokee olevansa velvollinen noudattamaan. Syyllisyyden tunne ei ole ihmisen syntymälahja, vaan se kehittyy kulttuurin mukaisesti.

Yksilön on hyväksyttävä omassa kulttuurissaan olevat tietyt oikean ja väärin, hyvän ja pahan niin sanotut standardit omakseen. Yksilön on myös hyväksyttävä käyttäytymisen säätelyyn liittyvä velvollisuus siten, että hän noudattaa standardia. Lisäksi yksilöllä on oltava niin sanottu itsekriittinen kyky tunnistaa, milloin käyttäytymisen ja arvojen välille muodostuu ristiriita. (Ausubel, 1955, 378–379.) Häpeä viittaa käsitteenä yksilön kokemaan epämiellyttävään tunnereaktioon toisten ihmisten joko todellisesta tai oletetusta kielteisestä arvioinnista, joka alentaa yksilön arvoa suhteessa ryhmään. Tällainen tunne voi olla esimerkiksi ”kasvojen menetys”. (Ausubel, 1955, 379.) Ausubelin (1955, 382) mukaan häpeä on vain yksi syyllisyyden osa, johon sisältyy jonkinlainen ulkoinen tuomio ja seuraamus. Syyllisyyttä taas voidaan kokea riippumatta toisten tuomitsevuudesta tai reaktioista. Ausubelin (1955, 378) määritelmässä mainitaan lisäksi, ettei käyttäytymistä voida hallita yksinomaan pelolla, fyysisellä voimalla, rangaistuksilla, hyväksynnän pidättäytymisellä tai jatkuvalla valvonnalla, vaan tunteena syyllisyys on yksi tärkeimmistä psykologisista mekanismeista, jonka kautta yksilö sosiaalistuu kulttuurinsa tavoille ja auttaa yksilöä sovittamaan käyttäytymisensä yhteiskunnan moraalisten arvojen kanssa yhteen. Kuten jo aiemmin mainittiin, tutkimusaineisto antaa viitteitä siitä, ettei tietoturva ole saavuttanut sosiaalisen normin asemaa, jota ylläpidettäisiin sosiaalisen kontrollin avulla. Vaikka työntekijä selittää tietoturvarikkomuksiaan, vaikuttaisi sille, ettei niiden päällimmäinen tarkoitus on poistaa syyllisyyden ja häpeän tunteita.

Osittain vaikuttaisi myös sille, että vaikka tietoturvapolitiikan joustamattomuus ei toimisikaan suoraan syynä tietoturvarikkomuksiin, se voi kuitenkin edesauttaa selontekoa. Hyvää tarkoittavat, mutta vaikeaselkoiset, puutteelliset ja päivittämättömät ohjeet, säännöt ja määräykset voivat jopa pahentaa ongelmaa, jota niillä halutaan torjua. Jos käyttäjä törmää liian usein päivittämättömiin, tai epäselviin ja puutteellisiin ohjeisiin, joita ei ole edes mahdollista käytännössä noudattaa, saattavat erilaiset ohjeet vähitellen menettää arvostuksensa. Toisaalta se, että kiiretilanteessa tietoturvaohjeen voi kuitenkin joko sivuuttaa tai kiertää, antaisi viitteitä siitä, ettei tietoturvapolitiikan mukainen ohje tai tietoturvaratkaisu palvele täysin tarkoitustaan.

Sykes ja Matza (1957, 667) viittaavat siihen, kuinka useat rikolliset osoittavat olevansa täysin tietoisia sosiologisista ja psykologisista selitysmalleista. Kuten Suoninen (1997) esittää, selonteot myös rakentavat kulttuuria. Suoninen (1997) esittää myös ajatuksen siitä, kuinka henkilö voi ikään kuin valikoida sosiaalisesti mahdollisimman sopivan normin toimintansa perusteeksi. Tällöin sopivia selontekoja on mahdollista käsitellä jo aloitetun teon tai toiminnan suhteuttamiseksi kulloiseenkin sosiaaliseen ympäristöön. Vaikka tutkimusaineistosta nousi esille eriäviä kokemuksia siitä, voiko kiire olla todellinen vai ei, vaikuttaisi silti, että selontekona kiireestä on saattanut tulla sosiaalisesti hyväksytty selitysmalli etenkin silloin, kun sitä käytetään työtehtävistä suoriutumisen perusteluna.

Siinä missä neutralisoinnit vähintäänkin myötäilevät yhteiskunnan vallitsevia ajattelutapoja, selonteot lienevät sikäli kulttuurisidonnaisia, että ne on jol-

lain tapaa opittava sosiaalisen vuorovaikutuksen kautta, koska jokaisessa kulttuurissa on omat hyväksyttävät selityksensä. Suoninen (1997) esittääkin artikkelissaan:

> ”Sellaisissa tilanteissa, joissa on verrattain tasaväkisiä perusteluvaihtoehtoja erilaisille teoille, yksilön - tai ainakin yksilöllisiltä näyttävillä - valinnoilla lienee eniten merkitystä. Normaalin ja selittelyä edellyttävän toiminnan rajan määrittely on ennen kaikkea yleisön - keskustelukumppanin, kanssatoimijan tai toiminnan seuraajan - asia.” (Suoninen, 1997)

7 KESKUSTELU

Tässä luvussa tarkastellaan tutkimuksessa esiin tulleita tuloksia sekä teorian että käytännön näkökulmasta. Lisäksi luvussa tarkastellaan tutkimuksen luotettavuutta ja pätevyyttä sekä esitellään suosituksia jatkotutkimuksille.

7.1 Tulosten merkitys ja suhteutus

Tutkimuksen tavoitteena oli monipuolistaa tietoturvatutkimusta ja tuoda uutta tietoa työntekijöiden tietoturvarikkomusten selonteoista sekä niihin liittyvästä hyväksynnästä. Nämä tutkimukselle asetetut tavoitteet saavutettiin. Tutkimuksella on sekä teoreettisia että käytännön vaikutuksia. Tutkimuksen tärkeimpänä kontribuutiona esitetään neutralisoimisteorian ja aiempien tutkimusten kriittinen tarkastelu sekä aiemmista tutkimuksista poikkeava näkemys tietoturvarikkomusten selontekoihin. Edellä mainittuihin peilaten, tutkimus tuo uuden ja erilaisen näkökulman tietoturvarikkomusten perusteluihin.

Tutkimuksessa esitetyt havainnot haastavat sen, että neutralisoimisteoria ja sen keskeiset oletukset selittäisivät työntekijöiden tietoturvarikkomuksia. Vaikka aiemmat neutralisoimisteoriaa tietoturvakontekstissa soveltaneet tutkimukset ovat esittäneet neutralisoimisteorian soveltuvan selittämään tai ennustamaan yksilön todellista tai aiottua käyttäytymistä paremmin kuin rangaistuksiin (sanktioihin) perustuvat teoriat, on tämän tutkimuksen väitteenä, etteivät työntekijät välttämättä hyödynnä neutralisoimisteoriassa esitettyjä neutralisoimistekniikoita ja oikeuta siten niiden avulla tietoturvarikkomuksiaan.

Tämä tutkimus esittää viisi perustelua (kykenemättömyys, tietämättömyys, ymmärtämättömyys, osaamattomuus ja kiire), joiden avulla työntekijät selittävät tietoturvarikkomuksiaan. Jos tietoturvarikkomusten syinä olisi se, että työntekijät oikeuttaisivat niitä, tarkoittaisi se samalla sitä, että neutralisoimistekniikat opitaan organisaatiossa vuorovaikutuksessa toisten työntekijöiden kanssa. Tutkimuksessa esiteltyjä viittä perustelua ei kuitenkaan tarvitse erityisesti opettaa.

Jos työntekijät oikeuttaisivat Sykes ja Matzan teorian mukaisesti tietoturvarikkomuksiaan, se tarkoittaisi samalla sitä, että työntekijöiden tietoturvaan liittyvän osaamisen olisi oltava vähintäänkin sillä tasolla, että työntekijä kykenisi arvioimaan myös tekojensa lopulliset seuraukset. Tutkimusaineisto antaa kuitenkin viitteitä siitä, etteivät työntekijät välttämättä omaa tosiasiallista tietämystä tietoturvarikkomusten seuraamuksista. Eivät siis teon rangaistavuuden ja/tai teon seurannaisvaikutusten vakavuudesta.

Työntekijöiden selonteoissa viittaukset kykenemättömyyteen, tietämättömyyteen, osaamattomuuteen, ymmärtämättömyyteen ja kiireeseen antavat myös viitteitä siitä, etteivät työntekijät koe olevansa yksin vastuussa tietoturvarikkomuksistaan. Se, ettei tietoturva vaikuttaisi, tärkeydestään huolimatta, saavuttaneen vielä tänä päivänä sosiaalisen normin asemaa ei kuitenkaan välttämättä tarkoita, että työntekijät suhtautuisivat aiheeseen välinpitämättömästi. He eivät välttämättä vielä ole täysin paikantaneet itseään tämän päivän monimutkaisiin tietojenkäsittely-ympäristöihin ja sisäistäneet omaa tärkeää rooliaan organisaatioon tieto- ja kyberturvaan kohdistuvien riskien minimoimisessa. Koska elämme aikakautta, joka korostaa yksilökeskeisyyttä, saattaa yksikön tietoturvakäyttäytymisestä puuttua muun muassa Parsonsin (1968, 75) normin määritelmässä esitetty ymmärrys siitä, että normin aikaansaamien yhteisten toimintatapojen tavoitteena on lopulta hyödyttää kaikkia ryhmän jäseniä.

Vaikka muun muassa Siponen ja Vance (2010, 495) sekä Cheng ym., (2014, 226) toteavat tutkimustuloksissaan neutralisoinnin olevan merkittävä ennustaja työntekijöiden tietoturvarikkomusten aikomuksissa, silti molemmissa tutkimuksissa mittauskohteet, jotka on esitelty luvussa neljä, viittaisivat enemmän ymmärtämättömyyteen tai tietämättömyyteen liittyviin selityksiin kuin oikeutukseen. Näin ollen edellä mainitut mittauskohteet tukevat tässä tutkimuksessa esitettyä havaintoa.

Sykes ja Matzan (1957) teorian antaa ymmärtää, ettei yksilö tarkastele niinkään sitä, mikä on sosiaalisesti hyväksyttävää, vaan sitä, mitä on mahdollista neutralisoida tai mitä on oppinut järkeistämään. Selonteot, joihin liittyy jotain inhimillistä, vaikuttaisivat olevan helpommin sosiaalisesti hyväksyttäviä kuin neutralisoimistekniikoilla avulla tai niiden kautta hyödynnettävät oikeuttamiset. Selontekona vetoaminen kiireeseen ei kuitenkaan vaikuttaisi saavan samankaltaista hyväksyntää. Kuten eräs haastateltava esitti: ”Missään ei lue, että vähän voi rikkoa lakia, jos on kiire.” Tietoturvapolitiikka ei kuitenkaan ole rinnastettavissa lakiin. Vaikka selontekona kiire herättää toisistaan eriäviä tunteita ja ajatuksia, vaikuttaisi silti sille, että selontekona kiire on sosiaalisesti hyväksyttävä tilanteessa, jossa työntekijä pyrkii edistämään organisaation toiminnan jatkuvuutta. Tilanne on ikään kuin poikkeuksellinen eikä pitkäkestoinen, joten se ei välttämättä lisää teon ennustettavuutta. Kuitenkin selontekona kiire vaikuttaisi hakevan sosiaalisen ympäristön hyväksyntää enemmän kuin muut aiemmin mainitut selonteot. Selonteot, joihin liittyy inhimillisyys, koetaan ymmärrettävinä ja anteeksi annettavina, vaikkakin ne toimisivat vain tekoselityksinä. Yksilön päätöksentekoprosessit, kun voivat vaihdella sosiaalisesta ympäristöstä riip-

puen (Piquero, Tibbetts & Blankenship, 2005, 162), joten esimerkiksi päätös noudattaa työpaikalla organisaation määräaikoja rikkoen silti samalla tietoturvapolitiikan mukaisia ohjeita ei välttämättä ole samankaltainen valintatilanne kuin esimerkiksi liikennelain rikkominen. Selontekona kiire ei ole yhtä yksiselitteinen kuin vaikkapa tietämättömyys, koska kiire vaatii usein parikseen lisäosan ”kiire, koska...”. Muun muassa Karjalainen ym., (2019, 693) kirjoittavat, kuinka työntekijän pyrkimys vastata kiireellisiin pyyntöihin ja nopeasti muuttuviin tilanteisiin, jolloin he tekevät työn tietoturvapolitiikan ohjeita rikkoen, tuottaa välittömiä etuja organisaation toiminnalle, mutta pitkällä aikavälillä toiminnasta saattaa koitua negatiivisia seurauksia. Selontekona ”kiire” vaatisi tarkempaa tutkimusta, jolla konkretisoitaisiin muun muassa kiireen luomien etujen ja haittojen suhdetta.

