Tiina Vestman

NEUTRALISOIMISTEKNIIKAT ORGANISAATION TIETOTURVAKONTEKSTISSA

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2017

TIIVISTELMÄ

Vestman, Tiina
Neutralisoimistekniikat organisaation tietoturvakontekstissa
Jyväskylä: Jyväskylän yliopisto, 2017, 78 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja: Siponen, Mikko

Työntekijöiden tietoturvapolitiikan mukaisten ohjeiden noudattamattomuus muodostaa organisaation toiminnalle merkittävän tietoturvauhkan. Arviolta puolet tietoturvarikkomuksista tai –loukkauksista tapahtuu työntekijöiden toimesta joko tahallisesti tai tahattomasti. Tutkimalla, miten työntekijät selittävät tietoturvarikkomuksiaan, voidaan tietoturvaohjeiden noudattamattomuuteen löytää selittäviä tai ennustavia syitä. Aikaisemmissa tutkimuksissa on esitetty, että tietoturvarikkomusten aikomuksia tai tietoturvarikkomuksia voidaan selittää neutralisoimisteorian avulla. Neutralisoimisteorian mukaan yksilö puolustelee tai selittelee normeista poikkeavaa käyttäytymistä erilaisten neutralisoimistekniikoiden avulla. Tämä tutkimus käsittelee työntekijöiden kokemuksia ja näkemyksiä tietoturvarikkomusten syistä. Näiden kokemusten ja näkemysten avulla verrattiin sitä, pitävätkö neutralisoimisteorian olettamukset paikkansa tietoturvakontekstissa sekä lisäksi verrattiin sitä, oikeuttavatko työntekijät tietoturvarikkomuksiaan oikeasti neutralisoimistekniikoiden avulla. Tutkimus toteutettiin laadullisena tutkimuksena ja tutkimuksen empiirinen aineisto kerättiin teemahaastatteluilla. Tutkimuksen merkittävin löydös on se, etteivät neutralisoimisteorian keskeiset olettamukset välttämättä pädekään tietoturvallisuuden alueella. Vaikka sosiaalinen järjestys ikään kuin edellyttää jonkinlaista selitystä sille, miksi joku toimii sopimattomasti tai väärin, neutralisoimistekniikat eivät välttämättä selitä tietoturvarikkomuksia. Tutkimuksen tuloksia voidaan hyödyntää tietoturvatoiminnan kehittämisessä ja tietoturvatietoisuuden parantamisessa. Lisäksi tutkimus tarjoaa tiedeyhteisölle sekä uutta tietoa että lukuisia jatkotutkimusaiheita.

Asiasanat: tietoturvallisuus, tietoturvarikkomus, tietoturvapolitiikka,
sosiaalinen normi, neutralisoimisteoria, neutralisoimistekniikat

ABSTRACT

Vestman, Tiina
Techniques of neutralization in the context of organization information security
Jyväskylä: University of Jyväskylä, 2017, 78 p.
Cyber Security, Master's thesis
Supervisor: Siponen, Mikko

Employees' non-compliance with information security policies constitutes a significant information security threat to the organization's operations. It is estimated that half of the information security violations or breaches are caused by employees, either intentionally or unintentionally. By researching how employees explain their security violations, explanatory or predictive reasons of non-compliance with information security policies can be revealed. Previous studies have suggested that intentions of information security violations or information security breaches can be explained by the Neutralization Theory. According to the Neutralization Theory, an individual defends or explains one's behavior that differs from norms or originates from rule-breaking through applying various neutralization techniques. This study discusses employees' experiences and views on the causes of information security violations. With gathered experiences and views of the employees it was made possible to compare if the assumptions of the neutralization theory were correct in the context of the information security and whether the employees justify their information security violations in real life by utilizing neutralization techniques. The study used qualitative research approach. The empirical data of the research was collected through theme interviews. The most notable finding of this study is that the central assumptions of the neutralization theory may not apply to the information security field. Although social order requires some sort of reasoning for why someone is acting improperly or incorrectly, the neutralization techniques may not explain the security violations. The results of this study can be utilized in the development of information security and in enhancing information security awareness. In addition, this study will provide new information to the scientific community and variety of further research topics.

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

KUVIOT

TAULUKOT

SISÄLLYS

KÄSITEHAKEMISTO

Seuraavassa tutkimuksen tietoturvallisuuteen liittyviä keskeisiä käsitteitä:

Tietoturvallisuus (*information security*): Tietoturvallisuudella tarkoitetaan järjestelyitä, joilla pyritään varmistamaan tiedon luottamuksellisuus, eheys ja saatavuus (Tietotekniikan termitalkoot, 2015).

Tietoturvauhka (*information security threats*): Uhka tarkoittaa mahdollisesti toteutuvaa epämieluisaa, pelottavaa tai vahingollista seikkaa, joka uhkaa tai jonka voi kuvitella uhkaavan jotakin (Kotimaisten kielten keskus, n.d.). Tietoturvauhkalla tarkoitetaan uhkaa, joka voi haavoittuvuutta hyödyntäen joko vahingossa tai tarkoituksellisesti vaarantaa tietoturvan (Calder & Watkins, 2010).

Haavoittuvuus (*vulnerability*): Haavoittuvuus määritellään alttiutena tietoturvaan kohdistuville uhkille. Haavoittuvuus voi olla mikä tahansa heikkous, joka mahdollistaa vahingon toteutumisen tai jota voidaan käyttää vahingon aiheuttamisessa. (Tietotekniikan termitalkoot, 2016.)

Tietoturvarikkomus (*information security violation*): Sana rikkomus tarkoittaa käskyjen, sääntöjen tai tapojen vastaista tekoa (Kotimaisten kielten keskus, n.d.). Vaikka rikkomuksen tahallisuus- ja vakavuusaste voivat vaihdella, tarkoittaa tietoturvarikkomus mitä tahansa toimintaa, joka aiheuttaa tietoturvan vaarantumisen (Calder & Watkins, 2010).

1 JOHDANTO

Usein sanotaan, että tieto on tänä päivänä organisaation tärkein omaisuus. Tietoturva on tärkeä ja ajankohtainen aihe, koska sähköinen tieto on haavoittuvainen ja arka tahallisille tai tahattomille muutoksille tai katoamisille. Dhanjanin ym., (2009) mukaan tietoturvauhkat eivät kohdistu yksinomaan tietoverkkoihin, käyttöjärjestelmiin tai erilaisiin sovelluksiin, vaan uudet teknologiat, kuten esimerkiksi lukuisat mukana kuljetettavat mobiililaitteet sekä pilvipalvelut, ovat tuoneet mukanaan uusia haavoittuvuuksia. Työ- ja vapaa-ajan rajojen hämärtyminen, erilaiset ryhmätyövälineet, etätyö, omien laitteiden käyttäminen sekä erilaiset päätelaitteet korostavat tietoturvaohjeiden ja –sääntöjen noudattamista.

Dhillon ym., (2016) selittää, kuinka tietoturvaa uhkaavat haavoittuvuudet syntyvät sosioteknisessä ympäristössä. Sosiotekninen ympäristö koostuu sekä sosiaalisesta että teknisestä ympäristöstä, siis ihmisistä ja teknologiasta, jotka kumpikin muovaavat toisiaan. Sosiaalinen ympäristö edustaa organisaation sosiaalisia normeja, uskomuksia ja käyttäytymismalleja, ja tekninen ympäristö muun muassa organisaation teknistä infrastruktuuria. Tietoturvarikkomuksissa tai –loukkauksissa nämä molemmat ympäristöt on otettava huomioon, koska ne yhdessä muodostavat monimutkaisen kokonaisuuden. (Dhillon ym., 2016.) Vaikka sosiaaliset normit ohjaavat toimintaa, Laineen (2007) mukaan yhteisön asettamia normeja rikotaan, enemmän tai vähemmän, kaikkialla ja kaikkina aikoina. Muun muassa Puhakainen (2006) viittaa siihen, kuinka ihminen voi omalla toiminnallaan kumota teknisten ratkaisujen avulla luodun tietoturvallisuuden. Peltier (2014) puolestaan tuo esille tyypillisiä uhkien aiheuttajia, joita ovat ulkopuolisten niin sanottujen hakkereiden lisäksi virheelliset tai huolimattomat toimintatavat, mutta näiden lisäksi myös luotettavana pidetty työntekijä saattaa pettää koko järjestelmän.

1.1 Tutkimuksen tausta

Tutkimus nojautuu vahvasti neutralisoimisteoriaan, jonka mukaan ihminen oikeuttaa itsensä toimimaan sosiaalisista normeista poikkeavasti erilaisten neutralisoimistekniikoiden avulla. Teoria esitellään yksityiskohtaisemmin myöhemmin luvuissa neljä ja kuusi. Teoriaa on sovellettu selittämään tietoturvarikkomuksia (Cheng ym., 2014; Kim ym., 2014; Li ym., 2013) ja muun muassa Siposen ja Vancen (2010) mukaan neutralisointi ennustaa työntekijöiden tietoturvapolitiikan rikkomisaikeita, koska työntekijät selittävät tai oikeuttavat tietoturvarikkomuksiaan erilaisten neutralisoimistekniikoiden avulla. Siposen ja Vancen (2010) mukaan huolimatta siitä, ettei tietoturvarikkomus tai –loukkaus olisikaan suoranainen rikos, sillä rikotaan silti sosiaalisia normeja. Tutkimustuloksensa perusteella Siponen ja Vance ovat koonneet tärkeimpiä ja yleisimpiä tietoturvarikkomuksia, joita organisaation työntekijät ovat tehneet. Näitä ovat muun muassa työasemien lukitsemattomuus poistuttaessa tietokoneen ääreltä, salasanoja jakaminen työkavereiden ja ystävien kanssa, arkaluonteisten tietojen kopioiminen suojaamattomille muistitikuille, luottamuksellisten tietojen paljastaminen ulkopuolisille tai luottamuksellisten tietojen toimittaminen salaamattomana. (Siponen & Vance, 2010.)

1.2 Aiheen merkitys ja tutkimuksen tavoite

On väitetty, että arviolta lähes puolet tietoturvarikkomuksista tai –loukkauksista tapahtuu joko välillisesti tai suoraan organisaation työntekijöiden toimintatapojen johdosta, koska työntekijät eivät noudata organisaation tietoturvapolitiikkaa (Siponen & Vance, 2010). Riippumatta tietoturvarikkomuksen tahallisuudesta tai tahattomuudesta, sen seuraukset voivat olla yhtä vahingollisia (Crossler ym., 2013). Tietoturvaohjeiden vastainen, tahallinen toiminta saattaa aiheuttaa organisaatiolle merkittäviä, välittömiä vahinkoja, joita ovat tulojen ja kilpailuaseman menetyksen lisäksi myös maineen ja uskottavuuden menetys. Toisaalta välillinen, epäsuora toiminta saattaa luoda haavoittuvuuden tai heikkouden, jota ulkopuoliset voivat hyödyntää hyökkäämällä organisaation sisäisiin järjestelmiin ja tartuttamalla organisaation tietokoneisiin viruksia tai vakoiluohjelmia, jotka ohittavat palomuurin ja pääsevät siten luottamuksellisiin tietoihin. (Crossler ym., 2013.) Baslow ym., (2013) kirjoittavat, ettei myöskään ole mahdollista tehdä eroa pienten ja suurten tietoturvarikkomusten välillä, koska pieneltä vaikuttavalla rikkomuksella saattaa lopulta olla valtavat seuraukset.

Informaatioteknologia kehittyy jatkuvasti ja tuo samalla mukanaan sekä uusia mahdollisuuksia että uhkia. Koska tietoturvassa myös käyttäjät ovat merkittävässä roolissa, ei heitä voida sivuuttaa tai jättää huomiotta. Aihe on tutkimisen arvoinen, koska jos organisaation toimintaan kohdistuva tietoturvauhka tulee organisaation sisältäpäin yhtä merkittävästi kuin ulkoapäin, on tärkeää

tietää ja ymmärtää, mitkä tekijät johtavat sääntöjen, määräysten ja ohjeiden rikkomiseen, jotta esimerkiksi tietoturvaohjeita laadittaessa olisi mahdollista yrittää jo etukäteen torjua virheellisiä toimintatapoja. Jos taustalla vaikuttavia tekijöitä ei kyetä selvittämään, ei ongelmaan voida keksiä myöskään ratkaisua.

Tutkimuksen tavoitteena on löytää selittäviä tai ennustavia syitä siihen, miksi tietoturvaohjeita rikotaan. Tutkimuksen avulla halutaan siis ymmärtää, mitkä tekijät voivat johtaa tietoiseen tietoturvarikkomukseen. Tutkimuksen odotetaan tuovan uutta tietoa.

1.3 Tutkimustehtävä ja rajaus

Tutkimustehtävänä on pyrkiä löytämään vastaus, miten työntekijät selittävät tietoturvarikkomuksiaan. Näiden selitysten avulla pyritään selvittämään ja vertaamaan, pätevätkö neutralisoimisteorian olettamukset tietoturvan yhteydessä ja oikeuttavatko työntekijät oikeasti tietoturvarikkomuksiaan Sykes ja Matzan (1957) neutralisoimisteorian mukaisten neutralisoimistekniikoiden avulla.

Tässä tutkimuksessa keskitytään muutamaan tietoturvakäyttäytymiseen liittyvään tietoturvakäytäntöön, joiden kautta pyritään vastaamaan tutkimuskysymykseen. Näitä tarkasteltavia käytäntöjä ovat:

- salasanojen säännöllinen vaihtaminen
- riittävän vahvan salasanan valitseminen
- epäilyttävien sähköpostiviestien avaamisen välttäminen

Organisaatioissa on usein käytössä erilaisia järjestelmiä, ja kaikissa tulisi käyttää erilaista salasanaa ja muistaa myös vaihtaa salasana säännöllisin väliajoin. Vaikka useat järjestelmät niin sanotusti pakottavat vaihtamaan salasanan säännöllisin väliajoin, kaikkia järjestelmiä ei ole vielä automatisoitu täysin. Vaikka useat järjestelmät ilmoittavat käyttäjälle jo valmiiksi, onko salasana riittävän vahva, sekä varmistavat automaattisesti, ettei samaa salasanaa voi uudelleenkäyttää samassa järjestelmässä, ei eri järjestelmillä useinkaan ole mahdollisuutta tarkastaa, onko sama salasana käytössä ko. henkilöllä jossain toisessa järjestelmässä. Niin sanotut kalasteluviestit ovat olleet runsaasti esillä viime vuosina ja ne ovat aiheuttaneet myös isojakin vahinkoja. Muun muassa Gouglidis ym., (2016) mainitsevat hyökkäyksistä Saksan terästehtaaseen sekä Ukrainan energialaitokseen, joissa molemmissa tapauksissa hyökkäys sekä aloitettiin että lopulta mahdollistettiin niin sanotun kalastelun avulla. Myös niin sanottu kaapattu sähköpostiosoite voi toimia roskapostittajana ja aiheuttaa organisaatiolle muun muassa maineen menetyksen.

1.4 Tutkimuksen rakenne

Tutkimus jakaantuu kahdeksaan lukuun. Luvussa kaksi esitellään tietoturvaan liittyviä käsitteitä, tietoturvakäyttäytymistä sekä organisaatiokulttuurin ja tietoturvakulttuurin merkitystä tietoturvakäyttäytymiseen. Luvussa kolme käsitellään normia, poikkeusta sekä niiden yhteyttä sosiaaliseen kontrolliin ja sosiaaliseen järjestykseen. Luvussa neljä esitellään tutkimuksen keskeinen teoria sekä aiemmat neutralisoimisteoriaa tietoturvakontekstissa soveltaneet tutkimukset. Luvussa viisi kerrotaan tutkimuksen toteutuksesta sekä perustellaan tutkimusmenetelmä. Luku kuusi sisältää tämän tutkimuksen tulkinnan neutralisoimisteoriasta ja sen olettamuksista. Lisäksi luvussa kuusi esitellään tarkemmin, mistä teemoista haastatteluaineisto on koottu ja esitellään tutkimuksen tuloksia. Luvussa seitsemän tarkastellaan tutkimuksen löydöksiä sekä tutkimustulosten perusteella tehtyjä johtopäätöksiä. Samalla tarkastellaan myös tutkimustavoitteen saavuttamista, tutkimuksen luotettavuutta ja esitellään jatkotutkimusaiheita. Viimeinen luku on tutkimuksen yhteenveto.

2 TIETOTURVALLISUUDEN MERKITYS

Tutkimus keskittyy organisaatioympäristöön, joten tässä luvussa esitellään tietoturvaan liittyviä käsitteitä tietoturvaan kohdistuvien tavoitteiden kautta. Samalla tarkastellaan tietoturvallisuuden merkitystä organisaation toiminnalle sekä sitä, kuinka tietoturvallisuutta ohjataan organisaatiossa. Lisäksi tuodaan esille myös työntekijän tärkeä rooli organisaation tietoturvallisuuden yhtenä osatekijänä. Luvun loppuosassa tarkastellaan organisaatiokulttuurin ja organisaation tietoturvakulttuurin osatekijöitä sekä merkitystä tietoturvakäyttäytymiseen.

2.1 Tietoturvallisuus ja tietoturvapolitiikka

Tietoturva on aiheena laaja, eikä tietoturvallisuuden määritelmä ole yksiselitteinen. Andersonin (2003, 309–310) mukaan eri määritelmät eivät kuvaa niinkään sitä, mikä tietoturva on, vaan mitä se tekee. Peltierin (2014) mukaan tietoturvallisuuden tavoitteena on suojata organisaation arvokkaita tietoja, laitteistoja ja ohjelmistoja. Tietoturvallisuuden hallintajärjestelmän vaatimukset määrittävä ISO27001-standardi määrittelee tietoturvan kolmen käsitteen avulla. Näitä ovat tiedon luottamuksellisuus (engl. *confidentiality)*, eheys (engl. *integrity*) ja saatavuus (engl. *availability*). Tietoturva on näiden kolmen tiedolle asetetun tavoitteen suojaamista, koska tietoturvaan liittyvät riskit voivat kohdistua yhteen tai useampaan näistä tietoturvan niin sanotuista kulmakivistä. Luottamuksellisuudella tarkoitetaan sitä, ettei tietoja anneta tai luovuteta oikeudettomille henkilöille tai prosesseille. Se tarkoittaa siis, että vain käyttöoikeuden omaavilla on pääsy kulloinkin kyseessä oleviin tietoihin. Tiedon eheydellä taas tarkoitetaan sitä, ettei tietoihin saa kohdistua perusteettomia ja hallitsemattomia muutoksia, vaan niiden tulee säilyä tarkkoina ja täydellisinä. Tiedon saatavuudella tarkoitetaan, että tietojen tulee olla viiveettä sekä käyttäjien että tietojärjestelmien saatavilla. (Calder, 2008.) Whitman ja Mattord (2011) määrittelevät tietoturvan muodostuvan erilaisista osa-alueista, jotka liittyvät tietojen, laitteiden, tietojärjestelmien ja tietoverkkojen turvaamiseen sekä tietoturvallisuuden

hallintaan. Koska tietoon voi kohdistua monenlaisia, muun muassa ihmisen toimesta aiheutuvia uhkia, kuten tietojen tahallinen tuhoaminen, tahaton vahinko, varkaus tai muunlainen tietoon kohdistuva luvaton muutos tai väärinkäyttö, nostavat Whitman ja Mattord tietoturvaan liittyviksi tekijöiksi luottamuksellisuuden, eheyden ja saatavuuden lisäksi myös tiedon täsmällisyyden, autenttisuuden, käytettävyyden ja hallittavuuden. Tiedon täsmällisyydellä tai tarkkuudella (engl. *accurate*) tarkoitetaan, että tieto on virheetöntä. Täsmällisyyteen liittyy ikään kuin luottamus siitä, ettei tietoon ole kohdistunut perusteettomia muutoksia. Autenttisuudella (engl. *authenticity*) tarkoitetaan, että tieto on muun muassa siellä, missä se luotiin ja minne se sijoitettiin, varastoitiin tai siirrettiin. Se tarkoittaa samalla myös kiistättömyyttä, eli esimerkiksi sitä, ettei suoritettua toimintaa voida jälkikäteen kiistää. Lisäksi tiedon tulee olla käyttökelpoista (engl. *utility*) ja sen hallinnassa (engl. *possession)*, joka tiedon omistaa. Käyttökelpoisuudella tarkoitetaan, että pelkkä tiedon saatavuus ei yksin riitä tiedon hyödynnettävyyteen, mikäli tieto ei ole käyttäjän ymmärtämässä muodossa. Tiedon hallinnalla tarkoitetaan, että tiedon omistajalla on oltava sekä oikeus että mahdollisuus hallinnoida omistamaansa tietoa, kuten esimerkiksi hyödyntää salaustekniikoita. Tällöin tiedon hallinnan vahingoittuminen ei välttämättä riko tai vaaranna luottamuksellisuutta, koska ilman salauksen purkamista, salattu tieto on ulkopuoliselle hyödytön. (Whitman & Mattord, 2011, 8–15.)