Sykesin ja Matzan (1957) teoriassa syyllisyyden ja häpeän tunteet ikään kuin ohjaavat yksilön toimintaa. Tunteet kuvataan teoriassa niin voimakkaina, että yksilö suojelee neutralisoinnin avulla itseään omilta itsesyytöksiltään. Vaikka kykenemättömyyteen, tietämättömyyteen, osaamattomuuteen, ymmärtämättömyyteen ja kiireeseen saattaa liittyä yksilön kokemaa häpeää, vaikuttaisi sille, ettei tietoturvarikkomuksiin liity yhtä voimakkaita tunteita, kuin miten Sykes ja Matza teoriassaan kuvailevat. Vaikka työntekijät olisivat joko rationaalisesti tai tunnepohjaisesti sitoutuneita organisaation toimintaan, suhde tietoturvapolitiikkaan ja sen ohjeisiin saattaa silti jäädä etäiseksi. Myöskään aiemmat, luvussa neljä esitellyt, neutralisoimisteoriaa soveltaneet tietoturvatutkimukset eivät ole kyenneet osoittamaan syyllisyyden ja häpeän sidosta tietoturvarikkomuksiin.

Tutkimuksessa käsitellään myös tietoturvakäyttäytymiseen liittyvää yhdenmukaisuuden vaatimusta, eli tietoturvapolitiikka ohjeineen koskee kattavasti kaikkia organisaation tietojärjestelmiin käyttöoikeuden omaavaa. Haastatteluihin osallistuneet työntekijät eivät kuitenkaan ole yksi yhtenäinen joukko. Saman työnantajan palveluksessa olevat ovat teknisiltä taidoiltaan erilaisia, heidän työtehtävänsä ovat erilaisia ja heidän suhtautumisensa tietoturvaan on erilainen. Vaikka aiemmissa saman aihepiirin tutkimuksissa tutkimusten otantaan on osallistunut työntekijöitä eri ammattiryhmistä, ei aiemmissa tutkimuksissa ole juurikaan kiinnitetty huomiota siihen, kuinka organisaatiot pitävät sisällään DaVeigan ja Martinsin (2017) nimittämää kahta alakulttuuria. Tämän tutkimuksen tulos viittaa siihen, että tuolla kaksijakoisuudella on merkitystä suhtautumisessa tietoturvapolitiikkaan.

Sitoutuneisuus organisaation saattaa vaikuttaa siihen, että työntekijä haluaa toimia organisaation tavoitteiden mukaisesti. Tutkimuksen tulos viittaisi siihen, että organisaatioon sitoutunut työntekijä jaksaa ajoittaisen tietoturvaratkaisuista aiheutuvan turhautumisen. Sitoutuneisuus ei kuitenkaan poista ”räätälöidyistä” virheilmoituksista, yhteysongelmista tai muista ongelmista johtuvaa ärtymystä ja turhautuneisuutta.

7.2 Keskustelu käytännön kannalta

Tieto- ja kyberturvaan kohdistuvat uhkat muuttuvat ja muuttavat muotoaan, eikä ole olemassa yksinkertaista ja nopeaa ratkaisua, jolla jokainen käyttäjä kokisi tietoturvan aiheena omakseen. Vaikka työntekijöillä löytyisi tietokoneen lisäksi myös reipasta mieltä, myötäillään tässä tutkimuksessa Vroom ja Von Solms (2004, 195) esittämää realiteettia siitä, kuinka tietoturvakulttuuri, jossa organisaation työntekijät seuraisivat organisaatio ohjeita yhtä vapaaehtoisesti kuin se olisi heidän toinen luontonsa, on ajatuksena utopistinen. Tutkimustuloksen perusteella on kuitenkin mahdollista ehdottaa, kuinka selontekoja voi vähintääkin haastaa, ellei jopa torjua.

Tieto- ja kyberturva eivät merkitse kaikille ihmiselle samaa asiaa. Muun muassa moniammatillisissa organisaatioissa työtehtävät, asema ja koulutus vaikuttavat niin asenteisiin kuin käytännön työtehtävien hoitamiseen. Toisaalta tietoturva on erilainen eri organisaatioissa. Vroomin ja Von Solmsin (2004, 192) ajatusta myötäillen, tietoturvapolitiikan suhteen on syytä varmistaa, että organisaation säännöt ja määräykset todellakin ovat organisaation etujen mukaisia. Hyvää tarkoittavat ohjeet, säännöt ja määräykset voivat jopa pahentaa ongelmaa, jota niillä halutaan torjua. Toisaalta liiallinen tietotulva turruttaa vähitellen eivätkä tietoturvapolitiikan mukaiset ohjeet, määräyksen, säännöt ja käskyt rakenna tietoturvakulttuuria, jolla tietoturvasta voisi muodostua sosiaaliseen normiin rinnastettava itsestäänselvyys. Kuten jo luvussa kolme mainittiin, tietoturva on organisaation aktiivista toimintaa. Se tarkoittaa samalla myös sitä, että tietoturvaan liittyvät ohjeet eivät ole kertaluoteisesti tehtyjä, vaan nekin vaativat jatkuvaa uudelleen tarkastelua ja päivittämistä. Muun muassa tekniikka, lainsäädäntö ja maailman tilanne voivat muuttua nopeasti ja vaikuttaa myös organisaation tietoturvatoimintaan.

Ilman konkreettisia tietoturvan noudattamiselle ja tietoturvatietotietoisuudelle asetettuja selkeitä tavoitteita, tietoturvapolitiikka ohjeineen saattaa jäädä käyttäjälle vain niin sanotuksi sanahelinäksi. Konkreettisuudella tarkoitetaan tässä yhteydessä sitä, että tietoturvan ”miten” ja ”miksi” selitetään käyttäjille sekä koulutuksen että ohjeistuksen kautta. Pelkkä tietoturva syihin vetoaminen ei välttämättä selitä käyttäjälle, miksi ja miten hänen tulee noudattaa ohjeita. Vaikka Adamsin ja Sassen (1999) julkaisemasta artikkelista on kulunut jo yli kaksi vuosikymmentä, osittain vaikuttaisi sille, että Adamsin ja Sassen (1999, 4) esittämä näkemys ei ole vuosikymmenissä muuttunut. Turvallisuuteen liittyy oppi tai oletus siitä, että tiedon saatavuuden rajaaminen lisää turvallisuutta, koska mitä enemmän tietoturvamekanismeja tietää, sitä helpompi on kohdistaa myös hyökkäys niitä vastaan (Adam & Sasse, 1999, 4). Vaikka eräs tietoturvan kulmakivistä onkin edelleen se, ettei kaikki tieto kuulu kaikille, tutkimustuloksen perusteella voidaan kuitenkin ehdottaa, että työntekijöille tulisi havainnollistaa heidän omien käytännön työtehtäviensä kautta, mitä konkreettisesti tapahtuisi, jos hän ei noudata tietoturvapolitiikkaa ja miten heidän toimintansa vaikuttaa koko organisaation toimintaan. Jos siis käyttäjä on niin suuri tietoturvauhka,

ettei hänelle voida selittää käytännön tasolla, mitä tapahtuu, mikäli hän ei noudata organisaation tietoturvapolitiikan mukaisia ohjeita, määräyksiä ja sääntöjä, ei uhka välttämättä vähene kertomatta jättämisellä. Vaikka Hirsch (1969, 291) mainitsee, kuinka voimakkain tunne, joka estää ihmisiä rikkomasta lakeja, on pelko, saattaa pelottelu kääntyä tietoturvan yhteydessä organisaatiota vastaan. Jos pelko siis estää toimimasta tietyllä tavalla, yhtä lailla rangaistuksen pelko voi estää kertomasta tekemistään virheistä. Kuten Barlow ym., (2018, 701) esittävät, työntekijöille tulisi korostaa syitä, miksi tietoturvakäytännöt ovat olemassa. Jos työntekijä ei edes tiedä, mitä ei tiedä, ei hänen silloin voida olettaa ymmärtävän, millaiset seuraukset hänen ymmärtämättömyydellään ja tietämättömyydellä on tai voi olla.

Vaikka tietoturvakoulutusten pyrkimyksenä onkin tietoturvatietoisuuden lisääminen ja tehostaminen, ne eivät ole tehokkaita estämään tahallista tietoturvallisuuden vaarantamista, eli koulutus ei vaikuta heihin, jotka ovat jo valmiiksi motivoituneita vaarantamaan organisaatiota (Crossler ym., 2013, 92). Mikään tietoturvakoulutus tuskin voi tavoittaa ajoissa niitä, jotka haluavat tarkoituksellisesti vahingoittaa organisaation tietoturvaa, vaan keinot on etsittävä jostain muualta. Vaikeutena onkin havaita, ilman valvontaa, ne jotka näin toimivat, koska he eivät halua tulla havaituiksi. Yhtä lailla kuin Suthelandin mukaan rikollisuus opitaan vuorovaikutuksessa toisten ihmisten kanssa, samoin oikeat toimintatavat on mahdollista oppia vuorovaikutuksen kautta. Verkossa tapahtuva oppiminen ja itseopiskelu ovat tämän päivän arkea. Tietoturvan sisäistäminen pelkkiä sääntöjä tai ohjeita lukemalla, verkkokoulutuksena tai itseoppimalla yrityksen ja erehdyksen kautta eivät tämän tutkimuksen perusteella näyttäisi täysin tukevan tietoturvatyötä. Tietoturvan merkityksen sisäistäminen saattaa edellyttää olemassa olevien menetelmien muuttamista. Vaikka Ausubel (1955, 378) esittää, ettei käyttäytymistä voida hallinnoida yksinomaan pelolla, rangaistuksilla tai valvonnalla, silti tietoturvapolitiikan noudattaminen ei saa perustua vapaaehtoisuuteen. Onkin johdon ja esimiesten tehtävänä tuoda selkeästi esille, että tietoturvakäyttäytymiseen liittyy valvonta. Se ei kuitenkaan tarkoita, että tietoturvakäyttäytymistä tulisi ohjata ja hallita vain pelolla, rangaistuksilla tai valvonnalla, vaan enemmänkin sitä, että valvonnan avulla vääränlaisiin toimintatapoihin voidaan puuttua välittömästi ja pyrkiä löytämään ongelman ydin.

Jotta työntekijät eivät voi perustella tietoturvarikkomuksiaan erilaisilla selonteoilla, on myös syytä kiinnittää huomiota, millaisia käyttäytymismalleja organisaatio suosii. Vaikka tietoturvan rinnastaminen sosiaaliseen normiin olisi vielä pitkän matkan päässä, myötäillään tässä kohdassa Keizer, Lindenberg ja Steg (2008, 1681–1682) esittämää ajatusta, jonka mukaan käyttäytymismalli voi kopioitua enemmän siitä syystä, että tietyn toiminnan ajatellaan olevan suositeltavaa, eikä niinkään sen vuoksi, että käyttäytymismallin noudattaminen olisi velvollisuus tai siihen liittyisi sosiaalinen paine. Tutkimustulos antaa viitteitä, että useat käyttäjät haluisivat luottaa organisaation tietoturvaratkaisuihin kuin bussikuskiin, joka vie perille ilman, että käyttäjän tarvitsee itse tehdä ylimääräistä

tietoturvan eteen. Jokainen organisaatio pitää sisällään omat hyväksyttävät tapansa toimia, joten organisaatioissa onkin syytä herättää avointa keskustelua siitä, mistä työntekijä ottaisi mallia tietoturvakäyttäytymiseen.

Kuten luvussa kaksi mainitaan, Sykesin ja Matzan mukaan arvot ja normit näyttäytyvät pikemminkin toimintaa ohjaavana ja rajoittuneena sovellettavaksi tiettyyn aikaan, paikkaan, henkilöön tai sosiaaliseen tilanteeseen. Tietoturvassa tällaista joustavuutta ei välttämättä voi olla. Tietoturvapolitiikan ehdottomuuden kääntöpuolella on se, että tietoturvapolitiikkaan liittyvien ohjeiden on oltava ensinnäkin ymmärrettäviä, eli ne on kirjoitettava käyttäjän ymmärtämällä kielellä ja siten, että käyttäjä voi noudattaa niitä. Lisäksi ohjeiden on oltava jatkuvasti ajantasaisia sekä helposti ja nopeasti löydettävissä. Onkin suositeltavaa informoida käyttäjiä ohjeisiin tulleista muutoksista ja esimerkiksi mahdollisista muuttuneista osoitepoluista. Näin voidaan välttyä tietämättömyyden selonteolta.

Kuten luvussa kolme esiteltiin 10 niin sanottua kuolemansyntiä, joista ensimmäinen on se, että tietoturva on organisaation ylimmän johdon vastuulla. Vastuu ei siis ole jaettu, jolloin vaarana on, että jaettu vastuu on ei-kenenkäänvastuu. Loppukäyttäjien vastuulla taas on se, että he toimivat annettujen ohjeiden mukaisesti. Eräs tutkimukseen haastatelluista esitti: ”Alkaa olla jo klisee se johdon sitoutuminen turvallisuuteen.” Baskerville (1991, 123) on todennut, kuinka tyypillisesti tietoturva on johdon alhaisella prioriteetilla siihen asti, että jotain katastrofaalista tapahtuu. Silti on väitetty, että johdon käytännöt voivat olla tehokkaampia vähentämään tietoturvaloukkauksia kuin monet tekniset ratkaisut (Buss & Salerno, 1984). Vaikka sanonta turvallisuuteen sitoutuneesta johdosta tuntuisi vanhentuneelta, silti tänäkin päivänä organisaation johto määrittelee organisaation strategiset linjaukset, jolloin ilman ylimmän johdon sitoutumista, ei tietoturvakaan rakenneta. Vain erittäin harvalla eheyden, saatavuuden ja luotettavuuden turvattava tieto on identtinen jonkin toisen organisaation kanssa. Organisaation ylimmän johdon tehtävänä on määritellä organisaation strategian ja toiminnan kannalta keskeisimmät ja tärkeimmät turvattavat tiedot. Myöskään toimintaprosessit eivät välttämättä ole yhtäläisiä, joten tietoturvan tarve, merkitys ja toteuttamisen keinot eivät ole identtiset organisaatiosta toiseen. Tänä päivänä tietotekniikka on valjastettu niin kattavasti yhteiskunnan ja eri organisaatioiden käyttöön, ettei moni asia edes toimi ilman tietotekniikkaa. Siellä missä on tietotekniikkaa, siellä on otettava huomioon myös tietoturva, jonka kehittäminen ja ylläpito vaativat toteutuakseen riittäviä resursseja. Se, mikä kullekin organisaatiolle on riittävä, vaihtelee organisaatiosta toiseen. Jokainen organisaatio joutuu itse arvioimaan, millaisia tietoturvariskejä se on valmis ottamaan ja millainen on organisaation riittävä tietoturvan taso. Tietoturvaa ei voida ulkoistaa, eikä tänä päivänä voi olla enää erillistä yksikköä tai osastoa tai yksittäistä henkilöä, jonka tehtävänä on huolehtia tietoturvasta.

7.3 Tutkimuksen rajoitteet

Jokaiseen tutkimukseen liittyy myös rajoitteita (Yin, 2014, 4). Ensinnäkin ei ole teknisesti tai käsitteellisesti mahdollista esittää kattavaa luetteloa kaikista niistä (teko)selityksistä, joita yksilö tietoturvarikkomuksen tehdessään käyttää. Myöskin syyllisyyden mittaaminen tai havaitseminen on haastavaa, koska yksilö voi pyrkiä peittelemään tunnetta taidokkaasti. Tutkimuksen rajauksena toiminutta Sykes ja Matzan neutralisoimisteoriaa on täydennetty lukuisilla erilaisilla neutralisoimistekniikoilla. Silti alkuperäinen teoria kaikkine olettamuksineen loi tälle tutkimukselle perustan tarkastella teorian pätevyyttä tietoturvakontekstissa, eli sitä, onko tietoturvarikkomuksissa kyse oikeuttamisesta ja hyödynnetäänkö niissä neutralisoimistekniikoita. Kuitenkin alkuperäisessä teoriassa pitäytymistä voidaan pitää tutkimuksen yhtenä rajoitteena.

Laadullinen tutkimus kohtaa paljon kritiikkiä siitä, että tutkimuksen kontekstiin liittyy erityispiirteitä, joita ei välttämättä voida yleistää laajemmin. Tämänkin tutkimuksen yhtenä rajoitteena on se, että tutkimuksen aineisto on kerätty kahdesta organisaatiosta. Kahdesta eri organisaatiosta kerätty tutkimusaineisto tarjosi kuitenkin etua siinä, että haastateltavien senhetkinen kokemusmaailma oli oletettavasti suhteellisen samanlainen.

Yksilön tietoturvakäyttäytymiseen vaikuttaa se ympäristö, jossa yksilö toimii. Tässäkään tutkimuksessa yksilöä ei voitu irrottaa toimintaympäristöstä, joten tarkastelussa sivutaan myös organisaatiokulttuuria. Tutkimukseen osallistuneiden organisaatioiden näkökulmasta on erittäin myönteistä, että tutkimukseen osallistuneet haastateltavat vaikuttaisivat olevan organisaatioon sitoutuneita. Kuitenkin juuri sitoutuneisuus on saattanut vaikuttaa tutkimustulokseen. Organisaatio, jossa suositaan niin sanottuja epätyypillisiä työsuhteita, saattaisi tuoda erilaista näkökulmaa niin organisaatioon sitoutumiseen kuin tietoturvapolitiikan sisäistämiseen. Voi siis olla mahdollista, että osa-aikaista ”pätkätyötä” tekevä työntekijä saattaisi olla vain osittain sitoutunut eikä tietoturvapolitiikankaan sisäistäminen olisi kuin osittaista. Toisaalta voi olla myös täysin mahdollista, ettei osa-aikaista ”pätkätyötä” tekevä edes uskaltaisi jättää ohjeita noudattamatta tai kritisoida niitä, vaikka ne olisivatkin ristiriidassa hänen oman ymmärryksensä kanssa. Vaikka epätyypillisessä työsuhteessa olevalle työntekijälle voisikin olla luontaista kysyä: eikö tämän voisi tehdä toisin, tapoihin saatetaan pyrkiä sopeutumaan työpaikan säilyttämisen vuoksi.

Sykesin ja Matzan (1957, 667) mukaan neutralisointi on kulttuurisidonnaista. Se, että tutkimuksen aineisto kerättiin suomalaisista organisaatioista liittää tutkimukseen, ainakin osittaisen, kulttuurisen rajoitteen. Vaikka onkin viitteitä siitä, että tietoturvarikkomusten kirjo on kansainvälinen ilmiö, eikä siten kulttuurien välillä ole huomattavia eroja (Vance, Siponen & Straub, 2020, 7), on kuitenkin oletettavaa, että kunkin yksilön omaan kulttuuriin, jopa työkulttuuriin liittyy jonkinasteinen sosiaalistaminen, jolloin toisenlaisessa kulttuurissa/työkulttuurissa tehty tutkimus olisi voinut voisi tuoda erilaisia näkökulmia.

Kuten Topalli (2005, 826) ja Maruna ja Copes (2005, 231) toteavat, neutralisoimisteorian testattavuus on hankalaa, koska yksilön voi olla vaikea ennustaa, aikooko hän neutralisoida jotain, tai toisaalta, kertooko yksilö jälkikäteen selityksiä toiminnastaan. Tämän tutkimuksen yhtenä rajoitteena voikin mainita sen, ettei tutkija tehnyt havainnoivaa tutkimusta, vaan aineisto koostui haastatteluista. Havainnointi tai pitkittäistutkimus olisi saattanut paremmin auttaa vertaamaan aikomusta/uskomusta ja todellista käyttäytymistä haastatteluiden ohella. Kuitenkin kulttuuriin liittyvien normien ja uskomusten vaikutukset yksilön käyttäytymiseen edellyttävät pitkäaikaista henkilökohtaista vuorovaikutusta, eikä siltikään voi olla täysin varmaa, onko kulttuuriset vaikutukset ymmärretty täysin. (Kirk, Miller & Miller, 1986, 32.) Tälle tutkimukselle varattu aika ei kuitenkaan olisi mahdollistanut esimerkiksi pitkittäistutkimusta.

7.4 Luotettavuus ja pätevyys

Tieteellisissä tutkimuksissa tarkastellaan tutkimuksen luotettavuutta (engl. *reliability*) ja pätevyyttä (engl. *validity*). Tyypillisesti luotettavuudella on tarkoitettu kvantitatiivisen tutkimuksen toistettavuutta, eli esimerkiksi kaksi tutkijaa pystyy tuottamaan samat tutkimus tulokset samalla menetelmällä uudelleen. Pätevyydellä puolestaan tarkoitetaan tutkimuksessa käytetyn mittarin kelvollisuutta, eli mittaako tutkimus todella sen, mitä sen oli tarkoitus mitata tai kuinka totuudenmukaisia tutkimustulokset ovat. (Golafshani, 2003, 599.) Laadullisen tutkimuksen lähestymistapa ei välttämättä tuota havaintoja, joita tarkastellaan tilastollisin menetelmin, eikä esimerkiksi ihmisen käyttäytymiseen sidoksissa oleva tutkimus ole täysin toistettavissa, joten laadullisessa tutkimuksessa jo pelkät käsitteet ”luotettavuus” ja ”pätevyys” voivat olla harhaanjohtavia (Golafshani, 2003, 601). Vaikka laadullisen tutkimuksen yhteydessä näitä edellä mainittuja käsitteitä ei voitaisikaan käyttää täysin samassa merkityksessä kuin määrällisissä tutkimuksissa, tarvitaan myös laadullisissa tutkimuksissa jonkinlainen tarkastus (Golafshani, 2003, 602; Morse, Barrett, Mayan, Olson, & Spiers, 2002, 13).

Laadullisen tutkimuksen luotettavuuden ja pätevyyden ongelmallisuuteen on ehdotettu eri menetelmien yhdistämistä ajatuksena se, että minkä tahansa menetelmän niin sanotut vääristymät voitaisiin poistaa toisella menetelmällä (Seale, 1999, 473). Myös triangulaation käyttöä on ehdotettu vahvistamaan tutkimusta ja lisäämään sen yleistettävyyttä (Golafshani, 2003, 603; Laine, 2007, 23). Lisäksi muun muassa tapaustutkimuksen pätevyyteen arviointiin on ehdotettu erilaisia kriteereitä, kuten sisäisen (engl. *internal*), ulkoisen (engl. *external*) ja rakenteen (engl. *construct*) pätevyyden (validiteetti) arviointia (Gibbert, Ruigrok ja Wicki, 2008, 1466–1468). Sisäinen pätevyys viittaa kysymykseen siitä, tarjoaako tutkija uskottavan loogisen päättelyn, joka on riittävä puolustamaan tutkimuksen johtopäätöksiä (Gibbert ym., 2008, 1466). Ulkonen pätevyys viittaa yleistettävyyteen. Vaikka laadulliseen tutkimukseen ei liitetä tilastollista yleistettävyyttä, Gibbert ym., (2008, 1468) viittaavat siihen, kuinka tutkijan tulisi esittää selkeä perustelu valinnalleen tarjoten samalla yksityiskohtia tapaustutkimuksen tilanteesta, jotta

lukija voi arvioida tutkimuksen otantavaihtoehtoja. Rakenteellinen pätevyys puolestaan viittaa siihen, missä määrin tutkimus oikeasti tutkii sitä, mitä väittää tutkivansa. Rakenteellista pätevyyttä voi pyrkiä parantamaan sillä, että tutkija esittää selkeän todisteketjun, jolla osoitetaan, kuinka alkuperäisestä tutkimuskysymyksestä siirryttiin lopullisiin johtopäätöksiin. (Gibbert ym., 2008, 1466–1468). Jokaiseen tutkimukseen sisältyy luotettavuutta ja pätevyyttä sekä parantavia että heikentäviä elementtejä. Tämän tutkimuksen sisäistä pätevyyttä vahvistaa se, että tutkimuksella on selkeä tutkimuskehys. Neutralisoimisteoria yhdessä aiempien tutkimusten kanssa toimi empiirisen tutkimusaineiston vertailukohteena. Tämän tutkimuksen ulkoista pätevyyttä heikentää se, että tutkimus ei tarjoa tilastollista yleistettävyyttä. Eisenhardtin (1989) laajasti mainitussa artikkelissa kuitenkin väitetään, että tapaustutkimus voi tarjota perustan analyyttiselle yleistykselle. Vaikka tässä tutkimuksessa ei täysin voitu noudattaa Eisenhardtin teorianmuodostusprosessia, pyrittiin ulkoista pätevyyttä parantamaan sillä, että tutkimuksen aineisto on kerätty kahden eri toimialan organisaatiosta. Tutkittava ilmiö ei esiinny vain yhdenlaisessa ympäristössä. Tässä tutkimuksessa rakenteellista pätevyyttä on pyritty vahvistamaan esittämällä koko tutkimuksen päättelyketju, eli tutkimuksen lähtökohdista tutkimustulosten merkitykseen ja suhteutukseen. Tutkimusaineistona on käytetty erilaisia tietolähteitä, jotka on kuvattu niin tarkasti kuin ne on mahdollista kuvata.

Morse ym., (2002, 17) esittävät, kuinka laadullisessa tutkimuksessa tutkimusprosessin itsessään tulee varmistaa valmiin tutkimuksen luotettavuus ja pätevyys. Morse ym., (2002, 17) tarkentavat vielä laadulliseen tutkimukseen liittyvää jatkuvaa järjestelmällistä tarkastusta, eli käsitteellistä analysointia ja tulkinnan seurantaa, jota vahvistetaan koko tutkimusprosessin ajan. Laadullinen tutkimus ei siten etene lineaarisesti, vaan iteratiivisesti, jolloin luotettavuutta ja pätevyyttä joudutaan tarkastelemaan vaiheittain koko tutkimusprosessin ajan (Morse ym., 2002, 17). Morse ym., (2002, 17–18) esittävät viisi laadullisen tutkimuksen tarkastuskohtaa, joita ovat: 1) metodologian johdonmukaisuus suhteessa tutkimuskysymykseen ja menetelmäkomponenttien yhteensopivuus, 2) otoksen riittävyys ja kylläisyys, 3) tietojen keräämisen ja analysoinnin tahdistus sekä näiden vuorovaikutus, 4) teoreettinen ajattelu, eli tietojen perusteella syntyvät ideat vahvistetaan ja tarkastetaan uudelleen ja 5) tiedon käsitteellistäminen ja teoreettinen ymmärrys.