Raggadin (2010) mukaan tietoturvallisuus tarkoittaa eri käytäntöjä, joilla pyritään turvaamaan organisaation toiminnan ja palveluiden jatkuvuus. Käytäntöjen avulla pyritään muun muassa turvaamaan tietojen luvaton käyttö, luovuttaminen, muuttaminen, lukeminen, tarkastaminen, tallentaminen tai tuhoaminen. Samalla se tarkoittaa myös tietojärjestelmien suojausta. Kun tiedot ovat tarkkoja, täydellisiä ja oikea-aikaisia, niillä on arvoa organisaation toiminnalle, koska tieto on muun muassa kilpailuedun perusta. Menetetyillä tiedoilla sitä vastoin voi olla lähes katastrofaaliset seuraukset. (Raggad, 2010, 5, 17–18, 205.) Watkins (2013) esittääkin joitakin tekijöitä, jotka ohjaavat organisaation tietoturvaan liittyviä vaatimuksia. Muun muassa asiakkaat ja sidosryhmät haluavat olla varmoja, että heidän tietojaan hallinnoidaan ja suojataan asianmukaisesti. Mikäli organisaatio haluaa säilyttää kilpailukykynsä, suojella immateriaalioikeuksiaan ja mainettaan, on erilaisilla tietoturvajärjestelyillä merkittävä tehtävä organisaation toiminnalle. (Watkins, 2013, 15–17.)

Höne ja Eloff (2002) kuvailevat, kuinka erilaisten kontrollien, säännösten ja toimenpiteiden avulla voidaan varmistaa organisaation tehokas tietoturva. Toimenpiteet sisältävät erilaisia teknisiä ratkaisuja, sopimuksia, riskienhallintaa sekä tietoisuutta uhkista ja haavoittuvuuksista. Kuitenkin tärkein näistä on organisaation tietoturvapolitiikka. Se on asiakirja, joka osoittaa organisaation johdon sitoutumisen tietoturvaan, sekä määrittää tietoturvan roolin organisaation toiminta-ajatuksen ja päämäärien saavuttamiseksi. Tietoturvapolitiikka on dokumentti, joka selittää tietoturvan tarpeellisuuden ja käsitteistöt kaikille organisaation käyttäjille. (Höne ja Eloff , 2002, 402.)

Peltierin (2014) mukaan tietoturva auttaa organisaatiota suojaamaan sen fyysisiä ja taloudellisia resursseja, mainetta, oikeudellista asemaa, työntekijöitä sekä muita aineellisia ja aineettomia hyödykkeitä, joten hyvin laadittu tietoturvapolitiikka on koko tehokkaan tietoturvan kulmakivi. Tietoturvapolitiikka on organisaation ylimmän tason julkilausuma tietoturvan päämääristä, tavoitteista ja menettelytavoista. Tietoturvapolitiikalla on siten kaksi roolia, sisäinen ja ulkoinen. Sisäinen kertoo työntekijöille, kuinka heidän tulisi toimia ja ulkoinen taas kertoo sen, kuinka organisaatio näkee vastuunsa. (Peltier, 2014, 2.) Raggadin (2010) mukaan tietoturvapolitiikka rajaa hyväksyttävät menettelytavat tietojenkäsittely-ympäristössä. Se määrittelee riskit ja tiedon turvaamisen periaatteet, kuten esimerkiksi, miten tietoja turvataan, ketkä käyttäjät tai mitkä prosessit oikeutetaan käyttämään mitäkin tietoja sekä sen, millaiseen toimintaan tietojen käyttö hyväksytään. Lisäksi tietoturvapolitiikassa eritellään organisaation eri osa-aluiden vastuualueet. (Raggad, 2010, 11, 161, 172–180.) Bulgurcu, Cavusoglu ja Benbasat (2010, 526-527) puolestaan määrittävät tietoturvapolitiikan ohjeeksi, joka kertoo työntekijöiden tehtävät ja vastuut organisaation tietojen ja teknologiaresurssien turvaamiseksi. Tietoturvapolitiikka ei siis ole vain teknisesti hallittavissa olevia käytäntöjä ja menettelytapoja, vaan sen tarkoituksena on ohjata ja säädellä myös käyttäytymistä (Boss ym., 2009, 152–153). 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. Vaccan mukaan hyvä tietoturvapolitiikka ei ole vain yksi asiakirja, vaan pikemminkin se on joukko erilaisille asioille määriteltyjä politiikkoja. Näitä voivat olla muun muassa sähköpostiin, etätyöhön, mobiiliteknologian käyttöön sekä tietokoneen ja verkon käyttöön liittyviä periaatteita. Tietoturvapolitiikan tulee olla kattava, helposti ymmärrettävä kokonaisuus, joka on sovitettavissa organisaation toimintaan. Koska tietoturvauhkat ja haavoittuvuudet muuttuvat, on tietoturvapolitiikankin kehityttävä ja muututtava yhdessä teknologian kehityksen mukana. Toisaalta tietoturvapolitiikan tulee ohjata työntekijöitä kaikissa eri tilanteissa. (Vacca, 2014, 34–35, 43–50.)

2.2 Tietoturvakäyttäytyminen

Kuten jo edellä mainittiin, tietoturvapolitiikan tarkoituksena on ohjata ja säädellä toimintaa ja käyttäytymistä. Tietoturvallisuudessa moni organisaatio keskittyy organisaation ulkopuolelta tuleviin uhkiin, vaikka myös työntekijät voivat muodostaa uhkan muun muassa vuotamalla organisaation luottamuksellisia asiakirjoja tai tietoja kilpailijoille. Työntekijöiden asenteet ja toimet ovatkin kasvaneet yhä merkittävämmäksi tekijäksi tietoturvallisuudessa. (Iivonen, 2011, 148.) Vaikka teknologia kehittää jatkuvasti menetelmiä ja työkaluja kriittisten tietojen turvaamiseen ja suojaamiseen, tekniikka yksin ei kuitenkaan välttämättä riitä organisaation tietovarantojen suojaamiseen (Siponen, Willison ja Baskerville, 2008). Usein sanotaankin, että ihminen on tietoturvan heikoin

lenkki (Bulgurcu ym., 2010, 523). Organisaation tietoturvassa onnistumisen, tai epäonnistumisen, yhtenä lähestymistapana on eri tutkimuksissa keskitytty tietoturvakäyttäytymiseen, eli siihen, mitä työntekijät tekevät tai eivät tee (Da Viega & Eloff, 2010, 196). Guo (2013) määrittelee tietoturvakäyttäytymisen tarkoittavan organisaation tietojärjestelmiin liittyvää käyttäytymistä ja toimintaa, joka vaikuttaa tietoturvallisuuteen. Tietojärjestelmiin luetaan kuuluvaksi niin laitteet, ohjelmistot kuin tietoverkot, mutta samaan yhteyteen kuuluvat yhtä hyvin myös henkilöstön toimet, kuten esimerkiksi se, kuinka henkilöstö huolehtii omista salasanoistaan, kuinka he käsittelevät organisaation tietoja, tai miten he käyttävät tietoverkon resursseja. (Guo, 2013, 243.)

Useat tietoturvakäyttäytymiseen liittyvät tutkimukset ovat keskittyneet erilaisten teoreettisten lähestymistapojen kautta löytämään keinoja, kuinka työntekijöitä voitaisiin motivoida huomioimaan heidän tärkeä roolinsa organisaation tietoturvallisuuden yhtenä osatekijänä. Motivoinnin keinoista on tutkimuksissa sovellettu muun muassa Deci ja Ryan motivaatioteoriaa (Kinnunen, 2015) sekä suojelumotivaatiteoriaa (engl. *protection motivation theory*) tai sen osia (Boss ym., 2015; Johnston ym., 2015; Siponen ym., 2014). Suojelumotivaatioteorian perustana on ollut malli, joka mukaan on tärkeää herättää riittävästi pelkoa motivoimaan suositeltavaa tai toivottavaa käyttäytymistä, mutta kuitenkin vain sen verran, että suositellun käyttäytymisen noudattaminen kumoaa pelkoreaktion. Tätä mallia on toteutettu erityisesti terveydenhoitoalalla, mutta myös tietoturvan yhteydessä. (Johnston ym., 2015, 114-115.) Toisaalta Boss ym., (2015, 44-45) tuovat esille näkökulman siitä, ettei pelkoon vetoaminen (engl. *fear appeal*) välttämättä toimi, koska samaan tapaan kuin yksilö muodostaa uhkaarvion, hän voi hahmottaa myös, kuinka hallita tilannetta, eli luoda ikään kuin selviytymisstrategian. Kuitenkin myös peloteteoria (engl. *deterrence theory*) on yksi useimmin käytetyistä teorioista etenkin tietoturvallisuuskäyttäytymisen tutkimuksissa (D'arcy & Herath , 2011).

Johnston ym., (2015, 120) mukaan huolimatta peloteteorian yhteydestä kriminologiaan, ja rikollisen ja poikkeavan käyttäytymisen ymmärtämiseen, sen oletukset ovat päteviä tietoturvapolitiikan noudattamisen havainnoinnissa. Peloteteorian keskeisenä ajatuksena on, että teon seurausten pelko estää toimimasta tietyllä tavalla ja siten esimerkiksi rangaistuksen pelko estää rikoksia. Teorian taustaoletuksena on, että henkilö tekee ikään kuin arvion seurausten vakavuudesta sekä rangaistuksen todennäköisyydestä päättäessään rikkoa sosiaalista normia tai vakiintuneita käytäntöjä. (Johnston ym., 2015.) Toisaalta seuraamusten tai rangaistusten pelko ei välttämättä toimi ohjaavana tekijänä työntekijöiden tietoturvakäyttäytymisessä, koska työntekijät oikeuttavat tietoturvarikkomuksensa neutralisoimistekniikoiden avulla (Siponen & Vance, 2010.) Nämä neutralisoimisteorian neutralisoimistekniikat esitellään tässä tutkimuksessa tarkemmin luvussa neljä.

Myös Stanton, Stam, Mastrangelo, ja Jolton, (2005) tutkimuksen näkökulmana oli organisaation tietoturvakäyttäytyminen ja työntekijöiden muodostamat uhkat. Stanton ym., (2005, 126) tutkimuksessa käyttäjät on jaettu kuuteen niin sanottuun käyttäytymismalliin. Esimerkiksi vahvan teknisen taustan omaa-

va työntekijä kykenee murtamaan työnantajansa suojattuja tiedostoja ja myymään niitä eteenpäin, kun taas toisaalla työntekijän kokemattomuus voi aiheuttaa uhkan, vaikkei tarkoituksena olekaan aiheuttaa organisaatiolle mitään vahinkoa (Stanton ym., 2005, 127). Mallin mukaan loppukäyttäjän tekniset tiedot ja taidot vaikuttavat tietoturvakäyttäytymiseen.

Stanton ym., (2005) mallissa esitellään sekä kielteistä että myönteistä käyttäytymistä. Mallissa käyttäytymisen on jaettu tahalliseen tuhoamiseen (engl. *intentional destruction*), vahingolliseen/haitalliseen väärinkäyttöön (engl. *detrimental misuse*), vaaralliseen korjailuun (puuhasteluun) (engl. *dangerous tinkering*), kokemattomuus virheisiin (engl. *naïve mistakes*), tietoiseen varmuuteen (engl. *aware assurance*) ja perushygieniaan (taitoihin) (engl. *basic hygiene*). Tahalliseen tuhoamiseen liittyvä käyttäytyminen edellyttää sekä teknistä osaamista että vahvaa aikomusta vahingoittaa organisaation resursseja. Vahingollinen väärinkäyttö ei puolestaan vaadi hyvää teknistä asiantuntemusta, vaan aikomuksen aiheuttaa vahinkoa, haittaa tai sääntörikkomuksia. Vaarallinen korjailu (puuhastelu) liittyy käyttäytymiseen, joka vaatii teknistä osaamista, mutta mitään selkeää aikomusta vahingon aiheuttamisesta ei ole. Kokemattomuus virheet eivät vaadi teknistä osaamista, mutta myöskään niissä ei ole aikomusta aiheuttaa haittaa tai vahinkoa. Tietoinen varmuus liittyy käyttäytymiseen, joka vaatii teknistä osaamista sekä vahvan myönteisen asenteen organisaation resurssien suojaamiseen. Myös niin sanottuun perushygieniaan liittyvä käyttäytyminen osoittaa myönteistä tahtoa organisaation resurssien suojaamiseksi, eikä vaadi teknistä osaamista. (Stanton ym., 2005, 126–127.)

2.3 Organisaatiokulttuuri ja organisaation tietoturvakulttuuri

Kuten jo johdanto luvussa mainittiin, on tietoturvassakin otettava huomioon organisaation sosiaalinen ympäristö. Se edustaa organisaation sosiaalisia normeja, uskomuksia ja käyttäytymismalleja, joiden kautta myös tietoturvakulttuuria luodaan. Koska organisaatiokulttuuri on aiheena laaja ja käsittää erilaisia määritelmiä ja teorioita, jäsennetään tässä tutkimuksessa organisaatiokulttuuria Scheinin esittämän mallin mukaan. Scheinin organisaatiokulttuuriteoria havainnollistaa organisaatiokulttuurin eri tasot ja niiden välisen vuorovaikutuksen. Malli soveltuu selittämään liike-elämän ja julkishallinnon organisaatiokulttuurin lisäksi myös tietoturvakulttuuria, joten valinta on luonteva tälle tutkimukselle.

Scheinin (1991, 14) mukaan kulttuuri ei rajoitu vain maakohtaisesti, vaan kulttuuria on kaikkialla, missä on ryhmiä. Yhtenäisiä kokemuksia on oltava riittävästi, jotta ne johtaisivat yhteiseen näkemykseen ja yhteisen näkemyksen tulee toimia riittävän pitkään, jotta siitä muodostuu itsestäänselvyys ja toiminta siirtyy tiedostamattomalle tasolle (Schein, 1991, 25). Schein (1991, 31) jakaa kulttuurin niin sanotusti kolmeen eri osatekijään, joista myös organisaatiokulttuuri koostuu. Osatekijät voidaan nähdä ikään kuin tasoina, joiden kautta on mahdollista tarkastella eri tasojen välistä vuorovaikutusta.

Scheinin (1991) mukaan kulttuurin ensimmäisellä, näkyvimmällä tasolla ovat artefaktit ja luomukset, eli ihmistyön aikaansaannokset. Tällä tarkoitetaan muun muassa ihmisen rakentamaa fyysistä ja sosiaalista ympäristöä, kuten fyysiset tilat, puhuttu ja kirjoitettu kieli, ja ryhmän jäsenten havaittavissa oleva käyttäytyminen. Scheinin mukaan pelkän näkyvän käyttäytymisen havainnointi ei kuitenkaan yksin selitä, miksi ryhmän jäsenet käyttäytyvät kuten he käyttäytyvät, koska havainnointi ei välttämättä kykene selittämään muun muassa keskinäisiä, syvällä rakenteissa olevia suhteita. (Schein, 1991, 32–33.)

Scheinin (1991) mallin toisella tasolla sijaitsee syvempi tiedostamisen taso. Organisaatiokulttuurin näkökulmasta tällä tasolla sijaitsevat organisaation viralliset arvot, kuten toimintaa ohjaavat viralliset periaatteet ja normit. Scheinin mukaan ne on tietoisesti valittuja ja selkeästi ilmaistuja, eikä niihin välttämättä liity niin sanottua historiallista näyttöä siitä, että arvot myötävaikuttaisivat organisaation menestykseen toimintaympäristössään. On siis täysin mahdollista, että arvojen mukaisen ja todellisen toiminnan välille muodostuu ristiriita. Mikäli arvot eivät perustu kulttuurissa tapahtuneeseen oppimiseen, saatetaan sanoa yhtä ja toimia toisin. Scheinin mukaan kulttuurinen oppiminen tarkoittaa sitä prosessia, jossa arvo kokee vähittäisen kognitiivisen muodonmuutoksen muuttuen ensin uskomukseksi ja lopulta oletukseksi. Vasta tuon prosessin myötä arvot muuttuvat tietoiselta tasolta alitajuisiksi ja automaattisiksi tavoiksi. Kaikki arvot eivät kuitenkaan koskaan muutu lopulta itsestäänselvyyksiksi. (Schein, 1991, 33–35.)

Scheinin (1991, 32) mallin alimmalla tasolla ovat perusoletukset, jotka ovat alitajuisia, näkymättömiä ja muodostuneet itsestäänselvyyksiksi. Perusoletukset toimivat kulttuurin ytimenä, sellaisena mitä kulttuuri todella on. Scheinin mukaan ne ovat myös vastaansanomattomia ja kiistattomia. Ryhmän kannalta perusoletusten merkitys näkyy muun muassa siinä, että ryhmä on vahvasti yhteisten perusolettamusten takana ja ryhmän perusolettamuksien vastaista käyttäytymistä pidetään käsittämättömänä. Tällaiset alitajuiset oletukset voivat kuitenkin vääristää tosiasioita, koska ne ohjaavat sitä, miten tulkitsemme toisten ihmisten käyttäytymistä. (Schein, 1991, 31, 36–37.)

Van Niekerkin ja Von Solmsin (2010) mukaan perusoletukset vaikuttavat yksilöiden normaaliin jokapäiväiseen toimintaan. Samalla ne vaikuttavat myös siihen, kuinka kukin tulkitsee organisaation toimintaperiaatteita ja menettelytapoja. Organisaation viralliset arvot voidaan nähdä johdon organisaatiokulttuurin suunnannäyttäjinä, mutta kuitenkin käyttäytymisen taustalla vaikuttavat perusoletukset. Organisaation tietoturvan näkökulmasta, kulttuurin tasot voidaan rinnastaa niin sanottuun inhimilliseen tekijään, joka koostuu tietämyksestä ja käyttäytymisestä, jotka molemmat liittyvät vahvasti toisiinsa. (Van Niekerk ja Von Solms, 2010, 478.) Sanalla tietoturvallisuuskulttuuri viitataankin käsitykseen siitä, miten tietoturvallisuuden periaatteet ilmenevät organisaation päivittäisessä toiminnassa ja millainen työntekijöiden käyttäytyminen on hyväksyttävää ja suositeltavaa (Iivonen, 2011, 148).

Van Niekerk ja Von Solms (2010, 478) esittävät, ettei organisaatiokulttuurin määritelmässä yleensä huomioida itse työn tekemiseen tarvittaa tietämystä,

koska yleisenä oletuksena on, että työntekijällä on työnsä tekemiseen tarvittava riittävä tietämys. Van Niekerk ja Von Solms esittävät myös, ettei työntekijä välttämättä tarvitse tavanomaisissa työtehtävissään tietoturvaan liittyvää tietämystä, vaan tietämystä tarvitaan vain silloin, kun normaalien työtehtävien on oltava sopusoinnussa hyvien tietoturvakäytänteiden kanssa. Mikäli organisaatio siis haluaa edistää tietoturvakulttuuria, tulisi kaikki toiminta suorittaa hyvien tietoturvakäytänteiden mukaisesti. (Van Niekerk & Von Solms, 2010, 478.) Van Niekerk ja Von Solms (2010, 478–479) ovat muokanneet (kuvio 1) Scheinin (1991) kulttuurin tasojen pohjalta nelitasoisen tietoturvakulttuurin mallin.

KUVIO 1 Tietoturvakulttuurin kerrokset (mukailtu Van Niekerk & Von Solms, 2010, s. 479)

Van Niekerk ja Von Solms (2010, 478–481) esittämän mallin ajatuksena on, että organisaatiokulttuurin jokainen taso voi vaikuttaa tietoturvakulttuuriin joko myönteisesti tai kielteisesti, koska eri tasot ovat vuorovaikutuksessa keskenään. Mallissa korostetaan sitä, että ilman riittävää tietämystä tietoturvan merkityksestä, ei tietoturvakulttuuri voi vastata sille asetettuja tavoitteita (Van Niekerk & Von Solms, 2010, 481). Se, että jokin asia muuttuu itsestäänselvyydeksi, edellyttää asian sisäistämistä. Muun muassa Tsohou, Karyda ja Kokolakis (2015, 128) sekä Siponen (2006, 97-99) kritisovat sitä, etteivät tietoturvallisuuden standardit ja parhaat käytännöt huomio riittävästi, kuinka yksilö sisäistää tietoturvallisuuteen liittyvän tiedon ja kuinka yksilö tekee siihen liittyviä päätöksiä. Kuitenkin yksilön käsitykset, uskomukset ja ennakkoluulot vaikuttavat tietoturvakäyttäytymiseen ja tietoturvapolitiikan noudattamiseen (Tsohou ym., 2015, 128).

Raggadin (2010) mukaan vain työntekijöiden riittävä ymmärrys tietoturvallisuusjärjestelmien tarpeellisuudesta, saa organisaation tietoturvakulttuurin kehittymään vähitellen. Tällöin ihmiset esimerkiksi kykenevät tunnistamaan järjestelmää vahingoittavat komponentit (ihmiset, teknologiat, toiminnat, tiedot ja tietoverkot), raportoimaan tietoturvaloukkauksista, sekä käyttäytymään

tietoturvapolitiikan määräysten mukaisesti. Raggadin mukaan ilman tietoturvakulttuuria, ihmiset voivat myös tahattomasti ja vahingossa vaarantaa tietojenkäsittely-ympäristön. He saattavat vaarantaa tietojen eheyden muun muassa vahingoittamalla tai vuotamalla tietoja. Toisaalta he voivat myös estää tietojen saannin henkilöltä, joka sitä tarvitsisi. (Raggad, 2010, 12, 289–290.)

3 NORMI, POIKKEAVUUS JA SOSIAALINEN KONTROLLI

Kuten edellisessä luvussa jo mainittiin, organisaatioiden toiminta pitää sisällään sosiaalisia normeja ja käyttäytymismalleja. Koska tutkimuksen keskeisin teoria käsittelee poikkeavuuden oikeutusta, käsitellään tässä luvussa ensin normin määritelmä. Sen jälkeen esitellään poikkeavuuteen liittyviä määritelmiä, sekä kerrotaan, miten normi ja poikkeavuus liittyvät toisiinsa. Lisäksi tässä luvussa tarkastellaan sosiaalisen kontrollin ja sosiaalisen järjestyksen yhteyttä normiin ja poikkeavuuteen. Vaikka sosiaalinen kontrolli viittaakin kontrolli-teoriaan, sen teorian käsittely jätetään tämän tutkimuksen ulkopuolelle.

3.1 Normi

Normille löytyy erilaisia määritelmiä riippuen tieteenalasta ja määrittelijästä. Tieteen termipankki sivustolla (2015) sana normi on määritelty muun muassa filosofian ja oikeustieteen osioissa. Filosofiassa normi on määritelty palkintojen ja rangaistuksen avulla ylläpidettäväksi sosiaaliseksi säännöksi. Oikeussosiologiassa normilla viitataan ihmisten väliseen vuorovaikutukseen, jonka kautta yhteisö saa jäsenensä toimimaan tai ajattelemaan yhdenmukaisella tavalla. (Tieteen termipankki, 2015.) Salmivalli ja Voeten (2004, 249) puolestaan esittävät käsitteen ryhmänormi, jolloin ryhmän normin mukainen käyttäytyminen johtaa myönteisiin seurauksiin ja ryhmän muiden jäsenten hyväksyntään, kun taas normien rikkominen johtaa kielteisiin seurauksiin ja ryhmän paheksuntaan. Yhteistä näiden eri tieteenalojen määritelmässä on se, että normin avulla vaikutetaan ihmisen käyttäytymiseen ja toimintaan yhteisössä. Laineen (2007, 17) mukaan normin ei tarvitse olla kirjoitettu laki tai säädös, vaan myös epäviralliset normit ohjaavat toimintaa, usein jopa virallisia normeja enemmän. Laine (2007) jatkaa, että normilla on yhteys sosiaaliseen kontrolliin, jolla tarkoitetaan sitä, että normista tulee normi vasta, kun sen noudattamista kontrolloi ja valvoo ihmisten muodostama yhteisö. Toisaalta on myös täysin mahdollista, että sää-

dettyä normia, kuten esimerkiksi lakia, ei pidetä varsinaisena normina, koska ihmiset eivät omaksu sitä, eivätkä siten myöskään noudata sitä. Normille on myös tyypillistä se, ettei sitä luoda pelkällä ulkoisella pakolla tai negatiivisten sanktioiden uhkalla. Sitä vastoin, positiivisten sanktioiden, eli palkkioiden, on arveltu toimivan paremmin normien vahvistajana kuin pelkkä rangaistuksen uhka. (Laine, 2007, 17–19.) Suonisen (1997) mukaan normit sisäistetään kognitiivisten mekanismien kautta, jolloin ilman sisäistämistä, normi ei saavuta sen toimintaa ohjaavaa merkitystä.

Toisin kuin lakia, normia ei voi rikkoa, siitä voi vain poiketa, eikä se siten kiinnity (rangaistavaan) tekoon, vaan (poikkeavaan) yksilöön (Jauho, 2003, 45). Ewaldin (2003) mukaan normi ei kuitenkaan ole yksilöllistä, vaan se toimii yksilöiden välisenä siteenä. Normin luo ryhmä, ilman, että kukaan sitä ehdottomasti haluisi. Sitä ei myöskään julisteta eikä sitä voida asettaa ryhmän ulkopuolisen yksipuolisella päätöksellä, vaan se neuvotellaan. Normi lukeutuu enemmän tosiasioihin kuin oikeuden järjestykseen, koska sen olemassaolo todetaan ja havaitaan ilman, että siihen liittyisi nimenomaista noudattamisvaatimusta. Ehdoton normi menettäisi luonteensa ja etunsa. Normi ei ole täysin rinnastettavissa yhteiseen haluun toteuttaa yhteisen edun mukaisia toimenpiteitä, vaan se toimii mittapuuna, joka mahdollistaa vertailtavuuden. Se sijoittaa tosiasiat ikään kuin eräänlaiselle jatkuvalle asteikolle ja erottaa normaalin epänormaalista keskiarvojen, kynnysten ja rajojen avulla. Perinteisesti sääntöjen ajatellaan perustuvan varmoille, järkeville ja universaaleille periaatteille, jotka ovat päteviä ajasta ja paikasta riippumatta. Normi ei kuitenkaan ole satunnainen sääntö, vaan suhteellinen ja muuttuva. Se ei myöskään ole universaali, vaan pätevä vain tietyssä ryhmässä, ja sen tulee muuttua yhdessä ryhmän käytäntöjen muutosten kanssa. Tästä syystä tietyn ryhmän normia ei välttämättä voida soveltaa johonkin toiseen ryhmään. Myös ympäristöllä on oma vaikutuksensa normiin. Vaikka esimerkiksi tekniset normit noudattavat erilaista aikataulua kuin useat muunlaiset normit, nekin voivat muuttua vain hitaasti, koska muutos on sidoksissa teknisen innovaation lisäksi myös ympäristön vastaanotto- ja omaksumiskykyyn. Ympäristö usein vastustaa muutosta siitä aiheutuvan tasapainotilan järkkymisen vuoksi. (Ewald, 2003, 20–67.)

3.2 Poikkeavuus

Käsitteenä poikkeavuus (engl. *deviance*) on ikään kuin normin vastakkainen puoli, eli jokin käyttäytyminen poikkeaa normeista. Tieteen termipankki sivustolla (2015) poikkeava käyttäytyminen määritellään joko yksilöä tai ulkopuolista yhteisöä vahingoittavaksi toiminnaksi. Franzesen (2015) mukaan perinteisesti poikkeavaksi käyttäytymiseksi on katsottu esimerkiksi mielenterveyden häiriöt, erilaiset riippuvuudet, päihteiden käyttö ja rikollinen käyttäytyminen. Laineen (2007, 19) mukaan poikkeavuuden määrittäminen ei ole täysin ongelmatonta, koska ei voida täysin määrittää, missä kulkee poikkeavuuden raja ja kuka rajan määrittää. Toisaalta myös poikkeavuuden tilastollinen määrittä-

minen on hankalaa, koska ihminen rikkoo päivittäin useita erilaisia normeja, niin perheessä, työpaikoilla kuin tuttavapiirissä. Poikkeavuus onkin siten sidoksissa myös olosuhteisiin. Sama käyttäytyminen on toisessa tilanteessa poikkeus ja toisessa ei. Poikkeavuus, sen määrittely ja kontrollointi ovat siten vahvasti sidoksissa siihen kulttuuriin, jossa eletään. Laineen mukaan poikkeavuudelle tai poikkeavalle käyttäytymiselle on lähes mahdoton löytää täydellistä, yleisesti hyväksyttyä ja tarkkaa määritelmää. Se on sopimuksenvarainen asia, ja kulttuurien erot poikkeavan käyttäytymisen määrittämisessä ja sen mahdollisissa sanktioissa ovat suuret. (Laine, 2007, 19–26.) Franzese (2015) kuitenkin toteaa, että määritelmien eroavaisuuksista huolimatta niistä on löydettävissä myös yhtäläisyyksiä. Ensinnäkin poikkeavuus liitetään käyttäytymiseen ja sosiaaliseen normiin tai yhteiskunnallisesti hyväksyttyyn tapaan toimia. Toiseksi määritelmissä tuodaan esille se, että poikkeavuus liittyy sosiaalisiin prosesseihin ja kommunikointiin. Lisäksi eri määritelmissä käytetään ilmaisuja kuten kontrolli, paheksunta ja seuraamukset. Näillä viitataan siihen, että poikkeavuus edellyttää reaktiota tai käyttäytymisen tunnistamista esimerkiksi ärsyttävänä, häiritsevänä tai jopa uhkaavana. Tarvitaan siis ikään kuin yleisö, joka arvio ja tuomitsee yksilön tai ryhmän toiminnan. (Franzese, 2015.) Laine (2007, 41) mainitsee, että ilman normia ja poikkeavuutta, ei olisi helppoa osoittaa, mikä on sallittua ja mikä ei. Eli normi ei ole normi, jollei siitä poiketa.

3.3 Sosiaalinen kontrolli ja järjestys

Blackin (2010) mukaan sosiaalinen kontrolli on keskeinen ihmisen käyttäytymiseen liittyvä käsite. Usein yhteiskunta tai muu yhteisö määrittää hyväksyttävän käyttäytymisen rajat. Sosiaalista elämää ikään kuin ohjataan erilaisilla ohjeilla, säännöillä, kielloilla ja rangaistuksilla, koska poikkeava käyttäytyminen saatetaan kokea ongelmaksi. Vaikka lait luovat virallisen sosiaalisen kontrollin, voi epävirallisella kontrollilla silti olla merkittävämpi vaikutus siihen, mitä teemme tai emme tee, koska myös kulttuuri luo mallit ja arvot, joiden kautta yksilö jäsentää ja ymmärtää maailmaa. Sosiaalinen kontrolli kuitenkin ennustaa ja selittää, miten ihmiset määrittävät poikkeavan käyttäytymisen sekä sen, kuinka he reagoivat siihen. (Black, 2010, 1–36; Black, 1983, 34.)

Innesin (2003) mukaan sosiaaliselle kontrollilla (engl. *social control*) on läheinen yhteys sosiaaliseen järjestykseen (engl. *social order*). Pohjimmiltaan kyse on siitä, kuinka sosiaaliset toimijat, joko yksilöt tai ryhmät, mukautuvat normeihin ja sääntöihin. Sosiaalisella kontrollilla tarkoitetaan usein yhteiskunnan sosiaalisen järjestyksen ylläpitoa. Yhteiskuntajärjestyksellä viitataan yhteiskunnan olemassaolon edellytyksiin, eli siihen, kuinka yhteiskunnissa on luontaisesti järjestäytymisaste ja siten sosiaalinen järjestys. Järjestys ei kuitenkaan ole staattinen, vaan alati muuttuva, ja siten se myös uudistaa arvoja, käytäntöjä, asenteita ja jäsentensä toimia. Sosiaalisella kontrollilla tarkoitetaan prosessia, jolla pyritään hallitsemaan sitä, mikä poikkeaa yhteiskuntajärjestyksestä tai on sen kanssa ristiriidassa. (Innes, 2003, 6–7.)

Innesin (2003) mukaan sosiaalisen kontrollin määrittelyyn liittyy monimutkaistavia tekijöitä. Sosiaalinen kontrolli jaetaan usein viralliseen ja epäviralliseen, mutta aina ei ole täysin selvää, onko tuollainen erottelu tarkoituksenmukaista. Lisäksi sosiaalista kontrollia on mahdollista tarkastella myös reaktiivisena tai ennakoivana. Reaktiivisuudella tarkoitetaan reaktiona ilmenevää, ulkoisesta ärsykkeestä syntyvää reaktiota. Reaktiivista sosiaalista kontrollia käytetään vasta sen jälkeen, kun jotain on tapahtunut. Tällaista on muun muassa poliisin tekemä rikostutkinta. Ennakoivaa sosiaalista kontrollia taas hyödynnetään arvioitaessa tulevaisuuden tapahtumia. (Innes, 2003, 6–7.)

Kuhn (2009) puolestaan kuvailee, kuinka perinteisissä rikosteorioissa oletetaan yleisesti, että yhdenmukaisuus ja lainkuuliaisuus yhteiskunnan lakeja kohtaan on luontaista. Kontrolliteoriat puolestaan olettavat, että sopeutumattomuutta ja lainvastaisuutta on odotettavissa silloin, kun sosiaalista kontrollia ei ole olemassa tai se on tehotonta. Jo pelkästään se, että on olemassa lakeja ja sääntöjä, osoittaa niiden tulleen luoduksi tarpeeseen. Jos kaikki olisivat kaikkina hetkinä yhtä mieltä siitä, kuinka tulee käyttäytyä, ei silloin myöskään käyttäytymistä tarvitsisi ohjata sääntöjen avulla. (Kuhn, 2009, 2–4.)

Suoninen (1997) on suomentanut Scott ja Lyman (1968) artikkelissa mainitun englanninkielisen *account*-termin tarkoittavan selontekoa. Suoninen (1997) määrittelee selonteon tarkoittavan: ”tapoja tehdä kielellisesti ymmärrettäväksi tai kulttuurisessa mielessä järjelliseksi omaa toimintaansa tai toisten toimintaa”. Tässä tutkimuksessa myötäillään Suonisen määrittelemää käsitettä. Scott ja Lyman (1968, 46) määrittelevät selonteon ikään kuin selvitykseksi, jolla sosiaalinen toimija, eli yksilö, selittää joko omaa tai toisten odottamatonta tai yllättävää käyttäytymistä ja käyttäytymisen kausaalista syy-yhteyttä. Scottin ja Lymanin (1968, 46) mukaan selonteoksi kutsutut keinot selittää toimintaa ja käyttäytymistä ovat keskeinen osa sosiaalista järjestystä. Ne toimivat ikään kuin siltana toiminnan ja odotusten välisessä kuilussa, ja ehkäisevät konfliktien syntymistä. Kun ihminen käyttäytyy oman kulttuuriympäristönsä rutiinien mukaisesti, ”maalaisjärjellä” ymmärrettävästi, selonteoille ei ole tarvetta. Tietynlainen käyttäytyminen on tietyssä kulttuuriympäristössä niin itsestäänselvyys, ettei sen syitä edes kysytä. Päinvastoin, kysyjää saatettaisiin oudoksua, jos itsestäänselvänä pidettyyn käyttäytymiseen pyrkisi löytämään syitä selontekojen kautta. (Scott ja Lyman, 1968, 47.)

Scottin ja Lymanin (1968, 47) mukaan on olemassa kahdenlaisia selontekoja: pahoittelevia ja oikeuttavia. Molemmilla selonteoilla viitataan tekoihin, jotka ovat sopimattomia, väärin, ei-toivottuja tai muuten odottamattomia nimenomaan negatiivisessa mielessä. Vaikka molemmat selonteot käyttävät niin sanotusti kielellisiä, sosiaalisesti hyväksyttyjä keinoja selittää tai perustella tekoa ja sen seurauksia, on selonteoissa silti ratkaiseva ero. Pahoitteleva selonteko liittyy tilanteisiin, joissa tekijä myöntää, että teko oli sopimaton, mutta kiistää vastuunsa täysin. Oikeuttavassa selonteossa tekijä kiistää teon vääryyden tai halveksittavuuden. Pahoittelevat selonteot viittaavat siis tilanteisiin, jotka pyrkivät tekemään rikkomuksia tai poikkeavuuttaa ymmärrettäväksi kiistämättä rikotuksi tulleen normin mielekkyyttä. Oikeuttavat selonteot puo-

lestaan viittaavat suoraan normin kanssa kilpailevaan normiin, tai sitä suhteellistavaan näkökulmaan. (Scott ja Lyman, 1968, 47–51; Suoninen, 1997.)

Scottin ja Lymanin (1968) mukaan pahoitteleva selonteko on esimerkiksi selitys onnettomuudesta, koska on epätodennäköistä, että sama onnettomuus tapahtuisi samalle henkilölle usein, jolloin selontekoa voidaan pitää hyväksyttävänä. Toisaalta henkilö voi vedota teon mitättömyyteen, eli vähätellä koko asiaa. Pahoitteleva selonteko voi liittyä myös niin sanottuihin mentaalisiin elementteihin, joita ovat muun muassa tieto ja tahto. Henkilö esimerkiksi puolustautuu vedoten riittämättömiin saatavilla oleviin tietoihin tai virheellisiin ja vääristeltyihin tietoihin. Scott ja Lyman esittelevät pahoittelevina selontekoina myös vetoamisen vapaan tahdon menetykseen ja biologisiin vietteihin, mutta niiden käsittely tämän tutkimuksen yhteydessä ei olisi tutkimuksen tavoitteisiin nähden relevanttia, joten niitä ei käsitellä tässä yhteydessä mainintaa enempää. (Scott ja Lyman, 1968, 48–50.) Viimeisenä pahoittelevana selontekona Scott ja Lyman (1968, 50) mainitsevat toisten syyllistämisen, eli tekijä vierittää syyn teostaan jollekin toiselle.

Oikeuttamisen selontekoon hyödynnetään neutralisoimistekniikoita, joita ovat muun muassa vahingon kieltäminen, uhrin kieltäminen, tuomitsijoiden tuomitseminen ja vetoaminen korkeampaan lojaliteettiin (Scott ja Lyman, 1968, 51). Neutralisoimistekniikat esitellään tarkemmin seuraavassa luvussa. Edellä mainittujen tekniikoiden lisäksi Scott ja Lyman tuovat esille vielä kaksi muuta oikeuttavaa selontekoa: surullinen tarina ja itsensä toteuttaminen. Surullinen tarina on ikään kuin kertomus äärimmäisen murheellisesta menneisyydestä, jolla henkilö selittää nykyhetkeen johtaneita syitä. Itsensä toteuttamisella viitataan tekoihin, jotka voivat olla vastoin lakia, kuten esimerkiksi huumeiden käyttö, mutta joita henkilö selittää elämäntapansa kuuluvina. (Scott ja Lyman, 1968, 52–53.)

Molemmat selontekojen 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).

Suoninen (1997) käsittelee myös kysymystä, miksi tiettyä normia noudatetaan ja toista rikotaan. Eräs selitys tähän voisi Suonisen mukaan löytyä normijärjestelmän hierarkisuudesta, eli järjestelmän ajatellaan koostuvan ylemmän tason arvostandardeista ja alemman tason normeista. Ylemmän normin rutiininomainen noudattaminen tehtäisiin siten alemman normin kustannuksella. Myös sosiaaliset statukset otetaan usein sellaisina, ettei hierarkisesti ylemmän tarvitse selitellä samoin kuin alemman. Vuorovaikutus kuitenkin vaikuttaa siihen, otetaanko sosiaaliset statukset huomioon tai ei. (Suoninen, 1997.)