Menetelmän johdonmukaisuus suhteessa tutkimuskysymykseen ja menetelmäkomponenttien yhteensopivuus tarkoittaa sitä, vastasiko tutkimusote ja siinä käytetyt menetelmät tutkittavaa ilmiötä (Morse ym., 2002, 18). Menetelmä itsessään ei vielä johda tietoon, vaan menetelmä on valittava sen mukaan, millaista tietoa halutaan. Kuten luvussa viisi mainitaan, tämän tutkimuksen menetelmän valinta tehtiin ennen aineiston hankintaa. Laadullisen tutkimuksen valintaan vaikutti se, että aiemmista tutkimuksista poikkeavan menetelmän valinnan toivottiin antavan lisäymmärrystä tietoturvaohjeiden noudattamattomuuteen. Toisaalta tutkijan esiymmärrys aiheesta vaikutti menetelmään valintaan siten, että

tutkimus halusi tuoda niin sanotusti haastateltavien äänen kuuluviin. Tutkimuksen kokonaisasetelmalla on pyritty muodostamaan looginen yhteys toisiinsa. Tutkimuksen metodologiset lähtökohdat on kuvattu luvussa viisi.

Otoksen riittävyydellä ja kylläisyydellä tarkoitetaan otoksen tarkoituksenmukaisuutta sekä sitä, että ilmiöstä on saatu tietoa eri näkökulmien huomioimiseksi. Lisäksi osallistujien tulisi olla tarkoituksenmukaisia siten, että he edustavat parhaiten tutkimusaihetta tai että heillä on tietoa aiheesta. (Morse ym., 2002, 18). Kun tavoitteena on saada mahdollisimman paljon tietoa tietystä ongelmasta tai ilmiöstä, edustava tapaus tai satunnaisotanta ei Flyvbjergin (2006, 229) mielestä ole ehkä sopivin strategia, koska tyypillinen tai keskimääräinen ei useinkaan ole rikkain/runsain tiedonlähde. Sitä vastoin epätyypillinen, kriittinen tai äärimmäinen tapaus paljastavat usein enemmän tietoa. Vaikka tässä tutkimuksessa haastateltavat valikoituivat lopulta niin sanotulla lumipallo-otannalla, oli organisaatioiden toimialoista mahdollista päätellä, että kummassakin organisaatiossa tietoturvan merkitys organisaation toiminnalle on kriittinen. Tästä syystä oli oletettavaa, että jokaisella haastateltavalla oli kokemusta tietoturvasta, sen merkityksestä ja vaikutuksesta päivittäisiin työtehtäviin. Haastateltavien määrä on verrattain pieni, mutta pienelläkin otannalla kyettiin saavuttamaan saturaatio siten, ettei uusia, täysin eriäviä näkökulmia saavutettu. Haastateltavat eivät olleet yksi yhtenäinen joukko, joten se mahdollisti niin sanotusti erilaisten äänien esiin tuomisen. Tutkimuksen luotettavuutta on parannettu esittämällä haastateltavien kertomia ilmaisuja. Lukijan on siten mahdollista vakuuttua, että analyysi on tehty haastateltavien ehdoilla.

Tietojen keräämisen ja analysoinnin tahdistus sekä näiden vuorovaikutus tarkoittavat keskinäistä vuorovaikutusta siitä, mitä jo tunnetaan ja mitä on tiedettävä (Morse ym., 2002, 18). Tässä tutkimuksessa tätä keskinäistä vuorovaikutusta käytiin sekä neutralisoimisteorian ja aiemman tutkimustiedon että kerätyn empiirisen tutkimusaineiston välillä. Tämä keskinäinen vuorovaikutus tuodaan esiin luvuissa kaksi ja neljä, jotka sisältävät sekä neutralisoimisteorian että aiempien tutkimusten kriittisen tarkastelun. Luvussa kuusi tätä aiemmin tehtyä tarkastelua hyödynnetään vuorovaikutukseen yhdessä tutkimusaineiston analyysin kanssa.

Teoreettinen ajattelu, eli tietojen perusteella syntyvät ideat vahvistetaan ja tarkastetaan uudelleen (Morse ym., 2002, 18). Vaikka valmiiksi raportoidussa tutkimuksessa laadullisen tutkimuksen iteratiivisuus ei välttämättä ilmene, tässä tutkimuksessa Sykes ja Matzan neutralisoimisteoriaan, sen yksityiskohtiin sekä aiempiin saman aihepiirin tutkimuksiin palattiin uudelleen ja uudelleen läpi koko tutkimusprosessin. Vaikka tutkimuksella on vahva teoriasidonnaisuus, kriminologian teorian tuominen tietoturvan yhteyteen mahdollisti teorian kriittisen tarkastelun ja antoi tilaa tutkijan itsenäiselle ajattelulle.

Tiedon käsitteellistäminen ja teoreettinen ymmärrys tarkoittaa Morse ym., (2002, 18) esittämänä sitä, että tutkimus tarjoaa käytännöllistä tieteellistä näyttöä, joka on integroitava kehittyvään tietopohjaan. Tämän tutkimuksen päätelmät esitetään sekä teorian että käytännön näkökulmasta. Tutkimuksessa ei voitu täysin noudattaa Eisenhardtin (1989) esittämää teorianmuodostusprosessia. Useiden tutkijoiden ja erilaisten teoreettisten näkökulmien käyttäminen olisi voinut antaa

tutkimukselle erilaisen lähestymistavan ja monipuolistaa tutkimusta. Tästä syystä tutkimus antaa useita aiheita tulevaisuuden tutkimuksille.

Vaikka tutkijaa tuskin voidaan irrottaa erilleen mistään tutkimuksesta, mainitsevat Eskola ja Suoranta (1998) osuvasti sen, että tutkija on usein laadullisen tutkimuksen keskeisin työväline. Eli kun luotettavuuden kriteerinä on tutkija itse, koskee luotettavuuden arviointi silloin koko tutkimusprosessia. Tässä tutkimuksessa tutkimusprosessin kuvaukseen on kiinnitetty erityistä huomiota ja esitetty se niin tarkasti kuin sensitiiviseksi luokitellussa tietoturva-aiheisessa tutkimuksessa on mahdollista kuvata.

7.5 Tuleva tutkimus

Tutkimuksen tulokset tarjoavat useita aiheita tulevaisuuden tutkimuksille. Muun muassa Siponen ja Vance (2010), Li ja Cheng (2013), Silic ym., (2017) ja Vance ym., (2020) ovat esittäneet, että virallisilla tai epävirallisilla sanktioilla on vain vähäinen vaikutus tietoturvarikkomusten aikomukseen, jolloin neutralisoimisteoria selittäisi todellista tai aiottua tietoturvakäyttäytymistä paremmin kuin rangaistuksiin perustuvat teoriat. Koska rangaistuksilla pelottelu tai uhkailu ei välttämättä vaikuta tietoturvakäyttäytymiseen, eivätkä työntekijät myöskään suoranaisesti neutralisoi tietoturvarikkomuksiin liittyvää syyllisyyttä ja häpeää, eivät pelkät pahoittelevat selonteot kuitenkaan selitä kaikkia tietoturvarikkomuksia. Haastatteluissa esiin noussut kritiikki henkilön aseman vaikutuksesta tietoturvakäyttäytymiseen antaisi viitteitä siitä, että hierarkisesti korkeampi institutionaalinen rooli saattaa vaikuttaa oikeuttamisen tekniikoiden mahdolliseen hyödyntämiseen. Aihe vaatisi kuitenkin lisätutkimusta, onko henkilön asemalla oikeasti merkitystä tietoturvarikkomusten oikeuttamiseen. Vaikuttaisi myös sille, ettei etiikan ja moraalin merkitystä ole tutkittu riittävästi organisaatioiden tietoturvakontekstissa. Ovatko esimerkiksi teknologian tarjoamat henkilökohtaiset hyödyt heikentäneet tietoturvan yhteydessä, normin määritelmässäkin mainittua, yhteisten toimintatapojen tavoitetta?

Tutkimusaineistosta nousee esiin samankaltainen kahtiajako, eli koulutus, työtehtävät ja asema organisaatiossa vaikuttavaa myös asenteeseen tietoturvaa kohtaan sekä käytännön toimintatapoihin. Aihe vaatisi kuitenkin lisätutkimusta siitä, miten nuo niin sanotut alakulttuurit vaikuttavat tietoturvarikkomusten järkeistämiseen tai selittämiseen.

Selontekona ”kiire” vaatisi tarkempaa tutkimusta muun muassa siitä, miten työntekijät priorisoivat kiireellisiin työtehtäviin ja pyyntöihin tai muuttuviin tilanteisiin vastaamista. Voisiko siihen liittyä myös sosiaalisen hyväksynnän hakeminen? On oletettavaa, etteivät työntekijät kiirehdi kaikessa, joten tuon priorisoinnin selvittäminen voisi auttaa konkretisoitaisiin myös muun muassa kiireen luomien etujen ja haittojen suhdetta.

Tutkimusaineisto antoi myös viitteitä siihen, että erilaisten toimintojen ja palveluiden ulkoistaminen voi olla yhtenä tekijänä heikentämässä työntekijän mahdollisuutta ymmärtää tietoturvan ”miten” ja ”miksi”. Aihe vaatisi kuitenkin

lisätutkimusta ulkoistuksen todellisista vaikutuksista organisaatioiden tietoturvakäyttäytymiseen ja siihen, edesauttaako palveluiden ulkoistus samalla myös ymmärtämättömyyteen ja tietämättömyyteen liittyvien selontekojen hyödyntämistä.

Tulevissa tietoturvatutkimuksissa tulisi tulevaisuudessakin hyödyntää sekä laadullisia että määrällisiä tutkimusmenetelmiä. Tässä tutkimuksessa esitettyjä tuloksia tulisi haastaa, ja tutkia lisää, mitkä muut tekijät selittävät työntekijöiden tietoturvarikkomuksia.

8 YHTEENVETO

Organisaatioiden työntekijöiden tietoturvaan liittyvät asenteet ja toimet ovat kasvaneet yhä merkittävämmäksi kohteeksi tietoturvatutkimuksissa. Työntekijöiden tietoturvapolitiikan ja -ohjeiden noudattamattomuus voi muodostaa organisaatiolle merkittävän tietoturvauhkan, ja onkin väitetty, että lähes puolet tietoturvarikkomuksista tapahtuu organisaatioiden sisältäpäin. Koska yksilö voi omalla toiminnallaan edesauttaa tai vaihtoehtoisesti murentaa organisaation tietoturvan ylläpitämistä, on tietoturvaan liittyvää käyttäytymistä tutkittu erilaisten teoriasuuntausten ja teoreettisten lähtökohtien kautta. Tietoturvatutkimuksissa on sovellettu muun muassa psykologian ja kriminologian teorioita ja pyritty niiden avulla ymmärtämään ja selittämään, mikä ohjaa työntekijöiden tietoturvakäyttäytymistä. Aiemmat tutkimukset ovat esittäneet, ettei muun muassa seurausten tai rangaistuksen pelko ohjaa työntekijöiden tietoturvakäyttäytymistä, ja esittäneet näkemyksen siitä, kuinka työntekijät oikeuttavat tietoturvarikkomuksiaan erilaisten neutralisoimistekniikoiden avulla ja järkeilevät niiden avulla toimintaansa, jolloin seurauksetkin menettävät merkityksensä.

Tämän tutkimuksen aiheena on ollut tutkia, miten työntekijät selittävät ja perustelevat tietoturvapolitiikan ja –ohjeiden noudattamattomuutta. Tutkimuksessa sovelletaan yhtä vaikutusvaltaisena pidettyä kriminologian teoriaa ja tarkastellaan sen selitysvoimaa tietoturvakontekstissa. Sykes ja Matzan (1957) esittävät neutralisoimisteoriansa keskeisenä väitteenä, että ihminen oikeuttaa normeista poikkeavan käyttäytymisensä neutralisoimistekniikoiden avulla, ja välttää näin itsesyytösten aiheuttaman syyllisyyden ja häpeän kyetäkseen säilyttämään vahingoittumattoman minäkuvan. Vaikka aiemmat neutralisoimisteoriaan tietoturvakontekstissa soveltaneet tutkimukset ovat tuoneet esille arvokasta tietoa siitä, kuinka työntekijät pyrkivät selittämään tietoturvarikkomuksiaan, ei aiempien tutkimusten lähestymistapa neutralisoinnin roolista ja merkityksestä tietoturvapolitiikan noudattamattomuuteen ole ollut välttämättä riittävän järjestelmällinen ja kattava. Aiemmissa tutkimuksissa ei muun muassa ole riittävästi huomioitu ja sovellettu Sykes ja Matzan neutralisoimisteorian olettamuksia, jotka johdattelevat siihen, miksi yksilö neutralisoi toimintaansa. Väitteistään

huolimatta, aiemmat tutkimukset eivät ole itse asiassa soveltaneet Sykes ja Matzan neutralisoimisteoriaa, joten ei myöskään ole selvää, pystyvätkö Sykes ja Matzan neutralisoimisteorian neutralisoimistekniikat oikeasti selittämään tietoturvakäyttäytymistä.