4 NEUTRALISOIMISTEORIA

Tämän luvun alussa esitellään tutkimuksen keskeisin teoria sekä teoriasta johdetut neutralisoimistekniikat. Lisäksi esitellään aikaisempia, teoriaa soveltaneita tutkimuksia. Koska teoriaa on eri tutkimuksissa tulkittu eri tavoin, esitellään tässä luvussa näitä erilaisia näkemyksiä ja tulkintoja tietojärjestelmätieteen näkökulmasta sekä tarkastellaan sitä, kuinka eri tutkimukset ovat huomioineet eri neutralisaatiotekniikat sekä alkuperäisen teorian olettamukset. Tämän tutkimuksen tulkinta teoriasta esitellään yhdessä tutkimustulosten kanssa myöhemmin luvussa kuusi. Suomenkielisissä käännöksissä sana ”neutralization” on käännetty muun muassa neutralisaatio, neutraloiminen ja neutralisointi. Tässä tutkimuksessa käytetään termejä neutralisoimisteoria ja neutralisoimistekniikat.

4.1 Neutralisoimisteoria

Yhdysvaltalaisten kriminologien Gresham Sykesin ja David Matzan (1957) neutralisoimisteorian lähtökohtana oli kyseenalaistaa ajatus rikollisesta alakulttuurista, jonka arvot olisivat yhteiskunnan arvojen käänteisarvoja. Sykes ja Matza ikään kuin jatkoivat Sutherlandin (1955) teoriaa, jonka mukaan lainvastainen ja rikollinen käyttäytyminen opitaan. Samoin rikosten tekemisen tekniikat, motiivit, pyrkimykset ja lainvastainen asenne opitaan. Sutherland kyseenalaisti liian yksinkertaisina selitykset, joiden mukaan rikollisuuden taustalla olisivat johtajan seuraaminen tai tunne-elämän levottomuus.

Sykes ja Matza (1957) tutkimus keskittyy nuorisorikollisuuteen ja siihen, kuinka rikollinen oikeuttaa rikollisuutensa. Sykes ja Matza ovat todenneet, kuinka huolimatta rikollisista, jotka eivät tunne syyllisyyttä tai häpeää rikoksistaan, on silti tärkeämpää tuoda esille se, ettei nuorisorikollinen ole kovapintainen gangsteri, vaan monet heistä tuntevat aidosti syyllisyyttä ja häpeää. Nuorisorikollinen näyttäisi olevan sitoutunut, ainakin osittain, yhteiskuntaan ja kykenisi erottamaan sopivan ja sopimattoman toiminnan. Koska nuorisorikollisen arvot eivät ole yhteiskunnan arvojen käänteisarvoja, rikollinen myön-

tää arvostavansa lainkuuliaisia ihmisiä sekä voi myös itse paheksua laitonta toimintaa. Nuorisorikollinen osaa myös erottaa tilanteet, kuten ajan ja paikan, jolloin laiton toiminta ei ole hyväksyttävää. Muun muassa kavereilta ei varasteta tai oman uskonnon kirkkoon ei kohdisteta ilkivaltaa. Toisaalta on myös epätodennäköistä, että nuorisorikollinen korvaisi jollain toisella järjestelmällä vallitsevan yhteiskunnan arvot ja normit. Siten hän ei voi myöskään paeta oman poikkeavuutensa tuomittavuutta, vaan kykenee tuntemaan teoistaan syyllisyyttä ja häpeää. (Sykes ja Matza, 1957, 664–665.)

Sykesin ja Matzan (1957) näkökulman mukaan nuorisorikollisen käyttäytyminen perustuu samaan tapaan arvoihin ja normeihin kuin lainkuuliainenkin käyttäytyminen. Ihmisen käyttäytymiseen liittyy kuitenkin eräs ongelma. Lakeja, joihin uskotaan, rikotaan silti. Sosiaalisen järjestelmän säännöt ja normit vaativat harvoin, jos koskaan, ehdotonta pakkoa. Pikemminkin arvot ja normit näyttäytyvät toimintaa ohjaavana ja rajoittuneena sovellettavaksi tiettyyn aikaan, paikkaan, henkilöön tai sosiaaliseen tilanteeseen. Moraalisestihan tappaminen on väärin, paitsi sodan aikana vihollista vastaan. Säännöt eivät siis ole sitovia kaikissa olosuhteissa. Juuri tämä joustavuus on itseasiassa olennainen osa rikosoikeuden puolustusmekanismeja, jolloin vedotaan humalaan, pakkoon tai itsepuolustukseen. Tuo joustavuus antaa tavallaan yksilölle mahdollisuuden sekä moraalisen syyllisyyden että yhteiskunnan asettamien rangaistusten välttämiseen, mikäli hän pystyy osoittamaan, että teosta puuttui rikollinen tarkoitus. (Sykes ja Matza, 1957, 666.)

Sykesin ja Matzan (1957) väitteen mukaan suuri osa nuorisorikollisuudesta perustuu poikkeavuuden oikeutukseen. Oikeutuksesta käytetään myös termiä järkeily. Vaikka oikeutusta ei nähtäisikään perusteluna oikeudellisessa järjestelmässä tai yhteiskunnassa, henkilö suojelee sen avulla itseään omilta itsesyytöksiltä ja syyttää teosta muita, kuten toisia henkilöitä tai olosuhteita. Henkilö haluaa ikään kuin tehdä tyhjäksi sekä sosiaalisen kontrollin että sisäistettyjä normeja vastaan tehdyn teon paheksunnan. Sykes ja Matza esittävät myös, että poikkeavuuden oikeutus voi toimia rikollisuuden mahdollistajana. Näitä poikkeavan käyttäytymisen perusteluja kutsutaan neutralisoimistekniikoiksi. (Sykes ja Matza, 1957, 666–667.)

4.2 Neutralisoimistekniikat

Alkuperäinen neutralisoimisteoria jakaantuu viiteen neutralisoimistekniikkaan: 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 (*vetominen korkeampiin lojaliteetteihin*). (Sykes ja Matza, 1957, 667–669.) Seuraavaksi nämä viisi tekniikkaa esitellään tarkemmin.

Vastuun kieltäminen (engl. *denial of responsibility*). Rikollinen voi kieltää vastuun poikkeavaan toimintaan ja itsesyytöksiin. Neutralisoimistekniikka laajentaa vastuun kieltämiseen pidemmälle kuin väitteeseen, että poikkeava teko

olisi vain onnettomuus. Rikollinen voi väittää, että teot johtuvat yksilön ulkopuolisista tekijöistä, kuten rakkaudettomista vanhemmista, huonosta seurausta tai huonosta asuinalueesta (slummista). Rikollinen näkee itsensä ikään kuin avuttomana tilanteesta toiseen ajautujana. Psykodynaamisesta näkökulmasta tämä suuntaus edustaa ehkä syvällisempää vieraantumista itsestään, mutta Sykesin ja Matzan mielestä on tärkeä korostaa tosiasiaa, että vastuun tulkitseminen on kulttuurin muodostama eikä omaperäinen uskomus. Se on suhteellisen riippumaton persoonallisuuden rakenteesta. (Sykes ja Matza, 1957, 667.)

Vahingon kieltäminen (engl. *denial of injury*). Toinen neutralisoimistekniikka keskittyy rikolliseen toimintaan osallistumiseen. Rikollinen kyseenalaistaa, onko joku selvästi kärsinyt hänen poikkeavasta toiminnasta, ja tämä kyseenalaistus on avoin erilaisille tulkinnoille. Rikollinen tuntee, ettei käytös oikeastaan aiheuta suurta vahinkoa, huolimatta siitä, että käytös on ristiriidassa lakiin nähden. Aivan kuten yhteys yksilön ja hänen toimintansa välillä kieltää vastuun, liittyy vahingon kieltäminen toiminnan ja sen seurausten väliseen yhteyteen. (Sykes ja Matza, 1957, 667.)

Uhrin kieltäminen (engl. *denial of victim*). Vaikka rikollinen myöntää syyntakeisuutensa sekä myöntää, että hänen poikkeava käyttäytymisensä aiheuttaa vahinkoa tai satuttaa, hän ei koe tehneensä moraalisesti väärin. Pikemminkin hän kokee, että teko on eräänlainen laillinen kosto tai rangaistus. Uhri siis muutetaan väärintekijäksi. Rikollisen silmin joku nyt vain sattui olemaan väärässä paikassa väärään aikaan, tai vähemmistöryhmän edustaja. Rikollinen voi myös omaksua Robin Hood -tyylisen asenteen. Kun uhri on fyysisesti poissa, tuntematon tai epämääräisen abstrakti, kuten muun muassa omaisuusrikoksissa tilanne on usein näin, tietoisuus uhrin olemassa olosta hämärtyy. (Sykes ja Matza, 1957, 668.)

Tuomitsijoiden tuomitseminen (engl. *condemnation of the condemners*). Neljäs neutralisoimistekniikka liittyy tuomitsijoiden arvosteluun. Rikollinen siirtää huomion omasta poikkeavasta käyttäytymisestään ja motiiveistaan. Kyynisyys vallitsevia yhteiskunnan normeja ja niiden valvojia kohtaan voivat johtaa tällaiseen suuntaukseen. Tällaista voi olla esimerkiksi väite poliisin korruptoituneisuudesta. Hyökkäämällä muita kohtaan, oma lainvastainen käytös on helpompi peittää tai kadottaa. (Sykes ja Matza, 1957, 668.)

Vetominen korkeampiin lojaliteetteihin (engl. *appeal to higher loyalties*). Viides, ja viimeinen neutralisoimistekniikka, liittyy sisäisten ja ulkoisten sosiaalisten kontrollien vaatimuksiin. Yhteiskunnan vaatimukset ikään kuin sivuutetaan pienempien sosiaalisten ryhmien, kuten sisarusten, jengin tai ystävyyssuhteiden vuoksi. Rikollinen ei välttämättä hylkää vallitsevan normatiivisen yhteiskunnan järjestelmän vaatimuksia, vaikka ei niitä noudatakaan. Enemmänkin rikollinen voi kokea sotkeutuneensa vaikeaan pulmaan, joka on ratkaistava. Valitettavasti se tapahtuu lain kustannuksella. Normeista poikkeavuus ei johdu itse normeista, vaan muut normit katsotaan pakottavimmiksi tai niihin sisältyy suurempi lojaliteetti, jolloin ne normit menevät edelle. Molempiin normeihin siis uskotaan, mutta niihin liittyy rooliristiriita. Ystävyyden ja lain vaatimusten

välinen ristiriita on pitkään tunnettu yhteisenä ihmisten ongelmana. (Sykes ja Matza, 1957, 669.)

Eli selitykset ”En tarkoittanut sitä”, ”En todellakaan vahingoittanut ketään”, ”Siitäs saivat”, ”Kaikki vain kiusaavat minua” ja ”En tehnyt sitä itseni vuoksi” ovat muunnelmia, joilla rikolliset perustelevat rikollisia tekoja. Kuitenkaan neutralisoimistekniikat eivät kykene täysin suojaamaan yksilöä hänen omilta sisäisiltä arvoiltaan ja muiden reaktiolta, koska rikolliset näyttävät usein kärsivän syyllisyyttä ja häpeää poikkeavasta käytöksestään. (Sykes ja Matza, 1957, 669.)

4.3 Aiemmat tutkimukset

Sykesin ja Matzan (1957) kirjoittama artikkeli lienee yksi useimmin mainituista ja vaikutusvaltaisimmista rikollista tai poikkeavaa käyttäytymistä selittävistä teorioista. Teorian avulla selitettäviä rikoksia ovat olleet muun muassa väkivaltarikokset, kuten raiskaus, murha, kansanmurha ja talousrikokset eli niin sanotut valkokaulusrikokset. Lisäksi teoriaa on käytetty myös esimerkiksi selittämään sitä, kuinka nykypäivän saksalaiset nuoret pyrkivät välttämään leimautumisen holokaustiin. (Maruna ja Copes, 2005.) Neutralisoimisteoriaa soveltaneita, ei-rikollista toimintaa käsitelleitä tutkimuksia on muun muassa Topallin (2005) tutkimus siitä, kuinka kovan linjan huumekauppiaat ja taskusekä autovarkaat käsittelevät syyllisyyden tunnetta epäonnistumisistaan, ei perinteisiin rikoksiin, vaan epäsovinnaisia ja rikollisia arvoja vastaan. Poikkeavaan käyttäytymiseen liittyviä tutkimuksia ovat muun muassa opiskelijoiden alkoholin käyttöön liittyvä neutralisointi (Piacentini ym, 2012), psykiatrisen sairaalan potilaiden pakkokeinoihin osallistuneiden vartijoiden hyödyntämät neutralisoimistekniikat (Johston ja Kilty, 2016) sekä kuluttajien käyttämät neutralisoimistekniikat asenteiden ja käyttäytymisen välisessä ristiriidassa kestävän kehityksen mukaisessa ostokäyttäytymisessä (Gruber ja Schlegelmilch, 2014).

Tätä tutkimusta varten läpikäytyjen lähes 500 tutkimuksen joukosta eri tietokantoihin tehdyt haut osoittivat, että aikaisempien neutralisoimisteoriaa tietoturvan yhteydessä soveltaneiden tutkimusten määrä on verrattaen vähäinen. Myös Sommestad ym., (2014) tekemässä systemaattisessa kirjallisuuskatsauksessa, oli löytettävissä vain muutama tutkimus. Suosituksia ja malleja tulevaisuuden tutkimukseen on silti esitelty muun muassa Garzan ja Guon (2015) sekä Willison ja Warkentin (2013) tutkimusartikkeleissa. Seuraavaksi käydään läpi, millaisista näkökulmista neutralisoimisteoriaa on tietoturvan yhteydessä tarkasteltu. Luvun loppupuolella taulukkoon 1 on koottu aikaisempia tutkimuksia sekä tutkimuksissa huomioituja alkuperäisen neutralisoimisteorian olettamuksia sekä neutralisoimistekniikoita. Taulukkoon 2 on koottu aikaisemmissa tutkimuksissa käytetyt menetelmät, otanta sekä tutkimusten päälöydökset.

Bansal ja Shin (2016) sovelsivat neutralisoimisteoriaa pyrkiessään selvittämään sukupuolen suhdetta moraalikäsitykseen ja tietoturvarikkomukseen.

Vaikka Bansal ym., (2016) tutkimuksen aihepiiri oli sama, tutkimuksessa ei sovellettu yhtään alkuperäisteorian neutralisoimistekniikkaa, joten sitä tutkimusta ei käsitellä tässä yhteydessä. Bansal ja Shin tutkimuksen pyrkimyksenä oli selvittää, onko sukupuolella vaikutusta moraalikäsitykseen ja tietoturvapolitiikan ymmärtämiseen tietoturvapolitiikan noudattamisessa eri neutralisoimistekniikoita hyödynnettäessä. Tutkimuksessa ei esitelty, millaisen tietoturvarikkomuksen pohjalta erilaiset skenaariot oli luotu. Tutkimuksen näkökulmat perustuivat eettisen päätöksenteon malliin (moraalinen intensiteetti), prospektiteoriaan (engl. *prospect theory*) sekä rooliteoriaan (engl. *social role theory*). Tutkijat väittävät, että eri neutralisoimistekniikat erovat moraaliselta intensiteetiltään. Tutkijat väittävät myös, että naiset ja miehet reagoivat eri tavoin eri neutralisoimis-skenaarioihin riippuen siitä, millainen moraalinen intensiteetti kuhunkin skenaarioon liittyy. Tutkijoiden mukaan tahallinen tietoturvapolitiikan rikkominen edellyttää eettistä päätöksentekoa. Tutkimuksessa sovellettiin kolmea neutralisoimistekniikkaa, joista yksi oli alkuperäisteoriasta. Tutkijoiden mukaan moraalikäsitys ja sukupuoli vaikuttavat rikkomusaikeisiin, vaikkakin niiden merkitys vaihteli eri neutralisoimis-skenaarioissa. Tutkimuksessa teoriaa ei analysoitu tarkasti, vaan viitattiin aiempiin tutkimuksiin, joiden mukaan teorian on todettu olevan yhteydessä tietoturvarikkomus aikeisiin. (Bansal & Shin, 2016.)

Barlow, Warkentin, Ormond ja Dennis (2013) tutkimuksessa neutralisoimisteoriaa sovellettiin yhdessä kehysteorian (engl. *framing theory*) kanssa. Tietoturvarikkomuksena tutkimuksessa oli salasanan jakaminen. Tutkimuksen tarkoituksena oli selvittää, lieventääkö tietoturvasta tiedottaminen neutralisoimistekniikoiden käyttöä ja voiko tiedottaminen siten vähentää työntekijöiden aikomusta rikkoa tietoturvaa. Tutkimuksessa sovelletun kehysteorian mukaan tapa, jolla asia esitellään, vaikuttaa siihen, kuinka ihminen asian käsittelee. Tutkijoiden mukaan tietoturvakoulutus on keskittynyt kielteisiin seurauksiin, jolloin työntekijät neutraloivat negatiivisen kehyksen mielestään. Tutkijat esittivät, että tiedottamisen tulisi keskittyä vähentämään neutralisoimistekniikoiden käyttämistä erilaisilla koulutuksilla, harjoituksilla ja tietoturvatietoisuuden lisäämisellä. Vaikka tutkimustulos antoi tutkijoiden mukaan lisänäyttöä siitä, että neutralisoimistekniikat ovat tärkeitä ennustajia tietoturvarikkomus aikomuksissa, tutkijat esittivät, että tekniikoiden merkitys vaihtelee riippuen siitä, millainen tietoturvarikkomus on kyseessä. Tutkijoiden mukaan tutkimus vahvisti, että koulutus vähentää tehokkaasti aikomuksia rikkoa tietoturvaa. Lisäksi tiedottamisen merkitys rikkomusten neutralisointiin tuli tutkimuksessa esille siinä, että virallinen ja epävirallinen tietoturvasta tiedottaminen voivat olla ristiriidassa keskenään. Tutkimuksessa sovellettiin vain yhtä alkuperäisteorian mukaista neutralisoimistekniikkaa. (Barlow ym., 2013.)

Bauer ja Bernroider (2017) tutkimuksessa neutralisoimisteoriaa sovellettiin yhdessä perustellun toiminnan teorian (engl. *theory of reasoned action*) kanssa. Tutkimuksen yhtenä pyrkimyksenä oli muodostaa käsitys työntekijöiden tietoturvatietoisuudesta ja siihen liittyvistä sosiaalista ja henkilökohtaisista normeista ja arvoista. Lisäksi tutkijat pyrkivät selvittämään, millaisten viestintä-

kanavien avulla tietoturvatietoisuutta voidaan parantaa ja hyödyntää tietoturvatietoisuuden kehittämisessä. Tutkijoiden mukaan sisäiset kanavat, kuten intranet-viestit ja muu organisaation sisäinen tiedottaminen olivat tärkeitä tietoturvatietoisuuden parantamisessa. Tutkijoiden mukaan kuitenkin ulkoisilla kanavilla, kuten itseopiskelulla ja perinteisillä medioilla, oli jopa vahvempi vaikutus tietoturvatietoisuuteen. Tutkimuksen mukaan asenteet ja neutralisoimistekniikoiden käyttö heijastelevat yksilön henkilökohtaisia moraalisia normeja. Tutkijoiden mukaan henkilökohtaiset moraalinormit ovat merkittävän tärkeitä tietoturvakäyttäytymisessä. Tutkijat korostivat, että kuitenkin tärkein tekijä tietoturvapolitiikan noudattamisessa on asenne. (Bauer & Bernroider , 2017.)

Cheng, Li, Zhai ja Smyth (2014) tutkimuksen tarkoituksena oli tutkia neutralisoimisen vaikutusta työntekijän kokeman rangaistuksen vakavuuteen, rikkomuksen havaitsemisen varmuuteen sekä koettuihin etuihin internetin käyttöön liittyvässä tietoturvapolitiikan vastaisessa toiminnassa. Eli työntekijän työhön liittymättömässä internetin käytössä. Tutkimuksessa sovellettiin sekä neutralisoimisteoriaa että peloteteoriaa (engl. *deterrence theory*). Tutkimuksen taustalla oli 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. Tutkijat arvelivat myös, että henkilöt, jotka kokevat saavansa hyötyä henkilökohtaisiin tarkoituksiin liittyvässä internetin käytössä, valitsevat todennäköisesti mielummin riskin, vaikka tietävät olemassa olevan kiinnijäämisen riskin ja sen seuraukset. (Cheng ym., 2014.)