Sykesin ja Matzan (1957) neutralisoimisteoria yhdessä aiempien saman aihepiirin tutkimuksen kanssa on muodostanut tämän tutkimuksen teoreettisen viitekehyksen. Tämän tapaustutkimuksessa tapauksen muodostaa tutkimuksen keskiössä oleva ilmiö, eli tietoturvarikkomus. Ilmiö on rajattu organisaatioympäristöön. Tutkimusaineisto koostuu sekä tutkimukseen osallistuneiden organisaatioiden tietoturvaan liittyvästä dokumentaatiosta, että organisaatioiden työntekijöiden teemahaastatteluista. Tutkimusta varten haastateltiin kaikkiaan 24 työntekijää. Tutkimuksen tärkeimpänä kontribuutiona esitetään neutralisoimisteorian ja aiempien tutkimusten kriittinen tarkastelu sekä aiemmista tutkimuksista poikkeava näkemys tietoturvarikkomusten selontekoihin. Näiden selontekojen tarkastelussa on sovellettu Scottin ja Lymanin (1968) neutralisoimisteoriasta vaikutteita saanutta Accounts-nimistä artikkelia. Scott ja Lyman jakavat selonteot pahoitteleviin ja oikeuttaviin, ja esittävät näkemyksen näiden kahden selonteon eroista. Scottin ja Lymanin (1968, 47) mukaan oikeuttavat selonteot ovat selityksiä, joissa henkilö on vastuussa teostaan, mutta kiistää siihen liittyvän teon halveksuttavuuden. Pahoittelevat selonteot puolestaan viittaavat tilanteisiin, joissa yksilö myöntää teon olleen väärä, paha tai epäasianmukainen, mutta kiistää täyden vastuun.

Tutkimustuloksen perusteella vaikuttaisi sille, että huolimatta siitä, että työntekijät selittävät tietoturvarikkomuksiaan, he eivät välttämättä koe niistä henkilökohtaista vastuuta. Työntekijät ovat vain harvoin päättämässä niistä tietoturvaratkaisuista, joita he joutuvat käyttämään. Vaikka työntekijät eivät välttämättä suhtaudu organisaation tietoturvavaatimuksiin täysin välinpitämättömästi, tutkimustuloksen perusteella vaikuttaisi sille, ettei tietoturva ole saavuttanut sosiaalisen normin asemaa siten, että sitä ylläpidettäisiin sosiaalisen kontrollin ja sosiaalisen järjestyksen avulla. Tutkimuksen tulos tukee väitettä, etteivät työntekijät välttämättä hyödynnä neutralisoimisteoriassa esitettyjä neutralisoimistekniikoita ja oikeuta niiden avulla tietoturvarikkomuksiaan. Tutkimus esitteleekin viisi pahoittelevaa selontekoa, joiden avulla työntekijät selittävät tietoturvarikkomuksiaan. Tutkimus ehdottaa useita toimenpiteitä, joilla organisaatio voi vähentää tai jopa torjua näitä pahoittelevia selontekoja. Näitä ovat muun muassa tietoturvan noudattamiselle ja tietoturvatietoisuudelle asetetut selkeät tavoitteet. Koska tietoturvakäyttäytymiseen ei välttämättä voida soveltaa Sykes ja Matzan esittämää näkemystä, jonka mukaan arvot ja normit näyttäytyvät pikemminkin toimintaa ohjaavana ja rajoittuneena sovellettavaksi tiettyyn aikaan, paikkaan, henkilöön tai sosiaaliseen tilanteeseen, on tietoturvapolitiikan ohjeineen oltava selkeitä ja ymmärrettäviä, sekä esitetty siten, että käyttäjä voi niitä noudattaa. Lisäksi ohjeiden on oltava jatkuvasti ajantasaisia sekä helposti ja nopeasti löydettävissä. Tietoturva on organisaation ylimmän johdon vastuulla, joten jokainen organisaatio joutuu itse arvioimaan, millaisia tietoturvariskejä se on valmis ottamaan ja millainen on organisaation riittävä tietoturvan taso.

SUMMARY

The attitudes and actions of employees in organizations have become an increasingly important topic in information security researches. Non-compliance with employee security policies and guidelines can construct a significant security threat to the organization and it has been claimed that nearly half of intrusions, security breaches or security violations occur, indirectly or directly, from inside the organization. Because an individual's actions can help or alternatively crumble the maintenance of an organization's information security, information security-related behavior has been studied through various theoretical trends and theoretical starting points. Information security research includes different theories, such as theories of psychology and criminology. They have been used to understand and explain what drives employees' information security behavior. Previous studies have proposed that fear of consequences or informal and formal sanction does not control employees' security behavior because employees' neutralize their actions.

This thesis examines information security from an employees' viewpoint, it focuses on employee's non-compliance with security policies that can lead to security violations and/or breaches and how employees explain their actions. This thesis applies one of the most influential theories of criminology and examines its explanatory power in an information security context. "Neutralization Theory", published by Sykes and Matza in 1957 is the theoretical basis of this thesis. The central argument of Neutralization Theory is that man justifies his deviant behavior by means of neutralization techniques and thus avoids feelings of guilt and shame for his actions and behaviors to be able to maintain his intact self-image. Although previous studies that have applied Neutralization Theory to the information security context have presented valuable insights into how employees seek to explain their security breaches, previous studies have not necessarily been sufficiently systematic and comprehensive in their approach to the role and importance of neutralization. Among other things, previous studies have not sufficiently taken into account and applied the assumptions and arguments of Sykes and Matza's neutralization theory that indicates why an individual would neutralize their actions. Despite their arguments, previous studies have not actually applied Sykes and Matza's neutralization theory. And therefore it is unclear whether the neutralization techniques of Sykes and Matza's neutralization theory can really explain information security behavior.

The theoretical framework of this thesis consists of the neutralization theory of Sykes and Matza together with previous studies. In this case study, the case is called the information security violation or breach and it surrounds the whole study. The phenomenon is limited to the organizational environment. The analyzed data was taken from interviews of 24 employees and from the information security documents of the organizations involved in the research. The main contribution of the thesis is a critical inspection of neutralization theory and previous researches. In addition, this thesis provides a different view of the accounts of

information security violations or breaches than previous researches. In reviewing these accounts, this thesis has applied Scott and Lyman's article called Accounts, which has been influenced by neutralization theory. Scott and Lyman present two types of accounts: excuses and justification and describe the differences between the two accounts. According to Scott and Lyman (1968, 47) justifications are accounts in which one accepts responsibility for the act in question, but denies the pejorative quality associated with it. Excuses are accounts in which one admits that the act in question is bad, wrong, or inappropriate but denies full responsibility.

Based on the empirical results, it appears that despite employees' excuses for their information security breaches or violations they do not necessarily feel to be personally responsible for them. Employees are seldom deciding on the information security solutions they have to use. Although employees may not be completely indifferent to an organization's information security requirements, the research would suggest that information security has not achieved the status of a social norm in a way that is maintained through social control and social order. The result supports the argument that employees do not necessarily utilize of the neutralization techniques presented in the neutralization theory and use them to justify their information security breaches. This thesis presents five accounts through which employees explain their information security breaches or violations.

This thesis proposes numerous acts whereby the organization can reduce or even combat these excuses. Sykes and Matza's argument that values or norms appear as qualified guides for action, limited in their applicability in terms of time, place, persons, and social circumstances cannot necessarily be applied to information security behavior. Therefore, for example, clear aims must be set for compliance in information security and information security awareness. In addition, the information security policy's guidelines must be clear and comprehensible and presented in such a way that the user can follow them. In addition, the guidelines must be constantly up-to-date, easy, and quick to find. Ultimately, the information security is the responsibility of the organization's top management, thus each organization has to assess for itself what kind of security risks it is prepared to carry and what is the acceptable level of security of the organization.

LÄHTEET

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. Communications of the ACM, 42(12), 41-46.

Agnew, R. (1994). The techniques of neutralization and violence. *Criminology*, *32*(4), 555-580.

Ajzen, I. (1991). "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes* (50:2), 179-211

Allen, N. J., & Meyer, J. P. (1990). The measurement and antecedents of affective, continuance and normative commitment to the organization. *Journal of occupational psychology*, *63*(1), 1-18.

Alvarez, A. (1997). Adjusting to genocide: The techniques of neutralization and the Holocaust. *Social Science History*, *21*(2), 139-178.

Anderson, J. M. (2003). Why we need a new definition of information security. *Computers & Security*, 22(4), 308-313.

Andress, J. (2014). *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. Syngress. E-kirja.

Ausubel, D. (1955). Relationships between shame and guilt in the socializing process. *Psychological Review*, *62*(5), 378-390.

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & security*, 39, 145-159.

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2018). Don't Even Think About It! The Effects of Antineutralization, Informational, and Normative Communication on Information Security Compliance. *Journal of the Association for Information Systems*, *19*(8).

Baskerville, R., Straub, D. W., & Goodman, S. E. (2008). *Information Security : Policy, Processes, and Practices*. Armonk, NY: Routledge.

Bauer, S., & Bernroider, E. W. (2017). From information security awareness to reasoned compliant action: analyzing information security policy compliance in a large banking organization. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *48*(3), 44-68.

Bauer, S., Bernroider, E. W., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & security*, 68, 145-159.

Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The case research strategy in studies of information systems. *MIS quarterly*, 369-386.

Bishop, M. (2003). What is computer security?. *IEEE Security & Privacy*, *99*(1), 67-69.

Black, D. (2010). *The behavior of law*. Special edition. Emerald Group Publishing.

Bodin, L. D., Gordon, L. A., & Loeb, M. P. (2008). Information security and risk management. *Communications of the ACM*, *51*(4), 64.

Bone, J. (2017). *Cognitive Hack: The New Battleground in Cybersecurity... the Human Mind.* Auerbach Publications. E-kirja.

Boss, S.R., Galletta, D.F., Lowry, P.B., Moody, G.D., Polak, P. (2015). What do systems users have to fear? Using fear Appeals to engender threats and fear that. Motivate protective security behaviors. *MIS Quarterly*, 39(4), 837-A10.

Brauer, M., & Chaurand, N. (2010). Descriptive norms, prescriptive norms, and social control: An intercultural comparison of people's reactions to uncivil behaviors. *European Journal of Social Psychology*, *40*(3), 490-499.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, *34*(3), 523-548.

Calder, A. (2008). ISO27001/ISO27002 : A Pocket Guide. Ely: IT Governance Publishing. E-kirja.

Calder, A., & Watkins, S. G. (2010). *Information Security Risk Management for ISO27001/ISO27002*. Cambridgeshire: IT Governance Publishing. E-kirja.

Carrabine, E., Iganski, P., Lee, M., Plummer, K., South, N. (2004). *Criminology: A Sociological Introduction*. Taylor & Francis. E-kirja.

Casey, D. (2008). Turning log files into a security asset. *Network Security*, *2008*(2), 4-7.

Cheng, L., Li, W., Zhai, Q., & Smyth, R. (2014). Understanding personal use of the Internet at work: An integrated model of neutralization techniques and general deterrence theory. *Computers in Human Behavior*, 38, 220-228.

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security*, *39*, 447-459.

Cialdini, R. B., & Goldstein, N. J. (2004). Social influence: Compliance and conformity. *Annu. Rev. Psychol.*, *55*, 591-621.

Cohen, A. (1955). Delinquent boys. *New York*, *84*.

Copes, H. (2003). Societal attachments, offending frequency, and techniques of neutralization. *Deviant Behavior*, *24*(2), 101-127.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, 32, 90-101.

Da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers & security*, *70*, 72-94.

Da Viega, A. & Eloff, J.H.P. (2010). A framework and assessment instrument for information security culture, *Computer & Security*, 196-207.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 20(1), 79-98.

Darke, P., Shanks, G., & Broadbent, M. (1998). Successfully completing case study research: combining rigour, relevance and pragmatism. *Information systems journal*, 8(4), 273-289.

Dhillon, G., Samonas, S., & Etudo, U. (2016). Developing a Human Activity Model for Insider IS Security Breaches Using Action Design Research. In IFIP International Information Security and Privacy Conference (49-61). Springer International Publishing.

DiCicco-Bloom, B., & Crabtree, B. F. (2006). The qualitative research interview. *Medical education*, *40*(4), 314-321.

Dubois, N. (Ed.). (2003). *A sociocognitive approach to social norms*. Routledge. E-kirja.

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of management review*, 14(4), 532-550.