Haag, Eckhardt ja Bozoyan (2015) sekä Haag ja Eckhardt (2015) tutkimukset pohjautuivat yhteen ja samaan tutkimukseen, joten ne esitellään yhdessä. Tutkimuksessa neutralisoimisteoriaa sovelletaan niin sanotun varjo-it:n käyttämiseen yksilön näkökulmasta. Tutkimuksessa tutkijat olivat määritelleet varjo-it:n näin: "the voluntary usage of any IT resource violating injunctive IT norms at the workplace as reaction to perceived situational constraints with the intent to enhance the work performance, but not to harm the organization". Tiivistetysti määritelmän voisi suomentaa tarkoittavan vapaaehtoista työpaikan it-normien asettamien kieltojen rikkomista suorituskyvyn parantamiseksi vahingoittamatta organisaatiota. Tutkijoiden mukaan varjo-it:n käyttäjät hyväksyvät neutralisoimistekniikat. Tutkijoiden mielestä varjo-it:n käyttäjien käyttäytymistä ohjaa ensisijaisesti käyttäytymisen prosessit, joiden avulla he hyväksyvät neutralisoinnin, jos säännöt ovat perusteettomat, jos teko on tarpeellista, eikä aiheuta vahinkoa. (Haag ym., 2015.)

Kim ym., (2014) tutkimuksen taustaoletus oli, että asenteet, normit ja luottamus omiin kykyihin vaikuttavat tietoturvapolitiikan noudattamisen aikomukseen. Tutkimuksessa sovellettiin kaikkiaan kahdeksaa hypoteesia, joista yksi oli johdettu neutralisoimisteorista. Hypoteesin mukaan, mitä korkeampi neutralisoinnin taso organisaation työntekijöillä oli, sitä alhaisempi oli myös työntekijöiden tietoturvapolitiikan noudattaminen. Tutkijoiden mukaan tutkimustulos tuki hypoteesia, ja tutkijoiden johtopäätös oli, että työntekijät yrittävät pe-

rusteella tietoturvarikkomuksiaan eri neutralisoimistekniikoiden avulla. Tutkijoiden mukaan myönteinen asenne tietoturvan noudattamiseen sekä ympäristö ja sosiaaliset tekijät vaikuttavat tietoturvapolitiikan noudattamisesta. Lisäksi tutkijoiden mukaan myös tietoturvan hyödyn sekä kustannusten ymmärrys edesauttoi työntekijöiden tietoturvapolitiikan noudattamiseen. Tutkimuksessa neutralisoimisteoria on tulkittu neutralisoimistekniikoiden osalta muun muassa siten, että vahingon kieltämisessä työntekijä voi esimerkiksi väittää, että teki parhaansa minimoidakseen organisaatiolle aiheutuvaa vahinkoa. Uhrin kieltäminen on tutkimuksessa tulkittu niin, että uhri on joku, joka ansaitsi rangaistuksen. Vetoaminen korkeampiin lojaliteetteihin on tulkittu siten, että teon oli tarkoitus suojella perhettä, ystäviä tai yritystä. (Kim ym., 2014.)

Li ja Cheng (2013) tutkimuksen pyrimyksenä oli tunnistaa taustat, jotka ohjaavat työntekijää internet-väärinkäyttöön työpaikalla. Tutkimuksessa sovellettiin sekä neutralisoimisteoriaa että rationaalisen valinnan teoria (engl. *rational choice theory*). Tutkimuksessa internetin-väärinkäyttö ei rajoitu pelkkään selaamiseen, kuten uutisten lukemiseen, vaan erilaisten tiedostojen lataamiseen (musiikki, elokuvat), verkko-ostosten tekemiseen, osakekurssien selaamiseen, henkilökohtaiseen viestintään eri keskustelukanavien kautta (chat-viestintä), tai jopa verkkorikollisuuteen osallistumiseen. Tutkijat esittivät, että työntekijät hyödyntävät joko neutralisoimistekniikoita tai rationaalisen valinnan teorian mukaista käyttäytymistä. Rationaalisen valinnan teorian mukaan ihminen toimii rationaalisesti pyrkiessään päämääriinsä. Yksilö tekemä kustannus-hyötyanalyysi määrittää siten yksilön toimintaa. Tutkijoiden mukaan neutralisoimistekniikat ennustavat työntekijöiden internet-väärinkäytön aikomusta lukuunottamatta vastuun kieltämisen –neutralisaatiotekniikkaa. Tutkijat toteavat lisäksi, että viralliset seuraukset eivät ennusta internet väärinkäytön aikomuksia. (Li & Cheng, 2013.)

Nicho ja Kamoun (2014) tutkimus keskittyy niin sanottuihin sisäpiirin muodostamiin tietoturvauhkiin. Tutkimuksen lähtökohtana oli, että sisäpiirin muodostama uhka voi olla vakava ja samalla myös vaikea ongelma, koska työntekijöillä on pääsy organisaation tietoihin, joista ulkopuoliset eivät edes tiedä. Tutkijat tarkoittavat sisäpiiriläisellä työntekijöitä, entisiä työntekijöitä, liikekumppaneita ja muita sidosryhmiä, joilla on joko lyhyt- tai pitkäaikainen pääsy organisaation järjestelmiin. Tutkimus pyrkii selvittämään mitkä muuttujat lopulta vaikuttavat sisäpiiriläisen tekemään väärinkäytöksiin. Tutkijat olettivat muun muassa, että neutralisoiminen ja piittaamattomuus sekä teknisiin että ei-teknisiin tietoturvakäytäntöihin sekä tehoton viestintä vaikuttavat sisäpiirin väärinkäytöksiä. Tutkimus esitteli kolme todellista tapausta, joissa yhdessä viestintä oli puutteellista, toisessa tapauksessa tyytymätön irtisanottu työntekijä vuoti luottamuksellista tietoa ja kolmannessa tapauksessa luotettu IT-tukihenkilö asensi järjestelmään haittaohjelman. Tutkijoiden mukaan sisäpiiriläiset käyttivät neutralisoimistekniikoita oikeuttaakseen rikollisen toiminnan. (Nicho & Kamoun, 2014.)

Nykäsen (2011) tutkimuksen keskeisenä tavoitteena oli selvittää yksilön ja organisaation tietoturvakäyttäytymisen taustalla vaikuttavia tekijöitä sekä tieto-

turvakoulutuksen vaikuttavuutta. Tutkimuksessa neutralisoimisteoriaa sovellettiin selittämään organisaation työntekijöiden työhön liittymätöntä internet-käyttäytymistä. Tutkimuksen tavoitteena oli selvittää, vaikuttaako tietoturvakoulutus työhön liittymättömään internet-käyttäytymiseen. Tutkijan mukaan tutkimustulos osoitti, että koulutuksella oli vaikutusta työhön liittymättömään internet-käyttäymiseen. Tutkijan mukaan koulutuksen jälkeen vahingon kieltäminen (engl. *denial of injury*) –neutralisoimistekniikan osuus oli muuttunut, eli toimintaa ei pidetty koulutuksen jälkeen enää niin hyväksyttävänä. Kuitenkaan muut tutkimuksessa sovelletut neutralisoimistekniikat eivät olleet tilastoillisesti merkittäviä tekijöitä yksilön työhön liittymättömän internetin käyttämisen selittämisessä. Tutkimuksessa neutralisoimisteoria tulkittiin siten, että se on eräänlainen mielleyhtymäteoria, jossa henkilö tarkastelee reflektoiden omaa käyttäytymistään verraten sitä vahvaan teoreettiseen taustaan pohjautuviin väittämiin suhteuttaen niitä omaan toimintaansa. (Nykänen, 2011.)

Silic, Barlow ja Back (2017) tutkimuksessa tarkasteltiin neutralisoimisen roolia niin sanottuihin varjo-it:n käyttäjiin. Tutkijat tarkoittivat varjo-it:llä työkaluja, palveluita ja järjestelmiä, joita työntekijät käyttävät, mutta joita organisaation IT-osasto ei ole hyväksynyt. Yhtenä esimerkkinä mainittiin Dropbox-pilvipalvelu, jota työntekijät saattavat käyttää ilman organisaation IT-osaston hyväksyntää. Tutkimuksessa sovellettiin sekä neutralisoimisteoriaa että peloteteoriaa (engl. *deterrence theory*). Tutkimus halusi selvittää neutralisoimistekniikoiden merkitystä erityisesti varjo-it:n yhteydessä. Tutkimuksessa tutkittiin myös itse ilmoitetun aikomuksen ja todellisen käyttäytymisen välistä eroa. Lisäksi tutkimuksessa pyritään löytämään vastaus häpeän roolista neutralisoimistekniikoiden ja organisaation tietoturvarikkomusten välillä, erityisesti varjo-it:n yhteydessä. Tutkijoiden mukaan vain ”metaphor of the ledger”, joka ei ole alkuperäisteorian mukainen tekniikka, oli yhteydessä organisaation varjo-it:tä koskevaan tietoturvapolitiikan rikkomukseen. Myöskään häpeällä, virallisilla tai epävirallisilla seurauksilla ei tutkijoiden mukaan ollut pelotevaikutusta varjo-it käyttäjien aikomuksiin. Tutkijoiden mukaan kuitenkin häpeä vaikuttaa epävirallisiin seurauksiin ja joihinkin neutralisoimistekniikoihin, kuten muun muassa vahingon kieltämiseen. Tutkijat arvelivat, että kun työntekijät käyttävät muita neutralisoimistekniikoita, heidän tavoitteenaan ei ole lieventää häpeää. Siitä syystä tutkijat arvelivat, että häpeä on suhteessa vain joihinkin neutralisoimistekniikoihin. Lisäksi tutkijoiden mukaan aikomuksen ja todellisen käyttäytymisen välillä ei ole juurikaan eroa. (Silic ym., 2017.)

Siposen ja Vancen (2010) tutkimuksessa neutralisoimisteoriaa sovellettiin työntekijöiden tietoturvarikkomusten aikeisiin. Tutkimuksen näkökulmana oli, että rangaistuksen tai sanktioiden pelko ei välttämättä toimi työntekijöiden tietoturvarikkomuksissa, koska työntekijät käyttävät neutralisoimistekniikoita ja järkeilevät niiden avulla toimintaansa, jolloin seuraukset menettävät tehonsa. Tutkimuksessa ei käsitelty uhrin kieltämistä. Tutkijat perustelivat tekniikan huomiotta jättämistä sillä, että tietoturvarikkomusten yhteydessä on vaikea osoittaa, kuka on uhri. Tutkijoiden mukaan tutkimustuloksista oli mahdollista päätellä muun muassa se, että neutralisointi sekä ennustaa työntekijöiden tieto-

turvarikkomus aikomuksia että vaikuttaa merkittävästi taipumukseen rikkoa tietoturvapolitiikkaa. Lisäksi tutkijoiden mukaan epävirallisilla seuraamuksilla oli suurempi vaikutus kuin virallisilla seuraamuksilla. Tulkinta teoriasta oli, että neutralisoimistekniikat vapauttavat työntekijän tilapäisesti muodollisista rajoituksista, sekä virallisista ja epävirallisista seuraamuksista. (Siponen & Vance, 2010.)

Willison, Warkentin, ja Johnston (2016) tutkimus keskittyi työntekijän kokeman, työssä tapahtuvan epäoikeudenmukaisuuden vaikutukseen tietokoneen väärinkäytössä. Tutkijat sovelsivat tutkimuksessaan neutralisoimisteorian lisäksi organisaation oikeudenmukaisuusteoriaa (engl. *organizational justice – distributive and procedural*) ja peloteteoriaa (engl. *deterrence theory).* Tutkijoiden mukaan yksittäinen teoria ei pysty tarjoamaan perusteellista ja täysin ymmärrettävää selitystä ilmiöstä. Tutkimuksessa organisaation epäoikeudenmukaisuuteen sovellettiin sekä distributiivista että prosessuaalista näkökulmaa. Distribitiivinen (epä)oikeudenmukaisuus käsittelee muun muassa organisaation palkkojen ja muiden resurssien jakoa. Prosessuaalinen (epä)oikeudenmukaisuus liittyy resurssien jaossa noudatettaviin toiminta- ja menettelytapoihin. Tutkijat asettavat väitteen, jonka mukaan henkilöt, jotka kokevat työnantajan taholta epäoikeudenmukaisuutta, ovat todennäköisemmin yhteydessä väärinkäytöksiin. Tutkijoiden mukaan vain prosessuaalinen epäoikeudenmukaisuus oli yhteydessä väärinkäytös aikomuksiin ja lisäsi myös neutralisoimistekniikoiden todennäköisyyttä työntekijän väärinkäytös aikomuksiin. Tutkijoiden mukaan havainto viittaa siihen, että työntekijät ovat enemmän tyrmistyneitä epäoikeudenmukaisista toimintatavoista kuin siitä, etteivät työstä maksetut korvaukset ole tasapuolisia. Tutkijoiden mukaan väärinkäytöksestä saatavan rangaistuksen varmuus vähentää kuitenkin tehokkaasti työntekijän väärinkäytös aikomusta prosessuaalisen epäoikeudenmukaisuuden kokemuksessa. Tutkimuksessa organisaation tietoturvapolitiikan rikkominen on tulkittu poikkeavaksi käyttäytymiseksi, jolla rikotaan sosiaalisen ryhmän yhteisiä sääntöjä, arvoja ja hyväksyttävää käyttäytymistä, jolloin syyllisyyden ja häpeän tunteita pyritään neutralisoimaan. (Willison ym., 2016.)

TAULUKKO 1 Neutralisoimisteorian soveltaminen

Aiemmat tutkimukset	**Tutkimuksissa huomioidut neutralisoimistekniikat ja alkuperäisen teorian olettamukset**								
	denial of responsibility	denial of injury	denial of victim	condemnation of the condemners	appeal to higher loyalties	guilt and shame	guilt avoidance	social control & social order	make deviant behavior possible
Bansal & Shin (2016)		X							
Barlow ym., (2013)		X							X
Bauer & Bernroider (2017)	X	X		X				X	
Cheng ym., (2014)	X	X	X	X	X				
Haag ym., (2015)		X		X					
Kim ym., (2014)	X	X		X	X				
Li ym., (2013)	X	X	X	X	X				
Nicho & Kamoun (2014)		X		X					
Nykänen (2010)	X	X		X	X				
Silic ym., (2017)	X	X		X	X	X			
Siponen & Vance (2010)	X	X		X	X	X		X	X
Willison ym., (2016)		X	X			X		X	

Vaikka aikaisempien tutkimusten tulokset osoittavat yksittäisten neutralisoimistekniikoiden selittävän tietoturvarikkomuksia, tutkimuksissa ei juurikaan ole huomioitu alkuperäisen neutralisoimisteorian olettamuksia tai olettamuksia on tulkittu eri tavoin. Tutkimuksissa on myös ristiriitaisuuksia, ovatko kaikki tekniikat yhteneväisiä riippumatta siitä, minkä tyyppistä tekniikkaa tutkimuksessa on sovellettu ja millaisesta tietoturvarikkomuksesta oli kyse. Tutkijat olivat saaneet riistiriitaisia tutkimustuloksia muun muassa työntekijöiden työhön kuulumattomassa internet-käyttäytymisessä sekä varjo-it:n käyttämisessä.

TAULUKKO 2 Aikaisempien tutkimusten kooste

Aiemmat tutkimukset, jotka ovat soveltaneet suoraan Sykes ja Matzan (1957) alkuperäisteoriaa ja/tai sen osia tietoturvan yhteydessä			
Tekijä/ tekijät	**Menetelmä**	**Näyte/otanta**	**Keskeisimmät löydökset**
Bansal & Shin (2016)	Kyselytutkimus kuudella skenaariolla ja kahdeksalla hypoteesilla	221 opiskelijaa.	Moraalikäsitys ja sukupuoli vaikuttavat aikomukseen rikkoa tietoturvapolitiikka, mutta merkitys vaihtelee eri neutralisoimistekniikoissa.

Barlow ym., (2013)	Kyselytutkimus, 36:lla skenaariolla ja seitsemällä hypoteesilla	90 kokoaikaista työntekijää, jotka vastasivat neljään satunnaiseen skenaarioon, eli yhteensä näyte oli 360 vastausta	Koulutus vähentää tieto-turvarikkomus aikomuksia, eri neutralisoimistekniikoilla on erilainen merkitys
Bauer & Bernroider (2017)	Kolmivaiheinen tapaustutkimus, joka sisälsi 4 puoli-strukturoitua haas-tattelua, online-kyselyn ja inter-aktiivisen esittelyn	2 tietoturvajohtajaa, 1 PR johtaja, 1 turvallisuusjohtaja ja 97 työntekijää	Suhtautuminen tietoturvapolitiikan noudattamiseen on tärkein muuttuja sosiaalisissa ja henkilökohtaisissa normeissa, jotka vaikuttavat tietoturvakäyttäytymiseen
Cheng ym., (2014)	Kyselytutkimus neljällä hypoteesilla (1 neutralisoimisteorian hypoteesi)	230 työntekijää	Neutralisointi on vahvin ennustaja aikomuksessa rikkoa tietoturvapolitiikkaa. Myös henkilökohtainen hyöty lisää rikkomuksen todennäköisyyttä.
Haag ym., (2015)	Laboratorio koe	148 opiskelijaa	Varjo-it:n käyttäjät hyödyntävät neutralisoimistekniikoita.
Kim ym., (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)	Kyselytutkimus kymmenellä hypoteesilla	428 eri ikäistä ja eri koulutustautoilta olevaa työntekijää	Työntekijät hyödyntävät neutralisoimistekniikoita internet väärinkäytön aikomuksissaan lukuun ottamatta vastuun kieltämisen -tekniikkaa.
Nicho & Kamoun (2014)	Monivaiheinen laadullinen tutkimus	Kolme tapausta	Niin sanotut sisäpiiriläiset oikeuttavat toimintansa neutralisoimistekniikoilla
Nykänen (2011)	Kaksivaiheinen toimintatutkimus	15 työntekijää	Tietoturvakoulutus vaikutti vahingon kieltämisen – tekniikkaan neutralointia heikentävästi, muut neutralisoimistekniikat eivät olleet merkittäviä
Silic ym., (2017)	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)	Kyselytutkimus kolmella skenaariolla ja neljällä hypoteesilla	Kolme organisaatiota, yhteensä 1449 työntekijää eri ammattiryhmistä	Neutralisointi vaikuttaa merkittävästi työntekijöiden aikomukseen rikkoa tietoturvapolitiikkaa.
Willison ym., (2016)	Kyselytutkimus neljällä skenaariolla ja 12 hypoteesilla	968 työntekijää eri ammattiryhmistä (näyte kaikkiaan 3872, koska jokainen kävi läpi neljä skenaariota)	Prosessuaalinen epä-oikeudenmukaisuus on yhtedessä väärinkäytöksiin sekä neutralisoimis-tekniikoiden hyödyntämisen aikomuksiin.
Aiemmat tutkimukset, jotka soveltavat Sykes ja Matzan (1957) alkuperäisteoriaa tai sen osia muussa kuin tietoturvan yhteydessä			
Hinduja (2007)	Kyselytutkimus 51 kysymyksellä	433 opiskelijaa	Neutralisoimistekniikat ovat heikko määräävä tekijä ohjelmisto-piratismissa.
Ingram & Hinduja (2008)	Kyselytutkimus	2032 opiskelijaa	Mitä hyväksytympinä vastaaja neutralisoimis-tekniikat koki, sitä merkittävämmäksi muodostui myös musiikkipiratismiin osallistumisen ennuste.
Lowry ym., (2016)	Kyselytutkimus yhdeksällä hypoteesilla	1003 englanninkielistä yhdysvaltalaista (opiskelijoita, työttömiä, osa- ja kokoaikaisessa työssä käyviä)	Nimettömyys lisää neutralisointia verkkokiusaamisessa. Neutralisointi liittyy lisääntyneeseen verkkokiusaamiseen.
Riekkinen (2016)	Kyselytutkimus kuudella hypoteesilla	322 henkilöä (eri keskustelupalstoilta)	Neutralisointi vaikuttaa myönteisesti musiikkipiratismissa
Siponen ym., (2012)	Kyselytutkimus neljällä skeaariolla ja 10 hypoteesilla	183 opiskelijaa	Neutralisoimistekniikat ennustavat ohjelmistopiratismin aikomuksissa
Zhang ym., (2016)	Kyselytutkimus kahdella skenaariolla ja kolmella hypoteesilla	174 Facebook käyttäjää (opiskelijoita)	Neutralisoinnilla on merkittävä rooli verkkokiusaamisen mahdollistajana

4.4 Kritiikkiä

Vaikka neutralisoimisteoriaa sovelletaankin erittäin laajasti, on siihen kohdistunut myös kritiikkiä. Maruna ja Copes (2005) nostavat neutralisoimisteoriasta esille sen, että teorian mukaan poikkeava käyttäytyminen etenee kronologisessa järjestyksessä. Tällä tarkoitetaan sitä, että rikollinen teko neutralisoidaan tai järkeistetään jo ennen tekoa, eikä vasta teon jälkeen. Neutralisointi siis edelsi nuorisorikollisuutta ja toimi poikkeavan käyttäytymisen mahdollistajana, koska vastuu kiellettiin jo ennen tekoa. Marunan ja Copesin mukaan, tämä tekee teoriasta vaikeasti testattavan. Miten joku voi neutralisoida teon, jota ei ole vielä tehnyt? Maruna ja Copes esittävät myös empiriseen näyttöön liittyvä ongelma on se, kuinka voi mitata neutralisaatiotekniikoiden käyttämistä jälkikäteistarkastuksena. (Maruna ja Copes , 2005.)