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory building from cases: Opportunities and challenges. *Academy of management journal*, 50(1), 25-32.

ENISA. (2019). ENISA Threat Landscape Report 2018. 15 Top Cyber-Threats and Trends. Haettu 9.2.2019 osoitteesta https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

Eriksson, P., & Koistinen, K. (2014). *Monenlainen tapaustutkimus*. Kuluttajatutkimuskeskus. Haettu 25.2.2018 osoitteesta: https://helda.helsinki.fi/bitstream/handle/10138/153032/Tutkimuksia%20ja%20selvityksi%C3%A4_11_2014_%20Monenlainen%20tapaustutkimus_Eriksson_Koistinen.pdf?sequence=1.

Eskola, J., & Suoranta, J. (1998). *Johdatus laadulliseen tutkimukseen*. Vastapaino. E-kirja.

EUR-lex. (2004). Euroopan parlamentin ja neuvoston asetus (EY) N:o 460/2004. Haettu 20.9.2018 osoitteesta https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:FI:HTML.

Ewald, F. (2003). *Normi yhteisen mittapuun käytäntönä*. Suomalaisen lakimiesyhdistyksen julkaisuja, E-sarja N:o 8. Helsinki: Suomalainen lakimiesyhdistys.

Festinger, L. (1962). *A theory of cognitive dissonance*. Stanford university press.

Finlex (2007). Laki rikoslain muuttamisesta 540/2007. Annettu Helsingissä 11.5.2007. Haettu 9.11.2019 osoitteesta https://www.finlex.fi/fi/laki/alkup/2007/20070540#Lidp445967248.

Finlex (2003). Rikoslaki 19.12.1889/39. 6 § (13.6.2003/515) Lieventämisperusteet. Haettu 27.12.2019 osoitteesta https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001.

Fishbein, M. (2008). A reasoned action approach to health promotion. *Medical Decision Making*, *28*(6), 834-844.

Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention and behavior: An introduction to theory and research.

Fishbein, M., & Ajzen, I. (2011). *Predicting and changing behavior: The reasoned action approach*. Psychology Press.

Flyvbjerg, B. (2006). Five misunderstandings about case-study research. *Qualitative inquiry*, 12(2), 219-245.

Franzese, R. J. (2015). *The Sociology of Deviance : Differences, Tradition, and Stigma*. Springfield : Charles C Thomas. 2015. E-kirja.
French, J. R., Raven, B., & Cartwright, D. (1959). The bases of social power. *Classics of organization theory*, *7*, 311-320.
Fritsche, I. (2005). Predicting deviant behavior by neutralization: Myths and findings. *Deviant Behavior*, *26*(5), 483-510.
Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, 31(8), 983-988
Gawronski, B., & Bodenhausen, G. V. (2015). *Theory and explanation in social psychology*. Guilford Publications.
Gerring, J. (2007). *Case study research: Principles and practices*. Cambridge university press.
Gibbert, M., Ruigrok, W., & Wicki, B. (2008). What passes as a rigorous case study?. *Strategic management journal*, *29*(13), 1465-1474.
Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The qualitative report*, *8*(4), 597-607.
Goldkuhl, G. (2012). Pragmatism vs interpretivism in qualitative information systems research. *European journal of information systems*, *21*(2), 135-146.
Grasmick, H. G., and Bursik, R. 1990. "Conscience, Significant Others, and Rational Choice: Extending the Deterrence Model,"*Law and Society Review* (24:3), 837-862.
Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security*, 32, 242-251.
Haag, S., & Eckhardt, A. (2015). Justifying Shadow IT Usage. In PACIS (p. 241).
Haag, S., Eckhardt, A., & Bozoyan, C. (2015). Are shadow system users the better IS users?–insights of a lab experiment. AIS Electronic Library (AISel) ICIS2015.
Haaparanta, L., & Niiniluoto, I. (2016). *Johdatus tieteelliseen ajatteluun*. Gaudeamus: Helsinki.
Harris, L. C., & Dumas, A. (2009). Online consumer misbehaviour: an application of neutralization theory. *Marketing Theory*, 9(4), 379–402
Hazani, M. (1991). The universal applicability of the theory of neutralization: German youth coming to terms with the holocaust. *Crime, Law and Social Change*, 15(2), 135-149.
Herath, T., & Rao, H. R. (2009a). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106-125.
Herath, T., & Rao, H. R. (2009b). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154-165.
Heuer Jr, R. J., Heuer, R. J., & Pherson, R. H. (2015). *Structured analytic techniques for intelligence analysis*. Second Edition.CQ Press.
Heuer, R. J. (1999). *Psychology of intelligence analysis*. Lulu. com.
Hindelang, M. J. (1970). The Commitment of Delinquents to Their Misdeeds: Do Delinquents Drift?. *Social Problems*, 502-509.

Hirschi, T. (1969). A control theory of delinquency. *Criminology theory: Selected classic readings*, *1969*, 289-305.

Hirsjärvi, S., & Hurme, H. (2008). *Tutkimushaastattelu*. *Teemahaastattelun teoria ja käytäntö*. Helsinki: Gaudeamus Helsinki University Press

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2004). *Tutki ja kirjoita* (10. osin uud. painos). Helsinki: Tammi.

Holtkamp, P., Soliman, W. & Siponen, M. (2019) Reconsidering the Role of Research Method Guidelines for Qualitative, Mixed-methods, and Design Science Research. In Hawaii international conference on system sciences, proceedings of the 52nd annual. IEEE.

Horne, C. (2001). Sociological perspectives on the emergence of social norms. Kirjassa: Social norms. Sivuilla 3-34. Toim. Hechter M, Opp K-D. New York: Russell Sage Foundation.

Hsu, C., Lee, J. N., & Straub, D. W. (2012). Institutional influences on information systems security innovations. *Information systems research*, *23*(3-part-2), 918-939

Humphreys, T. (2016). Implementing the ISO/IEC 27001 ISMS Standard. Boston: Artech House.

Höne, K., & Eloff, J. H. P. (2002). Information security policy—what do international information security standards say?. *Computers & Security*, *21*(5), 402-409.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83-95.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, *51*(1), 69-79.

Ilvonen, I. (2011, July). Information Security Culture or Information Safety Culture-What do Words Convey?. *In European Conference on Cyber Warfare and Security* (p. 148). Academic Conferences International Limited.

Im, G. P., & Baskerville, R. L. (2005). A longitudinal study of information system threat categories: the enduring problem of human error. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *36*(4), 68-79.

Innes, M. (2003). *Understanding Social Control : Deviance, Crime and Social Order*. Open University Press. E-kirja.

Joensuu, J. (2019). Yle Uutiset. Taas tietomurto Satakunnassa: Tällä kertaa kohteena Porin kaupunki. Haettu 4.1.2020 osoitteesta https://yle.fi/uutiset/3-10913191.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS quarterly*, 549-566.

Johnston, A. C., Di Gangi, P. M., Howard, J., & Worrell, J. (2019). It Takes a Village: Understanding the Collective Security Efficacy of Employee Groups. *Journal of the Association for Information Systems*, *20*(3), 186-212.

Johnston, A. C., Warkentin, M., & Siponen, M. T. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *Mis Quarterly*, 39(1), 113-134.

Johnston, A. C., Warkentin, M., McBride, M., & Carter, L. (2016). Dispositional and situational factors: influences on information security policy violations. European Journal of Information Systems, 25(3), 231-251.

Järvinen, P. (2014). IS Reviews 2014. Haettu 14.2.2018 osoitteesta: http://www.uta.fi/sis/reports/index/R35_2014.pdf.

Järvinen, P. (2018). *Ammatillinen käyttäytyminen: tie onnistumiseen.* Alma Talent. E-kirja.

Järvinen, P., & Järvinen, A. (2004). *Tutkimustyön metodeista*. Opinpajan kirja:Tampere.

Karjalainen, M., Sarker, S., & Siponen, M. (2019). Toward a Theory of Information Systems Security Behaviors of Organizational Employees: A Dialectical Process Perspective. *Information Systems Research*.

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information systems security policies: a contextual perspective. *Computers & Security*, *24*(3), 246-260.

Keizer, K., S. Lindenberg & L. Steg (2008). The spreading of disorder. Science 322: 5908, 1681−1685.

Keutel, M., Michalik, B., & Richter, J. (2014). Towards mindful case study research in IS: A critical analysis of the past ten years. *European Journal of Information Systems*, 23(3), 256-272.

Khansa, L., Kuem, J., Siponen, M., & Kim, S. S. (2017). To cyberloaf or not to cyberloaf: The impact of the announcement of formal organizational controls. *Journal of Management Information Systems*, 34(1), 141-176.

Kielitoimiston sanakirja. (2018). Helsinki: Kotimaisten kielten keskus. Verkkojulkaisu haettu 20.6.2018 osoitteesta https://www.kielitoimistonsanakirja.fi/netmot.exe?ListWord=rikkomus&SearchWord=rikkomus&dic=1&page=results&UI=fi80&Opt=1.

Kim, D. W., Yan, P., & Zhang, J. (2015). Detecting fake anti-virus software distribution webpages. *Computers & Security*, *49*, 95-106.

Kim, S. H., Yang, K. H., & Park, S. (2014). An integrative behavioral model of information security policy compliance. The Scientific World Journal, 2014.

Kinnunen, N. (2015). Tietoturvaohjeistusten noudattamisen motivaatio ja sen muuttaminen. Väitöskirja. Vaasan yliopisto. Haettu 11.3.2017 osoitteesta http://www.uva.fi/materiaali/pdf/isbn_978-952-476-637-1.pdf.

Kirk, J., Miller, M. L., & Miller, M. L. (1986). *Reliability and validity in qualitative research*. Sage.

Klockars, C. B. (1974). The Professional Fence, New York: Free Press.

Kuhn, L. H.(2009). *Social Control And Human Nature: What Is It We Are Controlling?.* El Paso: LFB Scholarly Publishing LLC, 2009. E-kirja

Laine, M. (2007). *Kriminologia ja rankaisun sosiologia*. Helsinki : Tietosanoma Oy.

Laine, M., Bamberg, J., & Jokinen, P. (2007). Tapaustutkimuksen käytäntö ja teoria. Teoksessa M. Laine, J. Bamberg & P. Jokinen (toim.) *Tapaus-tutkimuksen taito*. Helsinki: Gaudeamus, 2, 9-40.

Lattu, E. (2016). Naisten tekemä väkivalta. Väitöskirja. Tampereen yliopisto. Haettu 14.4.2019 osoitteesta https://tampub.uta.fi/bitstream/handle/10024/99101/978-952-03-0138-5.pdf?sequence=1.

Lee, S. M., Lee, S. G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management*, *41*(6), 707-718.

Levi, K. (1981). Becoming a hit man: Neutralization in a very deviant career. *Urban Life*, *10*(1), 47-63.

Levy, Y., & Ellis, T. J. (2006). A systems approach to conduct an effective literature review in support of information systems research. *Informing Science*, 9.

Li, W., & Cheng, L. (2013). Effects of Neutralization Techniques and Rational Choice Theory on Internet Abuse in the Workplace. In PACIS (p. 169).

Lyytinen, K., & Newman, M. (2008). Explaining information systems change: a punctuated socio-technical change model. *European Journal of Information Systems*, *17*(6), 589-613.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of experimental social psychology*, *19*(5), 469-479.

Martins, A., & Elofe, J. (2002). Information security culture. In *Security in the information society* (203-214). Springer, Boston, MA.

Maruna, S., & Copes, H. (2005). What have we learned from five decades of neutralization research?. *Crime and justice*, 221-320.

Mason, R. O., Mason, F. M., & Culnan, M. J. (1995). *Ethics of information management* (109-48). Thousand Oaks, CA: Sage.

Metsämuuronen, J. (2011). *Tutkimuksen tekemisen perusteet ihmistieteissä 2*. Opiskelijalaitos. International Methelp Oy.

Meyer, J. P., & Allen, N. J. (1997). *Commitment in the Workplace: Theory, Research, and Application (Advanced Topics in Organizational Behavior)*. Thousand Oaks, CA: Sage Publications.

Mills, A. J., Durepos, G., & Wiebe, E. (Eds.). (2009). *Encyclopedia of case study research: L-Z; index*. Sage.

Mills, C. W. (1940). Situated actions and vocabularies of motive. *American sociological review*, *5*(6), 904-913.

Minor, W. W. (1984). Neutralization as a hardening process: Considerations in the modeling of change. *Social Forces*, 62(4), 995-1019.

Minor, W. W. (1981). "Techniques of Neutralization: a Reconceptualization and Empirical Examination," *Journal of Research in Crime and Delinquency* (18:2), 295–318.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, 42(1).

Morse, J. M., Barrett, M., Mayan, M., Olson, K., & Spiers, J. (2002). Verification strategies for establishing reliability and validity in qualitative research. *International journal of qualitative methods*, *1*(2), 13-22.

Myers, M. D. (2013). *Qualitative research in business and management*. Sage.

Myers, M. D., & Avison, D. (2002). An introduction to qualitative research in information systems. *Qualitative research in information systems*, *4*, 3-12.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*, *18*(2), 126-139.