Neutralisoimisteoriaa soveltavissa tutkimuksissa on hyödynnetty sekä kvalitatiivisia että kvantitatiivisia tutkimusmenetelmiä. Maruna ja Copes (2005) mainitsevat muun muassa haastatteluihin liittyvän hankaluuden, joka pätee erityisesti vankiloissa tai vankeinhoidon ympärisöissä tehtyihin haastatteluihin. Tutkittaessa poikkeavaa tai rikollisista käyttäytymistä, vankilassa suoritettu haastattelu tekee erittäin selväksi sen, kuka tilanteessa on poikkeava, jolloin haastateltava haluaa puolustaa itseään ja asemaansa, ja neutralisoimistekniikat tarjoavat haastateltaville heidän kaipaamansa selityksen. (Maruna ja Copes, 2005.)

5 TUTKIMUKSEN TOTEUTUS

Tässä luvussa kerrotaan tutkimuksen toteutuksesta. Samalla kerrotaan tutkimusmenetelmän valinnasta ja esitellään analysoitavan aineiston kerämiseen käytetty menetelmä, sekä kerrotaan tutkimuksen kohdeorganisaatiosta siltä osin, kuin se on mahdollista. Lisäksi luvun loppuosassa kerrotaan tutkimusaineiston analysointiin käytetyistä menetelmistä.

5.1 Tutkimusmenetelmän valinta

Kvalitatiivinen tutkimus rakentuu aiemmista tutkimuksista ja teorioista, empiirisestä aineistosta sekä tutkijan omasta ajattelusta ja päättelystä (Saaranen-Kauppinen ja Puusniekka, 2006). Tähän tutkimukseen käytettiin kvalitatiivista tutkimusmenetelmää. Tutkimuksen keskeisin teoria on toiminut tutkimuksen lähtökohtana, jolloin sen kautta on ensinnäkin hahmotettu, millaista aineistoa kerätään, mutta samalla teoriaa vasten on myös pyritty analysoimaan ja arvoimaan kerättyä aineistoa. Empiirinen aineisto kerättiin haastatteluiden avulla.

Saaranen-Kauppisen ja Puusniekan (2006) mukaan laadullisen ja määrällisen tutkimusmenetelmän yksinkertaistavasta jaottelusta huolimatta, erilaisilla menetelmillä on mahdollista saada erityyppistä tietoa. Eisenhardtin ja Graebnerin (2007, 28–29) mukaan kvalitatiivinen tutkimusmenetelmä voi tuoda esille tietoa, jota kvantitatiivinen menetelmä ei pystyisi paljastamaan. Lisäksi Saaranen-Kauppinen ja Puusniekka (2006) toteavat, että saman ilmiön tutkiminen eri lähestymistavoilla voi monipuolistaa tietoa ja lisätä siten ymmärrystä ilmiön luonteesta. Vaikka aikaisemmissa neutralisoimisteoriaa tietoturvan yhteydessä soveltaneissa tutkimuksissa tutkimusmenetelmänä on käytetty pääasiassa kvantitatiivista tutkimusmenetelmää skenaariopohjaisena, soveltui kvalitatiivinen menetelmä vastaamaan tämän tutkimuksen tarkoitusta. Se mahdollisti aiemmista tutkimuksista poikkeavan lähestymistavan ja siten mahdollisuuden tarkastella ilmiötä tarkasti ja avoimesti.

Tapaustutkimus on käsitteenä monitahoinen ja oikeastaan kaikki kvalitatiiviset tutkimukset ovat tapaustutkimuksia, koska niiden pohjalta ei ole tarkoitus tehdä samaan tapaan yleistäviä päätelmiä kuin kvantitatiivisissa tutkimuksissa. Vaikka tapaustutkimuksella pyritään lisäämään ymmärrystä tietystä ilmiöstä pyrkimättä yleistettävään tietoon, voi analysoitavan aineiston avulla saada kuitenkin yksittäistapauksen ylittävää tietoa. (Saaranen-Kauppinen & Puusniekka, 2006.) Myös Eisenhardt (1989, 534) tuo esiin, kuinka tapaustutkimus on tutkimusstrategia, joka keskittyy ymmärtämään tiettyyn ilmiöön liittyvää dynamiikkaa. Tapaustutkimuksessa tutkimuskohteena on jokin nykyhetken ilmiö ja sen avulla voidaan myös etsiä tai löytää uusia näkökulmia (Darke ym., 1998). Tämän tutkimuksen tavoitteena oli saada lisäymmärrystä syistä, jotka voivat johtaa työntekijöiden tekemiin tietoturvarikkomukseen. Koska tutkimusmenetelmäksi valittiin aiemmista tutkimuksista poikkeava lähestymistapa, pyrittiin ilmiöstä löytämään mahdollisia uusia tai erilaisia näkökulmia, joten tapaustutkimus soveltui tämän tutkimuksen tutkimusstrategiaksi.

Tapaustutkimusten tiedonkeruumenetelminä voidaan käyttää lukuisia erilaisia tietolähteitä, kuten haastatteluita, havainnointia, kyselyitä ja tekstianalyysiä. Kuitenkin haastatteluista tulee usein ensisijainen tietolähde sen tehokkuuden vuoksi. (Darke ym., 1998; Eisenhardt & Graebner, 2007, 28.) Haluttaessa esimerkiksi ymmärtää ihmisten perusteita heidän toiminnalleen, on luontevaa kysyä asiasta heiltä itseltään. Haastattelu on tieteellinen menetelmä, jonka eroaa keskustelusta siinä, että se tähtää informaation keräämiseen ja on ennalta suunniteltua, päämäärähakuista toimintaa. (Hirsjärvi & Hurme, 2001, 11, 42.) Vaikka Hirsjärven ja Hurmeen (2001, 35) mukaan haastatteluaineistojen analysointi, tulkinta ja raportointi osoittautuvat usein ongelmalliseksi, oli tämän tutkimuksen kannalta tärkeää antaa työntekijöiden itse kertoa omista kokemuksistaan ja näkemyksistään. Tälle tutkimukselle ei myöskään haluttu asettaa ennakko-olettamuksia, koska kuten Alasuutari (2012, 63) kirjoittaa, tutkittaessa sitä, miten ihmiset hahmottavat ja jäsentävät erilaisia asioita, aineistona tulee olla tekstiä, jossa ihmiset puhuvat asioista omin sanoin, eivätkä joudu valitsemaan tutkijan jäsentämistä vastausvaihtoehdoista.

5.2 Tiedon kerääminen

Tämän tutkimuksen tietolähteinä käytettiin sekä organisaation tietoturvapolitiikan dokumentaatiota että teemahaastatteluita. Hirsjärven ja Hurmeen (2001) mukaan teemahaastattelu on haastattelun muoto, joka etenee tarkkojen, valmiiksi muotoiltujen ja yksityiskohtaisten kysymysten sijasta ennalta suunniteltujen teemojen mukaisesti. Vaikka kysymysten muoto ei siis olekaan kaikille haastateltaville samanlainen, haastattelun aihepiirit ovat kaikille samat ja ohjaavat siten haastattelua. (Hirsjärvi & Hurme, 2001, 48.) Koska haastattelu perustuu kielelliseen vuorovaikutukseen, antaa keskustelunomainen haastattelu mahdollisuuden lähestyä myös aiheita, joita muutoin voisi olla vaikea saa-

da selville. Verrattuna lomaketutkimukseen, haastattelu tarjoaa myös paremmat mahdollisuudet motivoida haastatteluun osallistumista. Toisaalta haastattelun avulla voidaan saada kuvaavia esimerkkejä tai löytää ilmiöiden välisiä suhteita, koska haastatteluaineisto koostuu haastateltavien kokemuksista, ajatuksista, uskomuksista ja tunteista. (Hirsjärvi ja Hurme, 2001, 11, 36, 48.)

Teemahaastattelussa kaikki etukäteen suunnittellut teema-alueet käydään jokaisen haastateltavan kanssa läpi, mutta niiden laajuus tai järjestys saattavat vaihdella haastateltavasta toiseen. Koska teemahaastattelu on keskustelunomainen, ei haastattelijalla ole valmiita kysymyksiä, vaan esimerkiksi muistilista käsiteltävistä aiheista. Teemat luovat keskustelulle niin sanotun kehyksen, jolla varmistetaan, että jokaisen haastateltavan kanssa on puhuttu samoista aiheista. (Eskola & Suoranta, 2008, 86–87.) Vaikka teemahaastattelu edellyttää etukäteisvalmistautumista, eli teemojen valintaa, aineistoa ei kuitenkaan rajata valmiiden vastausvaihtoehtojen kautta.

Vaikka teemahaastattelu soveltuu ilmiöön tai asiaan, josta on vielä vähän tietoa, täytyy haastattelijan silti tuntea tutkimuksen aihepiiri, koska käsiteltävät teemat valitaan tutkimusaiheen pohjalta. Menetelmän etuna on se, että kerättyä haastatteluaineistoa voidaan analysoida teemojen pohjalta, mutta analysointi voi osoittaa myös uusia tutkimusaihetta jäsentäviä teemoja. (Saaranen-Kauppinen & Puusniekka, 2006.)

Tämän tutkimuksen haastatteluiden teemat oli johdettu sekä teorian oletamuksista että tutkimustehtävään rajatuista aiheista. Teemat käsittelivät siten salasanojen ja sähköpostiviestien lisäksi myös tietoturvakäyttäytymistä ja tietoturvapolitiikan noudattamista. Tietoturvakäyttäytyminen liittyy myös organisaatiokulttuuriin, joten haastateltavia pyydettiin kuvailemaan organisaation toimintatapoja. Schein (1991) on esittänyt, että organisaation arvojen perusteella voi olla vaikea tehdä johtopäätöksiä organisaation perusoletuksista. Scheinin mukaan tällaiset oletukset tulevat esille tavallisimmin haastattelemalla, koska ihmiset eivät mielellään tuo julki perusoletuksiaan, ja toisaalta niitä pidetään itsestäänselvyyksinä. (Schein, 1991, 38.) Koska haastateltavina oli eri ammattiryhmien edustajia, mahdollisti teemahaastattelu teema-alueiden järjestyksen ja laajuuden vaihtelun haastattelusta toiseen kunkin haastateltavan kokemusten ja näkemysten mukaisesti. Tutkimusaiheen voi luokitella niin sanotusti araksi aiheeksi, joten haastattelu antoi mahdollisuuden vuorovaikutukselle ja tarkentaville lisäkysymyksille. Vaikka haastattelu perustuu kielelliseen vuorovaikutukseen, tarjoaa se silti myös mahdollisuuden niin sanotun oheisviestinnän havaitsemiseen, eli ilmeiden, eleiden ja käyttäytymisen arvioimiseen. Tämän tutkimuksen haastatteluissa oheisviestinnän havainnoinnilla pyrittiin tulkitsemaan haastateltavan kertoman todenmukaisuutta. Tällä tarkoitetaan esimerkiksi sitä, että ilmeiden, eleiden ja käyttäytymisen havainnoilla pyrittiin tulkitsemaan, kertoiko haastateltava jonkin asian vakavissaan vai niin sanotusti leikillään. Metsämuuronen (2011) mainitsee, kuinka lukijan on pystyttävä raportin perusteella saamaan käsitys siitä, mistä tieto, eli analysoitava aineisto on hankittu sekä miten luotettavasta tiedosta on kysymys, joten seuraavaksi kerrotaan, mistä ja miten tutkimuksen aineisto kerättiin.

5.3 Tutkimuskohde

Tutkimuksen kohdeorganisaatio haluaa omasta pyynnöstään jäädä anonyymiksi, joten tutkimuksen raportoinnissa tätä organisaation toivetta pyritään kunnioittamaan, eikä tutkimuslupahakemusta ja siihen liittyvää päätöstä liitetä tämän tutkimusraportin liitteeksi. Myöskään haastateltavien henkilöllisyyteen tai ammattiin liittyviä asioita ei tulla esittelemään, eikä organisaatiokulttuurista kerrota tarkasti. Kohdeorganisaatio on julkishallinnon organisaatio, jossa työskentelee useita satoja henkilöitä eri toimialoilla. Organisaatio jakaantuu eri osastoihin, mutta tässä tutkimuksessa organisaation rakennetta ei tulla käsittelemään tarkasti. Myöskään organisaation maantieteellinen sijainti ei vaikuta tutkimustulokseen, joten sitä ei käsitellä tutkimuksessa. Organisaation päivittäisessä käytössä on erilaisia tietoverkkoratkaisuja ja tietojärjestelmiä erilaisiin käyttöympäristöihin. Lisäksi osa organisaation toiminnoista on ulkoistettu eri palveluntarjoajille.

Organisaatiolla on ajantasainen tietoturvapolitiikka, joka sisältää organisaation toiminnasta johdetut suhteellisen tarkat vaatimukset sekä noudattamisohjeet. Se sisältää muun muassa tietoturvapolitiikan keskeiset periaatteet, tietoturvallisuuden kehittämisen sekä riskienhallinnan. Organisaation tietoturvatoimintaa ohjaa myös lainsäädäntö, kuten muun muassa julkisuuslaki. Tarkkoihin toimintaohjeisiin vaikuttaa myös se, että tietoturva on merkittävä huomioon otettava tekijä jokaisen työntekijän päivittäisessä työssä.

Haastateltavien päivittäisessä käytössä olevien eri tietojärjestelmien määrä hieman vaihteli työtehtävittäin, ollen viiden ja kymmenen välillä. Järjestelmiin tunnistautuminen tapahtuu joko toimikortilla ja salasana-pin-koodi –yhdistelmällä, tai pelkällä salasanalla, tai pin-koodin ja salasanan yhdistelmällä, jolloin päivittäisessä työssä saatetaan käyttää kymmentä eri salasanaa tai pin-koodia tai niiden yhdistelmää. Lisäksi osassa järjestelmiä vaaditaan yli 14 merkkiä pitkiä salasanoja. Salasanojen tulee olla vahvoja ja eri järjestelmissä tulee käyttää erilaisia salasanoja. Osa järjestelmistä niin sanotusti pakottaa automaattisesti, säännöllisin väli ajoin salasanan vaihtamiseen, mutta eivät kaikki. Haastatteluiden perusteella päivittäisten sähköpostiviestien määrässä oli vaihtelua työtehtävästä riippuen, mutta ne kuuluvat kuitenkin jokaisen työntekijän arkipäiväiseen työskentelyyn.

5.4 Haastatteluiden toteutus

Kohdeorganisaatiolta pyydettiin tutkimuslupaa lokakuussa 2016. Myönteinen tutkimuslupa sisälsi joitakin rajoitteita, jotka eivät kuitenkaan liittyneet haastateltavien henkilöiden valintaan, mutta jotka oli otettava huomioon haastatteluiden toteutuksessa. Eisenhardt ja Graebner (2007) korostavat, että haastatteluaineiston tulisi koostua organisaation eri hierarkiatasoista, yksiköistä tai ryhmistä. Tämän tutkimuksen haastateltavien valinnan perusteena oli pyrkiä

keräämään mahdollisimman monipuolista aineistoa. Tutkimusta varten haastateltiin kohdeorganisaation 12 työntekijää, jotka työskentelevät erilaisissa työtehtävissä. Kaikilla haastateltavilla oli hyvä organisaatiotuntemus, eli kukin oli työskennellyt organisaatiossa useamman vuoden ajan. Muutamien haastateltavien työnkuvaan sisältyi tietoturvarikkomusten selvittämistä sekä erilaisten tietoturvaratkaisujen suunnittelua. Ensimmäisen kontaktin jälkeen suurin osa haastateltavista valikoitui niin kutsutun lumipallotekniikan avulla, eli tutkimukseen osallistuja antoi vihjeitä muista tutkimukseen mahdollisesti soveltuvista osallistujista.

Haastattelut toteutettiin joulukuun 2016 – maaliskuun 2017 välisenä aikana yksilöhaastatteluina. Haastateltavilla oli mahdollisuus tutustua tutkimussuunnitelmaan, joten he tiesivät, mihin haastatteluaineistoa tullaan käyttämään. Haastatteluita varten listattiin joitakin apukysymyksiä ja avainsanoja, jotka koottiin sekä tutkimustehtävästä että teoriapohjan perusteella.

Koska tietoturva on kohdeorganisaatiossa merkittävä tekijä, ja työntekijät joutuvat huomioimaan sen omissa työtehtävissään, aihepiiri itsessään toimi haastatteluihin osallistumiseen motivoivana tekijänä. Haastatteluun osallistuminen oli vapaaehtoista ja kaikki haastattelut suoritettiin työympäristön ulkopuolella, rauhallisessa ja häiriöttömässä paikassa. Jokaiselle haastattelulle varattiin reilusti aikaa ja kunkin haastattelun kesto oli noin tunnin. Haastattelut nauhoitettiin haastateltavien luvulla myöhempää litterointia varten. Vain yksi haastateltava koki nauhoituksen liian epämiellyttävänä, joten haastattelusta koostettiin muistiinpanot, jotka annettiin haastateltavalle luettavaksi ja jotka hän hyväksyi. Haastatteluiden litterointi suoritettiin kahta poikkeusta lukuun ottamatta mahdollisimman nopeasti kunkin haastattelun jälkeen, jotta haastattelu olisi sekä haastateltavan että haastattelijan tuoreessa muistissa mahdollisten täydennysten tai selvennysten varalle. Haastatteluista tehtiin myös paperille joitakin muistiinpanoja.

Koska kieli tai sen vivahteet eivät olleet haastatteluaineiston analyysin kohteina, haastatteluiden litteroinnissa ei käytetty erityisiä litterointimerkkejä. Nauhoitteet pyrittiin kirjoittamaan mahdollisimman sanasta sanaan, mutta viittaukset henkilöiden, tietojärjestelmien, organisaation tai paikkojen nimiin joko poistettiin tai muotoiltiin muutoin tunnistamattomiksi. Raportoinnissa puhekieli on muutettu kirjakielelle, jolloin mahdolliset murreilmaisut eivät yksilöi ketään haastateltavaa. Litteroitu teksti lähetettiin kullekin haastateltavalle tarkastettavaksi ennen haastatteluaineiston analysointia. Tällä tavoin haastateltavilla annettiin mahdollisuus tarkastaa keskustelun kulku ja tehdä mahdollisia tarkennuksia tai korjauksia. Yksi haastateltava tarkensi yhtä lausetta ja toinen haastateltava tarkensi organisaation tiettyä toimintatapaa. Haastattelut pyrittiin toteuttamaan mahdollisimman keskustelunomaisesti, jolloin aidolle vuorovaikutukselle annettiin riittävästi tilaa. Tutkimuksen raportointivaiheessa muutamaan haastateltavaan oltiin puhelimitse yhteydessä vielä varsinaisen haastattelun jälkeen organisaatiokulttuuriin liittyvissä tarkennuksissa.

Alasuutarin (2012, 83) mukaan tutkimusprosessi saavuttaa saturaatiopisteen, kun haastateltavat alkavat toistaa toinen toisiaan ja haastateltavien vas-

taukset voidaan aavistaa jo ennakolta. Tässä tutkimuksessa saturaatiopiste saavutettiin kymmenennen haastattelun jälkeen.

5.5 Aineiston analysointi

Alasuutari (2012) kuvailee laadullisen analyysin koostuvan kahdesta yhteen nivoutuvasta vaiheesta, havaintojen pelkistämisestä ja arvoituksen ratkaisemisesta, joita voidaan kutsua myös havaintojen tuottamiseksi ja selittämiseksi. Alasuutarin mukaan havaintojen pelkistämisellä tarkoitetaan aineiston tarkastelua tutkimukseen liittyvän teoreettisen viitekehyksen näkökulmasta kulloisenkin kysymyksenasettelun mukaisesti. Pelkistämisen ideana on havaintojen yhdistäminen, jolloin raakahavainnot yhdistetään yhdeksi havainnoksi tai harvemmaksi havaintojen joukoksi. Havaintojen yhdistämisen lähtökohtana on ajatus, että aineistossa ajatellaan löydettävän esimerkkejä tai näytteitä samasta ilmiöstä. Alasuutari selittää arvoituksen ratkaisemisen tarkoittavan tutkittavasta ilmiöstä tehtäviä merkitystulkintoja. (Alasuutari, 2012, 32–37.)

Saaranen-Kauppinen & Puusniekka (2006) selittävät analysoinnin olevan tutkimustehtävän näkökulmasta tehtävää tutkimusaineiston jäsentelyä. Muun muassa teemahaastatteluaineiston analysoinnissa aineisto voidaan ryhmitellä teemoittain. Kuitenkin on huomioitava, etteivät haastattelujen teemat välttämättä seuraa tutkijan laatimaa järjestystä ja jäsennystä, vaan aineistosta voi löytyä uusia teemoja. (Saaranen-Kauppinen & Puusniekka, 2006.) Hirsjärvi ym., (2004, 211) toteavat, ettei kvalitatiivisessa tutkimuksessa analysointia eroteta erilliseksi tutkimusvaiheeksi, toisin kuin kvantatiivisessa tutkimuksessa, vaan analysointi tapahtuu yhtä aikaa aineiston keräämisen kanssa.

Kuten jo aiemmin mainittiin, tässä tutkimuksessa haastatteluiden nauhoitteet litteroitiin analyysiä varten. Litteroitu aineisto luettiin useampaan kertaan kokonaiskuvan muodostamiseksi. Analysointia tehtiin kuitenkin yhtä aikaa aineiston keräämisen kanssa, eli jo haastattelutilanteessa haastateltavan kertomaa pyrittiin vertaamaan muun muassa taustateoriaan. Aineistoa pelkistettiin eri teemojen mukaan ja aineistosta pyrittiin löytämään mahdollisimman paljon erilaisia perusteluita tai syitä, jotka liittyivät tutkimustehtävään. Löydetyistä perusteluista ja syistä taas pyrittiin löytämään yhtäläisyyksiä ja eroavaisuuksia, kuten esimerkiksi löytämään toistuvia ilmaisuja tai selityksiä. Jokaisesta haastattelusta tutkimustehtävän kannalta tärkeimmät teemat merkittiin eri väreillä. Koska haastattelut olivat keskustelunomaisia, tuli haastatteluista esille myös uusia teemoja, joista muodostui niin sanottuja alateemoja.

Alasuutari (2012, 39–40) esittää laadullisen tutkimuksen analyysiin liittyvän viittaamisen aikaisempiin tutkimuksiin, aiemmin testattuihin hypoteeseihin, teoreettiseen viitekehykseen sekä muuhun aihetta käsittelevään kirjallisuuteen itse tuotettuja havaintoja selitettäessä. Tässä tutkimuksessa saman aihepiirin aiemmat tutkimukset on esitelty luvussa neljä, mutta vertailu muihin tutkimuksiin ja muuhun kirjallisuuteen esitellään luvussa seitsemän.

6 TUTKIMUSTULOKSET

Tämän luvun tarkoituksena on esitellä tutkimuksen tulokset. Kuten jo aiemmin luvussa neljä mainittiin, neutralisoimisteoria on yksi kriminologian eniten käytetyistä teorioista. Teorian tulkinnassa on kuitenkin eroja, riippuen millaisessa yhteydessä teoriaa on tarkasteltu tai millaista rikosta tai normien poikkeavuutta tutkimus käsitteli. Tästä syystä luvun alussa esitellään, miten teoria on tässä tutkimuksessa tulkittu ja liitetty tietoturvarikkomuksiin. Tutkimustulosten esittely on jaoteltu teemoittain neutralisoimisteorian olettamusten ja eri neutralisoimistekniikoiden mukaan. Luvun lopussa arvioidaan toteutetun tutkimuksen luotettavuutta.

6.1 Teorian tulkinta

Kriminologia on tieteenala, joka tutkii sekä rikoskäyttäytymistä että sen herättämiä yhteiskunnallisia ja yksilöllisiä reaktioita. Näihin reaktioihin kuuluvat rikosoikeudelliset rangaistukset, mutta myös rikollisiin kohdistuvat epäviralliset ja sosiaaliset sanktiot, kuten muiden ihmisten paheksunta. (Kivivuori, 2008, 19.)

Vaikka aiemmin luvussa neljä neutralisoimisteoria ja sen neutralisoimistekniikat esiteltiin jo lyhyesti, on tähän lukuun lainattu kaikki neutralisoimisteorian neutralisoimistekniikat niiden alkuperäiskielellä sekä otteita neutralisoimisteorian olettamuksista. Tällä tavoin lukijalle pyritään esittämään, mistä tämän tutkimuksen tulkinta on peräisin. Koska alkuperäinen neutralisoimisteoria on kehitetty hyvin erilaiseen sosiotekniseen ympäristöön kuin esimerkiksi tämän päivän organisaatioiden tietojenkäsittely-ympäristö, ei tämän tutkimuksen kannalta ole relevanttia käsitellä muun muassa rikollisuuden alakulttuuria. Seuraavien (taulukko 3, taulukko 4) alkuperäisestä teoriasta poimittujen lauseiden avulla pyritään kuvailemaan, kuinka teorian olettamuksia tulkitaan tässä tutkimuksessa tietoturvan yhteydessä.

TAULUKKO 3 Syyllisyyteen ja häpeää liittyviä olettamuksia

Syyllisyyteen ja häpeään liittyviä olettamuksia	
"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)	Henkilöstä voi havaita syyllisyyttä ja häpeää, joka on yhteydessä tietoturvarikkomukseen. Häpeä ja syyllisyys eivät ole esimerkiksi ymmärtämättömyyden aiheuttamaa häpeää, vaan nimenomaan tietoturvarikkomukseen eli teon tekemiseen liittyvää häpeän ja syyllisyyden tunnetta.
"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." (Sykes & Matza, 1957, 666)	Henkilö rikkoo tietoisesti tietoturvaohjetta, eikä tunne syyllisyyttä tai häpeää, koska henkilö kokee tekevänsä moraalisesti oikein. Teko luokitellaan enemmän esimerkiksi yhteiskunnan tai sosiaalisen yhteisön hyveeksi, kuten oikeudenmukaisuus tai kohtuus.
"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)	Henkilö on sitoutunut organisaation sosiaaliseen järjestelmään ja on sisäistänyt tietoturvaohjeet sekä niiden noudattamisen vaatimukset, eli kykenee erottamaan sopivan ja sopimattoman toiminnan toisistaan. Tietoturvarikkomus aiheuttaa siten henkilössä syyllisyyttä ja häpeää.
"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 & Matza, 1957, 666)	Välttyäkseen tietoturvarikkomuksen aiheuttamilta itsesyytöksiltä, henkilö oikeuttaa itsensä rikkomukseen (poikkeavaan käytökseen) ja syyttää teosta muita. Oikeuttaminen toimii poikkeavan käyttäytymisen mahdollistajana, ja oikeutuksella henkilö suojelee itseään itsesyytöksiltä, jolloin teon oikeutus tehdään siis jo ennen tekoa.

Eri kriminologian teoriat tuovat vahvasti esille se, että rikollinen käyttäytyminen opitaan vuorovaikutuksessa kommunikaatioprosessien kautta (Kivivuori, 2008). Vaikka tietoturvarikkomusten yhteydessä eri tekniikoiden oppiminen ei välttämättä olisikaan keskeinen tekijä, sitä ei täysin voida sivuuttaa tässäkään yhteydessä. Sykes ja Matza (1957) esittävät oppimiseen liittyvät olettamuksensa seuraavasti:

> "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. The classic statement of this position is found in Sutherland's theory of differential association, which asserts that criminal or delinquent behavior involves the learning of (a) techniques of committing crimes and (b) motives, drives, rationalizations, and attitudes favorable to the violation of law." (Sykes & Matza, 1957, 664)

> "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)

Tietoturvarikkomusten yhteydessä opittava asia voi olla motivaatio tai myönteinen asenne tietoturvarikkomuksia kohtaan. Kuten aiemmin luvussa kolme kerrottiin, sosiaalinen kontrolli liittyy sekä normiin että poikkeavuuteen, joten seuraavaan taulukkoon on koottu alkuperäisen teorian olettamuksia sosiaalisen kontrollin merkityksestä. Koska alkuperäisessä teoriassa viitataan useaan otteeseen yhdenmukaisuuden vaatimuksesta, tulkitaan teoriaa tässä tutkimuksessa enemmän oikeussosiologisesta näkökulmasta kuin filosofian näkökulmasta. Tällä tarkoitetaan tulkintaa, joka mukaan normia ei ylläpidetä vain palkintojen ja rangaistusten avulla, vaan ihmisten välisen vuorovaikutuksen kautta.

TAULUKKO 4 Sosiaaliseen kontrolliin liittyviä olettamuksia

Sosiaaliseen kontrolliin liittyviä olettamuksia	
"As Morris Cohen once said, one of the most fascinating problems about human behavior is why men violate the laws in which they believe. This is the problem that confronts us when we attempt to explain why delinquency occurs despite a greater or lesser commitment to the usages of conformity. 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 as qualified guides for action, limited in their applicability in terms of time, place, persons, and social circumstances. 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 condition." (Sykes & Matza, 1957, 666)	Sosiaaliset arvot ja normit ovat harvoin, jos koskaan, ehdottomia määräyksiä, jotka olisivat sitovia kaikissa olosuhteissa. Miksi siis tietoturvaohjeetkaan tätä olisivat? Eli vaikka henkilö tuntee tietoturvaohjeet ja ymmärtää ne, hän voi tulkita ne vain ns. suuntaa antavina. Kuitenkin henkilön tulee ymmärtää milloin ohjetta on noudatettava ja milloin se vain suuntaa antava.
"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)	Tietoturvarikkomuksiin liittyen tulkinta on, että henkilö pyrkii neutraloimaan sosiaalista kontrollia eli yhteisön normien mukaisen käytöksen ohjausta, vahingoittamatta silti omaa minäkuvaansa.
"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, 1957, 665)	Henkilö ei ole täysin piittaamaton vaatimuksille, joita mukautuminen organisaation sosiaaliseen järjestelmään vaatii. Eli henkilö ei täysin kiistä, etteivätkö tietoturvaohjeet ja niiden noudattaminen kuuluisi myös hänelle.
"Thus the delinquent represents not a radical opposition to law-abiding society but something more like an apologetic failure, often more sinned against than sinning in his own eyes." (Sykes & Matza, 1957, 667)	Henkilö ei suoranaisesti vastusta tietoturvaohjeita, vaan kokee oman poikkeavan käyttäytymisensä ikään kuin erillisenä, jolloin juuri hän kohdallaan tietoturvarikkomus on hyväksyttävää, ymmärrettävää tai oikeutettua.

Seuraavaksi poimintoja teoriasta, joiden tulkinta tietoturva kontekstissa ei olisi täysin relevanttia, mutta ne kuvailevat hyvin teorian lähtökohtia ja rikollisen asenteisiin liittyviä olettamuksia.

> "In the second place, observers have noted that the juvenile delinquent frequently accords admiration and respect to law-abiding persons." (Sykes & Matza, 1957, 665)

> "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." (Sykes & Matza, 1957, 665)

> "…but at least it is clear that the delinquent does not necessarily regard those who abide by the legal rules as immoral." (Sykes & Matza, 1957, 665)

> "In fact, as we shall see shortly, an understanding of how internal and external demands for conformity are neutralized may be crucial for understanding delinquent behavior." (Sykes & Matza, 1957, 666)

> "Somehow the demands for conformity must be met and answered; they cannot be ignored as part of an alien system of values and norms." (Sykes & Matza, 1957, 666)

> "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." (Sykes & Matza, 1957, 670)

On toki mahdollista, että henkilö muun muassa erottaa, sekä omat että muiden, erilaiset tietoturvarikkomukset sekä eri tilanteiden merkityksen tietoturvarikkomukselle. Tietoturvarikkomuksiin syyllistyvä voi myös paheksua niitä, jotka eivät noudata tietoturvassa yhteisön eettisiä käyttäytymissääntöjä ja arvoja, mutta suoranainen kunnioitus tai ihailu tietoturvaa noudattavia kohtaa ei välttämättä ole tässä yhteydessä relevanttia.

6.2 Tutkimustulokset

Tässä tutkimuksessa alkuperäistä neutralisoimisteoriaa peilataan tietoturvaan, ja siinä ennen kaikkea salasanojen säännölliseen vaihtamiseen, riittävän vahvan salasanan valitsemiseen sekä epäilyttävien sähköpostiviestien avaamisen välttämiseen, mutta kuten edellisessä luvussa mainittiin, haastatteluissa käsiteltiin myös tietoturvakäyttäytymistä ja tietoturvapolitiikan noudattamista. Koska tietoturvakäyttäytyminen liittyy organisaatiokulttuuriin, käsiteltiin haastatteluissa myös sitä aihetta. Tähän tutkimukseen ei sisällytetä muun muassa Siposen ja Vancen (2010) sekä Barlow ym (2015) tutkimuksissa sovellettuja tekniikoita, "defense of necessity" ja "metaphor of the ledger", vaan ainoastaan alkuperäisen neutralisoimisteorian neutralisoimistekniikat.

6.2.1 Laki vs tietoturva

Jos tarkastellaan Sykes ja Matzan (1957, 666) esille nostamaa ristiriitaa ihmisen käyttäytymisessä ”why men violate the laws in which they believe”, voidaan tietoturvarikkomustenkin yhteydessä tarkastella asiaa tietoturvapolitiikan ja sen noudattamisohjeiden rinnastattavuudesta lakiin. Laki sanana on toki tässä yhteydessä liian vahva, mutta tässä yhteydessä lakiin rinnastuksella kuvataan enemmänkin suhtautumista ja asennetta tietoturvapolitiikkaan ja sen noudattamisohjeisiin. Eli kohdistuuko tietoturvapolitiikkaan ja sen noudattamisohjeisiin samankaltaista kunnioitusta ja uskomista kuin lakiin ja arvostetaanko ohjeiden noudattamista.

Haastatteluiden teemat käsittelivät myös tietoturvakäyttäytymistä ja tietoturvapolitiikan mukaisten ohjeiden noudattamista. Haastateltavat kertoivat heidän kokemuksistaan ja näkemyksistään, ja kuvailivat ohjeiden noudattamiseen ja kunnioittamiseen liittyvää käyttäytymistä muun muassa näin:

> ”Enemmän se on niin, että ohjeen ehkä liiankin tarkka noudattaminen johtaa siihen, ettei uskalleta tehdä mitään, jos ei varmasti ymmärretä ohjetta.”
>
> ”Kyllä, itse ainakin pyrin toimimaan ohjeiden mukaan.”
>
> ”Sanoisin niin, että henkilöt, jotka työskentelevät arkaluontoisten asioiden kanssa, he varmasti tiedostavat ja noudattavat ohjeita.”
>
> ”Ihmiset haluavat miksi vastauksen. Jos sanotaan, että et voi tehdä näin, he kysyvät miksi. Mutta kun henkilö ei sitä syy-seuraus-suhdetta tiedä, eli miksi tarvitsee tehdä näin, koska henkilö ei tiedä tietojärjestelmien ”sielunelämää”, niin henkilö ei edes tiedä tekevänsä väärin.”
>
> ”Asian tekeminen täysin meidän organisaation ohjeiden mukaan aiheuttaa sen, että sieltä tulee loppukäyttäjä sen tehtävän tehneenä verisenä ja hakattuna ulos.”
>
> ”Jos vertaisi lakiin, niin vaihteluväli voi olla vähän suurempi. Organisaation monialaisuus ja erilaiset koulutustaustat vaikuttavat siihen, miten hyvin ohjeet tunnetaan ja sisäistetään, eli ymmärretään ja osataan. Tausta vaikuttaa siihen, mitkä ovat henkilön kiinnostuksen kohteet ja mihin hän kiinnittää huomiota ja keskittyy. Tausta vaikuttaa myös siihen, mitkä asiat henkilö kokee itselleen kuuluvaksi, eli 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 ei tämä minun toiminta nyt tähän vaikuta.”

Sykes ja Matza (1957, 666) ovat todenneet: ”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.” Eli sosiaaliset säännöt ja normit vaativat harvoin, jos koskaan, ehdotonta pakkoa. Sosiaalisiin sääntöihin tai normeihin ei liity ehdottomuutta, vaan ne on ikään kuin suhteellisia, ja sidottuja aikaan, paikkaan, henkilöön tai sosiaalisiin tilanteisiin. Normiin voidaan liittää oletus, että normin poikkeamisesta saattaa olla jokin seuraus tai tekoa voidaan pitää

paheksuttava. Ilman tuota tietoa, yksilö ei välttämättä edes kokisi tarvetta oikeuttaa normista poikkeamista eikä siten hyödyntää neutralisoimisekniikoita. Jos tietoturvapolitiikka ja sen noudattamisohjeet rinnastetaan edelleen lakiin, olkoonkin, että laki on tässä yhteydessä liian vahva sana, on lakiin kirjattu myös seuraukset lain noudattamattomuudesta. Haastateltavien kanssa keskusteltiin ohjeiden noudattamattomuuden seurauksista ja he kertoivat muun muassa näin:

> ”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.”

Eräs haastateltava pohdiskeli mahdollisia syitä tietoturvaohjeiden vastaiseen toimintaan, ja esitti yhtenä vaihtoehtona sen, ettei ohjeiden noudattamista valvota. Eli noudattamisesta tai noudattamattomuudesta ei kummastakaan ole mitään seurauksia, ei palkitsemista, muttei myöskään rangaistusta.

6.2.2 Tietoturvan noudattaminen sosiaalisena normina

Aiemmin tässä luvussa taulukkoon 4 on koottuna neutralisoimisteorian oletamuksia, jotka liittyvät sosiaaliseen kontrolliin. Luvussa kolme on esitetty, että sosiaalinen kontrolli on ihmisen käyttäytymiseen liittyvä käsite. Normilla on yhteys sosiaaliseen kontrolliin ja sosiaalinen normi puolestaan liittyy yhdenmukaiseen toimintaa ja ajatteluun, eli yhteisön jäsenet toimivat yhteiselle tavalla ja ajattelevat yhdenmukaisella tavalla. Kuten jo aiemmin mainittiin, haastateltavien kanssa keskusteltiin tietoturvakäyttäytymisestä ja ohjeiden noudattamisesta, mutta myös yleisesti tietoturvatietoisuudesta. Seuraavassa poimintoja haastateltavien näkökulmista:

> ”Meillä on aika pitkä perinne tietoturvasta, jo ennen tietojärjestelmiä. Tietojärjestelmät tekevät poikkeamat helpommiksi.”

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

> ”Se riippuu, mitä työtä henkilö tekee. Joka käsittelee tietyntyyppistä tietoa, saattaa olla aivan mestari tekemään sitä, ja noudattaa kaikkia ohjeita, ja tietää mitä tehdä. Sitten taas henkilö, joka vain sillon tällöin käyttää järjestelmää ei sitten välttämättä osaa, eikä tiedä kysyä.”

> ”Me saatetaan käyttää joitakin järjestelmiä harvoin, joten ei siihen voi tulla kulttuuria sen käyttämiseen. Toinen piirre on se, että miksi niitä järjestelmiä täytyy olla niin paljon ja kaikki erilaisia. Siksi jokainen niistä on aina tavallaan kuin uusi tilanne, kun joutuu työssä niitä käyttämään.”