Nagin, D. S., and Paternoster, R. (1993). "Enduring Individual Differences and Rational Choice Theories of Crime," *Law & Society Review* (27:3), 467-496

National Institue of Standards and Technology, Computer Security Division. (2013). Security and Privacy Controls for Federal Information Systems and Organizations. Special Publication 800-53 Revision 4. Gaithersburg: MD. Haettu 7.4.2019 osoitteesta: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf.

Nicho, M., & Kamoun, F. (2014). Multiple case study approach to identify aggravating variables of insider threats in information systems. *Association for Information Systems*.

Nickerson, R. S. (1998). Confirmation bias: A ubiquitous phenomenon in many guises. *Review of general psychology*, *2*(2), 175.

Niemi, R. (2019). Yle Uutiset. Kunnilla heikkoja salasanoja ja huteria palomuureja – Lahti maksoi kyberhyökkäykden torjunnasta liki miljoonan ja jakaa nyt oppeja muillekin. Haettu 27.12.2019 osoitteesta https://yle.fi/uutiset/3-11121273.

Niemimaa, E., & Niemimaa, M. (2017). Information systems security policy implementation in practice: from best practices to situated practices. *European Journal of Information Systems*, *26*(1), 1-20.

Niiniluoto, I. (2002). *Johdatus tieteenfilosofiaan. Käsitteen- ja teorianmuodostus*. (3.painos) Otava: Helsinki.

Nykänen, K. (2011). Tietoturvakoulutuksen vaikuttavuuden arviointi yksilön ja organisaation tietoturvakäyttäytymiseen. Väitöskirja. *Tampere: Oulun Yliopisto, luonnontieteiden tiedekunta, tietojenkäsittelytieteiden laitos.* Haettu 6.11.2016 osoitteesta http://jultika.oulu.fi/files/isbn9789514295713.pdf

Opp, K., & Hechter, M. (2001). Social Norms. New York: Russell Sage Foundation.

Pahnila, S., Siponen, M., & Mahmood, A. (2007, January). Employees' behavior towards IS security policy compliance. In *System sciences, 2007. HICSS 2007. 40Th annual hawaii international conference on* (156b-156b). IEEE.

Parker, D. B. (1995). Possession as an element of information security. *Information Systems Security*, *4*(2), 19-26.

Parsons, T. (1968). *The structure of social action*. The Free Press, New York.

Peltier, T. (2014). *Information Security Fundamentals*. Second Edition. CRC Press. E-kirja.

Peltier, T. R. (2006). Social engineering: Concepts and solutions. *Information Security Journal*, 15(5), 13.

Piquero, N. L., Tibbetts, S. G., & Blankenship, M. B. (2005). Examining the role of differential association and techniques of neutralization in explaining corporate crime. *Deviant Behavior*.

Puhakainen, P. (2006). A design theory for information security awareness. Väitöskirja. Oulun Yliopisto. Haettu 6.11.2018 osoitteesta http://jultika.oulu.fi/files/isbn9514281144.pdf.

Quinn, M. J. (2015). *Ethics for the information age*. Pearson Education 2015. 6th, Global edition. E-kirja.

Raamattu (1992). Suomen evankelilais-luterilaisen kirkon kirkolliskokouksen vuonna 1992 käyttöön ottama suomennos. Helsinki: Suomen Pipliaseura.

Raggad, B. G. (2010). *Information security management.* New York : CRC Press.

Robinson, S. L., & Bennett, R. J. (1995). A typology of deviant workplace behaviors: A multidimensional scaling study. *Academy of management journal*, 38(2), 555-572.

Saaranen-Kauppinen, A., & Puusniekka, A. (2006). KvaliMOTV – Menetelmäopetuksen tietovaranto. Tampere: Yhteiskuntatieteellinen tietoarkisto. Haettu 15.9.2019 osoitteesta http://www.fsd.uta.fi/menetelmaopetus/

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65-78.

Sarker, S., Xiao, X., & Beaulieu, T. (2013). Guest editorial: qualitative studies in information systems: a critical review and some guiding principles. *MIS quarterly*, *37*(4), iii-xviii.

Savolainen, J. (2019) Katsoi uteliaisuuttaan 187 henkilön terveystietoja – hovioikeus korotti henkilörekisteririkoksesta tuomitun 100 päiväsakon sakkorangaistuksen 45 päivän ehdolliseksi vankeudeks. Edilex 15.7.2019 Haettu 4.1.2020 osoitteesta www.edilex.fi.

Schein, E.H. (1991). *Organisaatiokulttuuri ja johtaminen*. 3. painos. Helsinki: Weilin+Göös. Ekonomia-sarja.

Schwandt, T. A. (2007). *The Sage dictionary of qualitative inquiry*. Sage Publications. E-kirja.

Scott, M.B. & Lyman, S. M. (1968). Accounts. *American sociological review*, 46-62.

Seale, C. (1999). Quality in Qualitative Research. *Qualitative Inquiry*, *5*(4), 465-478.

Silic, M., Barlow, J. B., & Back, A. (2017). A new perspective on neutralization and deterrence: Predicting shadow IT usage. *Information & management*.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31-41.

Siponen, M. T. (2001). On the role of human mortality in information system security: from the problems of descriptivism to non-descriptive foundations. *Information Resources Management Journal (IRMJ)*, *14*(4), 15-23.

Siponen, M. T. (2005). Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods. *Information and organization*, *15*(4), 339-375.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, 34(3), 487-A12.

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, *46*(5), 267-270.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & management*, *51*(2), 217-224.

Siponen, M., Puhakainen, P., & Vance, A. (2020). Can individuals' neutralization techniques be overcome? A field experiment on password policy. *Computers & Security*, *88*, 101617.

Siponen, M., Willison, R., & Baskerville, R. (2008). Power and practice in information systems security research. *ICIS 2008 Proceedings*, 26.

Steers, R. M. (1977). Antecedents and outcomes of organizational commitment. *Administrative science quarterly*, 46-56.

Suomen poliisi. (2019). Häiriötiedote. Poliisin verkkosivuilla on häiriöitä. Häiriön syytä selvitetään. Haettu 4.1.2020 osoitteesta https://twitter.com/SuomenPoliisi/status/1164437654403989504?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1164437654403989504&ref_url=https%3A%2F%2Fyle.fi%2Fuutiset%2F3-10933059.

Suoninen, E. (1997). Selonteot ja oman toiminnan ymmärrettäväksi tekeminen. *Sosiologia* : Westermarck-seuran julkaisu 34 (1997) : 1, 3. artikkeli.

Surakka, J. (2017). Ainakin 150 ihmisen potilastietoja luvattomasti käsitellyt kunnan kotihoidon toimistosihteeri tuomittiin sakkoihin ja suorittamaan korvausta kärsimyksestä lukuisille asianomistajille. Edilex 15.2.2017 Haettu 4.1.2020 osoitteesta www.edilex.fi.

Surakka, J. (2018). KHO: Maistraatilla oli erityisen painava syy irtisanoa henkirjoittajan virkasuhde - HAO:n päätös kumottiin. Edilex 21.2.2018 Haettu 4.1.2020 osoitteesta www.edilex.fi.

Surakka, J. (2019). Kainuun sosiaali- ja terveydenhuollon kuntayhtymän potilastietojärjestelmästä tietoja urkkinut keskussairaalan sisätautien poliklinikan osastosihteeri loukkasi teollaan myös lapsen vanhemman yksityiselämää - toisin kuin käräjäoikeus hovioikeus velvoitti vastaajan suorittamaan korvausta myös kärsimyksestä. Edilex 3.10.2019 Haettu 4.1.2020 osoitteesta www.edilex.fi.

Sutherland, E. H., Cressey, D. R., Luckenbill, D. F., & Luckenbill, D. (1992). Principles of criminology. Yhdestoista painos. Rowman & Littlefield.

Sutton, R. I., & Callahan, A. L. (1987). The stigma of bankruptcy: Spoiled organizational image and its management. *Academy of Management journal*, *30*(3), 405-436.

Sykes, G. & Matza, D. (1957). Techniques of Neutralization: A Theory of Delinquency. American Sociological Review, 22 (6), 664–670.

Tasavallan presidentin kanslia. (2017). Tasavallan presidentti Sauli Niinistön lausunto Helsingin Sanomien sotilastiedusteluun liittyvästä artikkelista. Haettu 27.12.2019 osoitteesta https://www.presidentti.fi/tiedote/tasavallan-presidentti-sauli-niiniston-lausunto-helsingin-sanomien-sotilastiedusteluun-liittyvasta-artikkelista/.

Tellis, W. M. (1997). Application of a case study methodology. *The qualitative report*, *3*(3), 1-19.
Tenbrunsel, A. E., & Messick, D. M. (2004). Ethical fading: The role of self-deception in unethical behavior. *Social justice research*, *17*(2), 223-236.
Thomson, K. L., & Von Solms, R. (2005). Information security obedience: a definition. *Computers & Security*, *24*(1), 69-75.
Tieteen termipankki. (2013). Kielitiede:teoria. Haettu 18.2.2018 osoitteesta: http://tieteentermipankki.fi/wiki/Kielitiede:teoria.
Tieteen termipankki. (2016). Filosofia:teoria. Haettu 15.2.2018 osoitteesta: http://tieteentermipankki.fi/wiki/Filosofia:teoria.
Tieteen termipankki. (2019). Filosofia:normatiivisuus. Haettu 13.11.2019 osoitteesta: https://tieteentermipankki.fi/wiki/Filosofia:normatiivisuus.
Tieteen termipankki. (2019). Oikeustiede:sosiaalinen kontrolli. Haettu 17.10.2019 osoitteesta: https://tieteentermipankki.fi/wiki/Oikeustiede:sosiaalinen_kontrolli.
Topalli, V. (2005). When being good is bad: An expansion of neutralization theory. *Criminology*, 43(3), 797-836.
Topalli, V. (2006). The seductive nature of autotelic crime: How neutralization theory serves as a boundary condition for understanding hardcore street offending. *Sociological Inquiry*, *76*(4), 475-501.
Topalli, V. (2018). Professori, kriminologi. Henkilökohtainen tiedonanto 17.10.2018. Sähköpostikeskustelu 18.10.2018.
Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: recommendations for information security awareness programs. *Computers & security*, 52, 128-141.
Tuomi, J. & Sarajärvi, A. (2018). *Laadullinen tutkimus ja sisällönanalyysi*: Uudistettu laitos. Helsinki: Tammi.
Turtia, K.(2010). *Otavan uusi sivistyssanakirja*. (3.painos). Helsinki: Otava.
Töttö, P. (1997). Pirullinen positivismi. *Kysymyksiä laadulliselle tutkimukselle*. Kampus kustannus: Jyväskylä
Urquhart, C., & Vaast, E. (2012). Building social media theory from case studies: A new frontier for IS research.
Vacca, J. R. (Ed.). (2014). *Network and system security*. Second Edition. Elsevier. E-kirja.
Valli, R., & Aaltola, J. (2018). Ikkunoita tutkimusmetodeihin 2–Näkökulmia aloittelevalle tutkijalle tutkimuksen teoreettisiin lähtökohtiin ja analyysimenetelmiin. *PS-kustannus. Jyväskylä*, *118*, 121. E-kirja.
Walsham, G. (1995). Interpretive case studies in IS research: nature and method. *European Journal of information systems*, *4*(2), 74-81.
Walsham, G. (2006). Doing interpretive research. *European journal of information systems*, *15*(3), 320-330.
Valtioneuvosto. (2009). *Yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta välttämättömien tieto- ja viestintäjärjestelmien käytettävyyden kehittäminen.* Liikenne – ja viestintäministeriön julkaisuja 50/2009. Haettu 16.1.2019

osoitteesta
https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/78226/Julkaisuja_50-2009.pdf?sequence=1.
Valtioneuvosto. (2019). *Suomen kyberturvallisuusstrategia 2019.* Haettu 23.11.2019 osoitteesta
https://valtioneuvosto.fi/paatokset/paatos?decisionId=0900908f80655af5.
Valtiovarainministeriö (2009). VAHTI 3/2009. Lokiohje. Haettu 16.3.2019 osoitteesta
https://www.vahtiohje.fi/c/document_library/get_file?uuid=775179cb-6c54-4dfb-b65d-e925d47c61d2&groupId=10229.
Valtiovarainministeriö (2009). VAHTI. Johdatus tietoturva-ajatteluun. Haettu 24.3.2019 osoitteesta
https://www.vahtiohje.fi/web/guest/chapter1?p_p_id=56_INSTANCE_jaK0&p_p_lifecycle=0&p_p_state=exclusive&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&_56_INSTANCE_jaK0_struts_action=%2Fjournal_content%2Fview&_56_INSTANCE_jaK0_groupId=10128&_56_INSTANCE_jaK0_articleId=25960&_56_INSTANCE_jaK0_viewMode=print.
Vance, A., Siponen, M. T., & Straub, D. W. (2019). Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures. *Information & Management*, 103212.
Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management*, *49*(3-4), 190-198.
Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*, *18*(2), 101-105.
Watkins, S. (2013). *An Introduction to Information Security and ISO27001* : 2013. Ely: IT Governance Publishing. E-kirja.
Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS quarterly*, xiii-xxiii.
Weiner, B. (1985). An attributional theory of achievement motivation and emotion. *Psychological review*, 92(4), 548.
Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security*. Fourth edition. Cengage Learning. E-kirja.
Viestintävirasto. (2018). *Tietoturvan vuosi 2017*. Viesintäviraston julkaisuja 001/2018 J. Haettu 13.3.2018 osoitteesta
https://www.viestintavirasto.fi/attachments/cert/tietoturvakatsaukset/Tietoturvan-vuosi-2017.pdf.
Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS quarterly*, *37*(1).
Willison, R., Warkentin, M., & Johnston, A. C. (2018). Examining employee computer abuse intentions: Insights from justice, deterrence and neutralization perspectives. *Information Systems Journal*, *28*(2), 266-293.

Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, *23*(5), 371-376.

Von Solms, R. (1999). Information security management: why standards are important. *Information Management & Computer Security*, *7*(1), 50-58.

Wright, S. (2009). PCI DSS : A Practical Guide to Implementation, Second Edition, Ely, UK: IT Governance Ltd.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & security*, *23*(3), 191-198.

Yazdanmehr, A., & Wang, J. (2016). Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems*, *92*, 36-46.

Yin, R. K. (2014). *Case study research: Design and methods*. Sage publications.

LIITE 1

TAULUKKO 16 ACH analyysin kahdeksan vaihetta

Kilpailevien hypoteesien analysoinnin vaiheet pääpiirteittäin	
1. vaihe	Tunnistetaan kaikki huomioon otettavat mahdolliset hypoteesit, jotka ansaitsevat yksityiskohtaisemman tutkimisen. (Jos mahdollista, käytetään aivoriihtä eri näkökulmien löytämiseksi.)
2.vaihe	Tehdään luettelo kaikista merkittävistä todisteista ja argumenteista kunkin hypoteesin suhteen. Konkreettisten todisteiden lisäksi luetteloon sisällytetään myös asiaankuuluvia olettamuksia ja loogisia päätelmiä. (edellä mainittujen löytämiseksi on syytä kysyä mm: millaisia tietoja tulisi löytyä/mitä pitäisi tapahtua, jotta hypoteesi olisi totta/ei olisi totta)
3.vaihe	Laaditaan matriisi (taulukko), jonka vaakariveillä ovat hypoteesit ja pystyriveillä todisteet. Arvioidaan todisteiden ja argumenttien merkittävyyttä, eli suhteellista todennäköisyyttä ja johdonmukaisuutta. (Vaiheen 1 oletuksiin yhdistetään vaiheen 2 todisteet, jolloin saadaan yleiskuva ongelman kaikista tärkeistä osista. Samalla analysoidaan, kuinka jokainen todiste liittyy kuhunkin hypoteesiin.)
4.vaihe	Tarkennetaan koko matriisia. Eli poistetaan hypoteeseja, todisteita ja argumentteja, jotka eivät ole merkityksellisiä ja lisätään niitä, jotka ovat merkityksellisiä. Täsmennetään hypoteesien tarkkaa sanamuotoa.
5.vaihe	Tehdään alustavia päätelmiä kunkin hypoteesin suhteellisesta todennäköisyydestä, ja yritetään vahvistamisen sijasta kumota hypoteeseja. Vaikka hypoteejä tarkastellaan kokonaisuutena, matriisin ei pitäisi kuitenkaan määritellä sitä, mihin johtopäätökseen tullaan päätymään, vaan se toimii ajattelun ja analysoinnin tukena. Matriisin tarkoituksena on tuottaa arvio siitä, mikä on tärkeää ja miten nämä tekijät liittyvät kunkin hypoteesin todennäköisyyteen.
6. vaihe	Analysoidaan, kuinka haavoittuva johtopäätös on suhteessa kriittisiin todisteisiin. Eli arvioidaan, onko olemassa vaihtoehtoisia selityksiä ja tulkintoja, voivatko todisteet olla puutteellisia ja harhaanjohtavia, tai perustuuko tulkinta kyseenalaisille olettamuksille? Myös analyysin seuraukset on otettava tarkasteluun. Eli mitä seuraa, jos todisteet ovat vääriä, harhaanjohtavia tai niitä tulkitaan eri tavalla. Tämä on vaihe, jossa voidaan päättää lisätutkimuksen tarpeesta, jolloin voidaan palata esimerkiksi alkuperäisen lähdemateriaalin äärelle.
7. vaihe	Raportoidaan päätelmistä, jossa kaikkien hypoteesien suhteellista todennäköisyyttä tarkastellaan, ei vain todennäköisimmän. Jos tarkasteltaisiin vain todennäköisintä hypoteesia, olisi olemassa mahdollisuus, että johtopäätökset olisi tehty olettamusten perusteella. (Tapahtumia, joita todennäköisesti esiintyy useammin, tai joita on tapahtunut aiemmin, on helpompi kuvitella jatkossakin tapahtuvaksi kuin epätodennäköisiä tapahtumia.)
8. vaihe	Analyysia on aina pidettävä alustavana, koska myöhemmät havainnot voivat tuoda uuttaa tietoa, joka saattaa merkitä muutosta myös todennäköisyyden arviointeihin. On kuitenkin syytä jo etukäteen hahmottaa tapahtumia, jotka voivat toimia käännekohtana tilanteen muutokselle.

TAULUKKO 17 Mallia analyysin ensimmäisestä vaiheesta

ACH vaihe 1: Tunnistetaan kaikki huomioon otettavat mahdolliset hypoteesit, jotka ansaitsevat yksityiskohtaisemman tutkimisen.	
1.Onko tietoturvapolitiikka on rinnastettavissa lakiin (vertauskuva laista)?	
	(Hypoteesin tulisi sisältää: kuka, mitä, milloin, missä, miksi (mahdollisesti miten) Hypoteesi on selkeä toteamus, joka perustuu havaintoihin tai tietoihin, se voidaan testata ja se voidaan todistaa vääräksi. Hypoteesi ennustaa selvästi tuloksia. Se sisältää riippuvan ja riippumattoman muuttujan. Riippuva muuttuja on ilmiö, jota selitetään ja riippumaton muuttuja on selittäjä.(Hypoteesit tulisi olla toisensa poissulkevia)
hypoteesi 1	Työntekijä on sitoutunut organisaatioon ja sen toimintatapoihin
selitys (mitä hypoteesi näyttää tarkoittavan)	Siinä missä yhteiskuntaan kuuluminen velvoittaa noudattamaan lakeja, organisaatioon sitoutuminen ja siihen kuuluminen velvoittaa noudattamaan sääntöjä. Organisaatioon sitoutunut työntekijä on motivoitunut tekemään organisaation hyväksi enemmänkin kuin vain se mitä palkan eteen on pakko tehdä.
Mitä voisi tapahtua?	*Henkilö A:lle tarjotaan samanlaista työtä samalla palkalla toisesta organisaatiosta, mutta A kieltäytyy tarjouksesta.*
hypoteesi 2	Tietoturvapolitiikan noudattamattomuudesta on tekijälleen seuraamuksia
selitys (mitä hypoteesi näyttää tarkoittavan)	Siinä missä lain rikkomuksesta seurannut rangaistus on osoitus sekä tekijälle että yhteisölle, ettei näin saa toimia, tietoturvarikkomuksesta seuraa rangaistus, jolla myös osoitetaan sekä tekijälle että yhteisölle, ettei näin saa toimia. Noudattamattomuudessa ei kuitenkaan ole kyse tietämättömyydestä.
Mitä voisi tapahtua?	*Järjestelmän ylläpitäjä toimii vastoin tietoturvapolitiikan ohjetta ja antaa työkaverilleen hänen roolistustaan laajemmat pääsyoikeudet hetkellisesti ilman erillistä lupaa. Ylläpitäjän saama rangaistus tulee julki työyhteisölle.*
hypoteesi 3	Tietoturvapolitiikka ei ole ehdoton
selitys (mitä hypoteesi näyttää tarkoittavan)	Tietoturvapolitiikka sallii tiettyjä ennalta määriteltyjä poikkeuksia (olosuhteita tai toimintoja), jolloin tietoturvapolitiikka ei ole sitova.
Mitä voisi tapahtua?	*Tietoturvapolitiikkaa ei sovelleta tilanteissa, joilla turvataan organisaation ydintoimintoja, kuten esimerkiksi liiketoiminnan vaatimuksista johtuvaa tilapäistä luottamuksellisten tietojen luovutusta.*
2. Liittyykö tietoturvapolitiikkaan sosiaalinen valvonta/sosiaalinen kontrolli?	
hypoteesi 1	Työntekijät paheksuvat (syrjintä, pilkkaaminen, epäilyttävän maineen leima, hyljeksintä tms. sosiaalinen paheksunta) työyhteisössä tapahtuvia tietoturvarikkomuksia
selitys (mitä hypoteesi näyttää tarkoittavan)	Tietoturvapolitiikka on sisäistetty vahvasti toimintaa ohjaavana ja työntekijät ovat tietoisia toistensa tietoturvakäyttäytymisestä. (Normin rikkomiseen puuttuminen on välttämätöntä normin ylläpitämiseksi, sillä normin rikkomisen paheksunta ja siihen puuttuminen (kontrollijärjestelmä) vahvistavat normin olemassaoloa ja säilymistä.)
Mitä voisi tapahtua?	*Henkilö B siirtää organisaation luottamuksellisia tietoja omalle suojaamattomalle muistitikulle. Muut työntekijät näkevät tai saavat*

	muutoin selville tapahtumasta, ja osoittavat selkeästi paheksuntansa joko sanallisesti tai käytöksen kautta, että rikkomus on poikkeavaa käyttäytymistä.
hypoteesi 2	Tietoturvapolitiikkaan liittyy käyttäytymisen yhdenmukaisuus
selitys (mitä hypoteesi näyttää tarkoittavan)	Tietoturvapolitiikan noudattaminen on rutiininomaista, ja kuvastaa sitä, mitä useimmat ihmiset tekevät ja mikä on sosiaalisesti hyväksyttävää. Sosiaalisen hyväksynnän menettämisen pelko vaikuttaa tietoturvapolitiikan noudattamiseen
Mitä voisi tapahtua?	*Henkilö H on sisäistänyt tietoturvapolitiikan mukaiset säännöt, ohjeet, lait ja vaatimukset siten, että tietää ja tuntee eri tilanteiden mukaiset toimintatavat ja käyttäytymissäännöt.*
hypoteesi 3	Tietoturvapolitiikan noudattaminen hyödyttää työyhteisön jäseniä
selitys (mitä hypoteesi näyttää tarkoittavan)	Tietoturvapolitiikan noudattamiseen on vakiintuneet toimintamallit, jotka tekevät mm. käyttäytymisestä ennustettavaa. Tietoturvapolitiikan noudattaminen ei siten hyödytä pelkästään yksittäistä työntekijää.
Mitä voisi tapahtua?	*Tietoturvapolitiikkaa piittaamattomasti rikkova tai tietoturvapolitiikkaa ylenkatsova palautetaan ns. nopeasti ruotuun, tai suljetaan työyhteisön ulkopuolelle.*
3. Opitaanko tietoturvapolitiikan noudattamattomuus?	
hypoteesi 1	Työntekijät oppivat työyhteisön sisällä tietoturvapolitiikan vastaisen asenteen, tekniikat ja motivaation.
selitys (mitä hypoteesi näyttää tarkoittavan)	Työtekijät opettavat toinen toisilleen tietoturvarikkomuksia.
Mitä voisi tapahtua?	*Organisaatiossa X työskentelee tietoteknisiltä taidoiltaan erilaisia henkilöitä, joten* *henkilö A opettaa henkilölle B, kuinka tietoturvaratkaisu teknisesti kierretään. Henkilö A opettaa samalla vähättelemään tietoturvaratkaisua, koska tietoturvaa kiertämällä työt ovat helpompi ja nopeampi tehdä, tai hyöty on jotain henkilökohtaista. Henkilö A opettaa siis kielteiselle teolle suotuisia tapoja, asenteita ja motiivia.*
hypoteesi 2	Työntekijät oppivat työyhteisön sisällä tietoturvarikkomusten selitysmallit (järkiperäistämisen).
selitys (mitä hypoteesi näyttää tarkoittavan)	Organisaatio opettaa, millaiset selitysmallit (neutralisointitekniikat) ovat ko. organisaatiokulttuurissa sosiaalisesti tai yleisesti hyväksyttyjä. Selitysmallit eivät ole kenenkään yksilön luonteenomaisia käyttäytymispiirteitä.
Mitä voisi tapahtua?	*Organisaatio S on rakentanut liiketoimintamallinsa nopean palvelun arvolupaukselle ja se on samalla organisaation kriittinen menestyksentekijä (tukipilari). Kiire on hyväksyttävä selitys, jos siten varmistetaan nopea palvelu, vaikka rikottaisiin tietoturvapolitiikkaa.*