6.2.3 Vastuun kieltäminen

Alkuperäisessä neutralisoimisteorianssa vastuun kieltämisestä kerrotaan näin:

> **The Denial of Responsibility.** “In so far as the delinquent can define himself as lacking responsibility for his deviant actions, the disapproval of self or others is sharply reduced in effectiveness as a restraining influence. As Justice Holmes has said, even a dog distinguishes between being stumbled over and being kicked, and modern society is no less careful to draw a line between injuries that are unintentional, i.e., where responsibility is lacking, and those that are intentional. 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. 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. 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. The similarity between this mode of justifying illegal behavior assumed by the delinquent and the implications of a "sociological" frame of reference or a "humane" jurisprudence is readily apparent. It is not the validity of this orientation that concerns us here, but its function of deflecting blame attached to violations of social norms and its relative independence of a particular personality structure. 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 ja Matza, 1957, 667.)

Neutralisaatiotekniikkana vastuun kieltäminen ei välttämättä viittaa mihinkään tiettyyn ulkoiseen tekijään, vaan ikään kuin henkilön oman tahdon katoamiseen, jolloin henkilö kokee olevansa enemmän uhri kuin tekijä. Muun muassa Nykäsen (2011) tulkinta vastuun kieltämisestä tietoturvarikkomusten yhteydessä oli se, että yksilö voisi oikeuttaa itsensä rikkomukseen, koska jokin tietty teko ei ole erikseen kielletty. Tällainen selitys voisi siis olla, että se, mikä ei ole kiellettyä, on sallittua. Tässä tutkimuksessa myötäillään enemmän Ewaldin (2003) tulkintaa, jonka mukaan normi ei noudata täysin lakiin rinnastettavaa logiikkaa, eli jyrkkää kielletyn ja sallitun rajaa. Myös neutralisoimisteoriassa tuodaan esille, ettei normiin sisälly niin sanottua absoluuttista oikeaa ja väärää, vaan normit luovat (myös joustavia) rajoja ja tietynlaista tilannesidonnaisuutta.

Tietoturvaohjeisiin liittyen eräs haastateltava mainitsikin näin:

> ”Onhan joissain ohjeissa varmasti puutteita, mutta ei niihin voi tyhjentävästi laittaa kaikkea, mitä saa tehdä ja mitä ei saa tehdä.”

Haastateltavien kanssa keskusteltiin tutkimustehtävän mukaisista teemoista, jotka liittyivät siihen, kuinka haastateltavat perustelevat itselleen sitä, että eivät vaihda salasanoja säännöllisesti, jos järjestelmä ei pakota, tai eivät valitse riittävän vahvaa salasanaa, jos sitä ei ehdottomasti vaadita. Haastateltavat kertovat muun muassa näin:

> ”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.”

> ”Se on yksinkertaisesti muistin takia, kun en voi kirjoittaa salasanoja jollekin paperille, josta joku muu voi löytää ne, ja siten saada kaikki salasanat samalla kertaa.”

Myös muut haastateltavat, jotka käyttivät useampaa kuin neljää tai viittä tietojärjestelmää, kertoivat salasanojen muistamiseen liittyvästä ongelmasta, jolloin käyttäjä oli joutunut esimerkiksi pyytämään järjestelmän tai järjestelmien niin sanottua uudelleen aukaisua, tai kirjoittamaan salasanoja paperille muistin tueksi.

Eräs haastateltava nosti esille myös kysymyksen siitä, onko tietoturvallisempaa, että käyttäjät joutuvat vaihtamaan salasanoja usein, jolloin rajallista muistia rasitetaan kohtuuttomasti, vai onko tietoturvallisempaa, että salasana vaihdetaan vain harvoin. Eräs haastateltava käänsi katsetta myös tietojärjestelmien laatuun:

> ”Ne pitää olla niin laadukkaita, että käyttäjän ei tarvitse taistella itsensä kanssa siitä, muuttaako sitä salasanaa, vaihtaako sitä ja onko se tarpeeksi vahva. Siis ainahan on käyttäjän syy, jos tulee joku tietoturvarikkomus tai rike. Sehän on aina käyttäjän syy, jos se ei johdu jostain laitteesta. Mutta miksi tehdä sellaisia järjestelmiä, jotka mahdollistavat sen rikkomuksen, koska jos se on mahdollista, silloin se myös tapahtuu. Käyttäjä on aina vastuussa, mutta ei pitäsi liikaa antaa mahdollisuuksia rikkeisiin.”

Epäilyttävien sähköpostiviestien avaamisen välttämiseen liittyen henkilö voisi perustella vastuun kieltämistä sillä, että ei tulkinnut viestiä epäilyttäväksi, koska se tuli esimerkiksi organisaatiossa olevalta henkilöltä tai että luotti organisaation tietoturvaratkaisuihin, jolloin epäilyttäviä sähköposteja ei pitäisi edes päästä läpi. Haastateltavat vaikuttivat suhtautuvan epäilyttäviin sähköposteihin erittäin epäilevästi, eikä niitä siten avata. Kuitenkin eräs haastateltava mainitsi näin:

> ”Mutta jos viesti tulee tai näyttää tulevan oman organisaation nimissä, ei me kyseenalaisteta sitä.”

6.2.4 Vahingon kieltäminen

Alkuperäisessä neutralisoimisteorianssa vahingon kieltäminen selitetään näin:

> **The Denial of Injury.** "A second major technique of neutralization centers on the injury or harm involved in the delinquent act. The criminal law has long made a distinction between crimes which are mala in se and mala prohibita that is between acts that are wrong in themselves and acts that are illegal but not immoral-and the delinquent can make the same kind of distinction in evaluating the wrongfulness of his behavior. 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. 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. We are not suggesting that this technique of neutralization, labelled the denial of injury, involves an explicit dialectic, Rather, we are arguing that the delinquent frequently, and in a hazy fashion, feels that his behavior does not really cause any great harm despite the fact that it runs counter to law. Just as the link between the individual and his acts may be broken by the denial of responsibility, so may the link between acts and their consequences be broken by the denial of injury. 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 ja Matza, 1957, 667).

Neutralisoimisteorian mukaan vahingon kieltämisessä tekijä ei kiellä tekoa, mutta tekijä haluaa kiistää sen, että teko aiheuttaisi vahinkoa. Tietoturvan yhteydessä tämän tekniikan tulkinnat ovat olleet muun muassa, ettei tietoturvarikkomuksesta aiheutunut vahinkoa, tai ettei käyttäytymisestä aiheudu mitään haittaa tai harmia, tai että työntekijä teki parhaansa minimoidakseen organisaatiolle aiheutuvaa vahinkoa (Siponen & Vance, 2010; Nykänen, 2011; Kim ym, 2014).

Tutkimuskysymyksen kannalta se tarkoittaisi esimerkiksi tilannetta, että henkilö täysin tietoisesti ja tarkoituksellisesti avaisi epäilyttävän sähköpostiviestin. Vaikka teko olisi täysin vastoin organisaation tietoturvapolitiikkaa, henkilö kyseenalaistaisi tai vähättelisi aiheuttamansa vahingon suuruutta. Haastatteluissa tällaista esimerkkinä mainittua sähköpostiviesteihin liittyvää tietoturvarikkomusta ei tullut esille.

Haastateltavien kanssa keskusteltiin myös heidän näkymyksistään ja kokemuksistaan siihen, kuinka kohdeorganisaatiossa suhtaudutaan tietoturva-rikkomuksiin. Haastatteluiden perusteella tietoturvarikkomuksia ei ole mitään syytä kieltää tai salailla. Organisaation ilmapiiristä kerrottiin muun muassa näin:

> "Siinä ei ole sellaista kynnystä, että joku peittelisi sen takia ja ei haluaisi kertoa kenellekään, vaan mielummin kertoo heti. Se tulee siitä, että voi olla oikeasti tosi vaarallista, jos ei kerro."

”Jos nyt sattuisi sen sähköpostin liitteen aukaisemaan ja sieltä tulisi virus, sen uskaltaa kertoo.”

”Käsi ylös virheen merkiksi. Eli kertoo suoraan, että tämä oli nyt virhe.”

Haastateltavien kanssa keskusteltiin myös salasanojen vaihtamiseen ja vahvojen salasanojen valitsemiseen liittyvistä teemoista, jolloin he kertoivat muun muassa näin:

”Minulla on niin vahvat salasanat, ja ne on niin hankalat tehdä, että koen ne turvalliseksi.”

”Jos pitäsi tietää, mistä se vaihdettasi, niin en edes muista enää.”

”Niin se salasana on aika vahva. Tosin se on ollut minulla pitkään, mutta se on vahva.”

Haastateltavat selittivät salasanojen vaihtamattomuutta myös näin:

”Perustelen sen sillä, että meidän järjestelmä, missä näitä salasanoja käytän, on kuitenkin sillä tavalla suljettu, jolloin ei tunnu merkitykselliseltä vaihtaa salasanaa, koska tieto siitä, että järjestelmään ei pääse ulkopuolelta pienentää tarvetta harkita sitä, että onko salasana tarpeen vaihtaa, että joku pääsee siihen minun salasanaan käsiksi, koska sen pitäsi päästä sen järjestelmän sisälle.”

”Olen sitä mieltä, että ei sillä ole mitään merkitystä.”

6.2.5 Uhrin kieltäminen

Alkuperäisessä neutralisoimisteorianssa uhrin kieltäminen selitetään näin:

The Denial of the Victim. “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. By a subtle alchemy the delinquent moves him- self into the position of an avenger and the victim is transformed into a wrong-doer. 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. As Orwell has pointed out, the type of criminal admired by the general public has probably changed over the course of years and Raffles no longer serves as a hero; but 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. To deny the existence of the victim, then, by transforming him into a person deserving injury is an extreme form of a phenomenon we have mentioned before, namely, the delinquent's recognition of appropriate and inappropriate targets for his delinquent acts. In addition, however, the existence of the victim may be denied for the delinquent, in a

> somewhat different sense, by the circumstances of the delinquent act itself. 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. 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 ja Matza, 1957, 668)

Neutralisoimisteorian mukaan uhrin kieltämisessä halutaan kertoa, että uhri olisi esimerkiksi niin moraaliton, että ansaitsi joutua rikoksen kohteeksi. Tekijä siis perustelee tekoa itselleen eräänlaisena laillisena kostona. Muun muassa Willison ym., (2016) olettamuksen mukaan työntekijän organisaation taholta kokema epäoikeudenmukaisuus on yhteydessä väärinkäytös aikomuksiin.

Kun teoriaa peilaa tietoturvarikkomuksiin ja tutkimuskysymyksessä mainittuihin salasanojen säännölliseen vaihtamiseen, riittävän vahvan salasanan valitsemiseen ja epäilyttävien sähköpostiviestien avaamisen välttämiseen, voidaan kysyä, kuka on uhri, joka muutetaan väärintekijäksi. Muun muassa Siponen & Vance (2010) ja Nykänen (2011) jättivät tämän tekniikan huomioimatta, koska heidän mukaansa tietoturvarikkomusten yhteydessä on vaikea osoittaa, kuka on uhri.

Haastatteluissa aiheesta kuitenkin keskusteltiin hypoteettisesti. Mikäli organisaatio katsottaisiin uhriksi, jolle haluttaisiin kostaa jotain, mainitsevat haastateltavat muun muassa näin:

> "No on se rikos, jos henkilö tietoisesti tekisi organisaatiota vastaan jotain."

> "Kyllä mä lähtisin rikoksesta puhumaan. Rikkomuksia sattuu, kuten väärään mediaan väärä laite, ja sellaisia tapahtuu, mutta jos tietoisesti vie tietoa väärään paikkaan väärälle taholle, niin kyllä minä lähtisin rikoksesta liikkelle. Tietysti on otettava huomioon, millaista tieto on ja mitä vaikutusta sillä on, kuten muuttaako se jotain kokonaisuutta."

> "Yleisesti näen niin, että jos henkilö tietoisesti rikkoo tietoturvallisuuden ohjeistusta... tai lähdetään purkamaan niin päin, että rikkoo lakia, ohjeistusta ja käskettyjä toimintatapoja ja menetelmiä, niin kyllä se on silloin vähintääkin rikkomus ja äärimmillään se voi olla rikos, kun mennään siihen, kuinka vaikuttava tiedon menetys oli. "

Teon tarkoituksellisuudessa nimenomaan halu kostaa jotain, muutti haastateltavien mukaan normien vastaisen tietoturvarikkomuksen rikolliseksi toiminnaksi. Tällainen rikos voisi olla esimerkiksi Nicho & Kamoun (2014) tutkimuksessa esitelty irtisanotun työntekijän halu kostaa. Myös Willison ja Warkentin (2013) tuovat esille tämän kaltaisen tahallisen toiminnan, joka voi tarkoittaa sisäpiiriläisen tekemiä väärinkäytöksiä, kuten tietojen tahallinen hävittäminen, tietomurto, petos, kiristys tai kavallus. Sisäpiiriläiset voivat myös myydä tai luovuttaa luokiteltua tai salaista tietoa julkisuuteen tai muille organisaation ulkopuolisille.

6.2.6 Tuomitsijoiden tuomitseminen

Alkuperäisessä neutralisoimisteorianssa selitetään näin:

> **The Condemnation of the Condemners.** "A fourth technique of neutralization would appear to involve a condemnation of the condemners or, as McCorkle and Korn have phrased it, a rejection of the rejectors." The delinquent shifts the focus of attention from his own deviant acts to the motives and behavior of those who disapprove of his violations. His condemners, he may claim, are hypocrites, deviants in disguise, or impelled by personal spite. 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. Teachers always show favoritism and parents always "take it out" on their children. By a slight extension, the rewards of conformity-such as material success- become a matter of pull or luck, thus de- creasing still further the stature of those who stand on the side of the law-abiding. The validity of this jaundiced viewpoint is not so important as its function in turning back or deflecting the negative sanctions attached to violations of the norms. 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 wrongfulness of his own behavior is more easily repressed or lost to view." (Sykes ja Matza, 1957, 668)

Neutralisoimisteorian mukaan tuomitsijoiden tuomitsemisessa henkilö neutralisoi oman poikkeavan käyttäytymisensä siirtämällä huomion itsestään ja omasta normista poikkeavasta käyttäytymisestä heihin, jotka paheksuvat tai tuomitsevat poikkeavan tai rikollisen käytöksen. Tietoturvarikkomusten yhteydessä tämä tekniikka on tulkittu yksilön asennoitumisena tietoturvapolitiikkaan ja sen noudattamisohjeita kohtaan (Nykänen, 2011; Siponen & Vance, 2010.)

Tutkimuskysymyksen kannalta tarkasteltuna henkilö neutraloisi omaa toimintaansa kyseenalaistamalla tietoturvapolitiikkaan liittyvät ohjeet salasanojen säännöllistä vaihtamisesta, vahvojen salasanojen käyttämisestä sekä epäilyttävien sähköpostiviestien avaamisen välttämisestä.

Haastateltavien kanssa keskusteltiin heidän näkemyksistään, kokemuksistaan ja asenteistaan tietoturvapolitiikkaan ja sen noudattamisohjeisiin. Haastateltavien kanssa keskusteltiin muun muassa, kuinka hyvin he tuntevat ohjeet, kuinka helposti ohjeet on löydettävissä, ovatko ohjeet selkeitä ja ymmärrettäviä, mutta myös yleisestä asennoitumisesta tietoturvaan. Keskustelujen avulla pyrittiin muodostamaan käsitystä haastateltavien asenteista. Ohjeiden löytämiseen liittyviä ajatuksia haastateltavat kertoivat muun muassa näin:

> "Ei edes tiedetä, mistä lähteä niitä etsimään. Tieto ei ole oikeastaan niin hajallaan, eli tiedon hakeminen ei välttämättä ole ongelma, vaan sen tiedon hyödyntäminen siinä omassa työssään."

> "Joo, siis kaikkihan on helposti löydettävissä, jos tiedät mistä etsiä. Sanotaanko, että jos työtehtävässä menee tunti tiedon löytämiseen, niin kyllähän siinä mielummin tekee, kuin etsii, koska muuten työt jää tekemättä."

Ohjeiden soveltamisesta eräs haastateltava kertoi näin:

> ”Pakkohan se on voida soveltaa, koska joku niitä kirjottaessaan ei voi tietää kaikkia tilanteita, missä niitä käytetään, mutta silloin se pitää tehdä henkilön kanssa, joka on vastuussa turvallisuudesta ja tietoturvallisuudesta, kun jotain tehdään vähän eri lailla. Mutta se ei ole lähtökohta tai tavoite, vaan kun on tietty toimitatapa muodostunut, sen mukaan tehdään, mikä on ohjeistettu. Ei joka kerta tehdä eri lailla.”

Haastatteluiden perusteella epäilyttävien sähköpostiviestien avaamisen välttämiseen liittyvään ohjeistukseen ja muuhun informaatioon suhtautuminen oli asiallista ja ohjeistus oli ymmärretty hyvin. Haastateltavat kertoivat muun muassa näin:

> ”Meillä intrassa aina varoitetaan, jos liikkeellä on suurempi määrä epäilyttäviä sähköposteja henkilöstölle, ja siellä on ilmoitus, että älkää avatko.”

> ”Kyllä tiedän, etten avaa ja ilmoitan, että tällainen viesti on tullut, ja ne perustiedot siitä mitä näen.”

> ”Minulle se on täysin selvä asia, että poistan viestit, jos en tunnista lähettäjää.”

Kysyttäessä, miten tämä yksittäinen ohjeistus oli sisäistetty niin hyvin, haastateltavat kertoilivat muu muassa näin:

> ”No kyllä tietoa tulee intrasta, ainakin jos on ollut havaintoja, mutta kun katson omaa henkilökohtaista sähköpostia ja kuinka paljon sinne roskapostiin kertyy viestejä, niin kyllä se tulee sieltäkin se tieto.”

> ”Ehkä se tieto perustuu enemmän siihen, mitä on lukenut julkisista lähteistä, ja mitä maailma koko ajan tuo esille. Ehkä se tulee selkeämmin esille sieltä.”

Vaikka osa ohjeista olikin ymmärretty hyvin, mainitsivat haasteltavat tietoturvapolitiikan olevan niin laaja, että vain harvalla on selkeä käsitys muun muassa sen sivumäärästä. Myös soveltaminen arkisiin työtehtäviin koettiin hankalaksi. Eräs haastateltava esittikin toiveen:

> ”Pitäsi olla sellainen kokopäivätoiminen henkilö, jolla olisi oikeasti aikaa perehtyä siihen, ja joka oikeasti lukisi niitä (tietoturvaohjeita), pitäsi yllä, tekisi koulutuksia ja tekisi omalle henkilöstölle siihen liittyviä ohjeita ja vastaavia.”

Toinen puolestaan selitti:

> ”Me keskustellaan myös työkavereiden kanssa, miten asioita pitäisi tehdä ja sanoisin, että jossain paikoissa asiat on tehty vähintään vaikeaksi ellei jopa mahdottomiksi ja koulutukseen ei panosteta missään nimessä tarpeeksi.”

Haastateltavat toivat myös esille, kuinka organisaation erilaisiin tarpeisiin luotujen tietojärjestelmien käyttöympäristöihin suhtauduttiin eri tavoin, vaikka tietoturvapolitiikka ja sen noudattamisohjeet ovat kaikkialla yhtäläiset.

6.2.7 Vetominen korkeampiin lojaliteetteihin

> **The Appeal to Higher Loyalties. "**Fifth, and last, 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. Rather, the delinquent may see himself as caught up in a dilemma that must be resolved, unfortunately, at the cost of violating the law. One aspect of this situation has been studied by Stouffer and Toby in their research on the conflict between particularistic and universalistic demands, between the claims of friendship and general social obligations, and their results suggest that "it is possible to classify people according to a predisposition to select one or the other horn of a dilemma in role conflict." For our purposes, however, 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 ja Matza, 1957, 669)

Neutralisoimisteorian mukaan korkeampiin lojaliteetteihin vetoamisella halutaan niin sanotusti hämärtää sekä itselleen että muille teon rikollista tarkoitusta. Tämä neutralisoimistekniikka on joissain tutkimuksissa käännetty suomeksi tarkoittamaan myös korkeampia arvoja tai korkeampia periaatteita. Tietoturvarikkomusten yhteydessä teoriaa on tulkittu siten, että työntekijä voisi väittää rikkoneensa tietoturvapolitiikkaa saadakseen työnsä tehtyä, tai työmotivaation tai työssä jaksamisen vuoksi, tai teon oli tarkoitus suojella perhettä, ystäviä tai yritystä. (Siponen & Vance, 2010; Nykänen, 2011, Kim ym., 2014).

Kun tätä neutralisaatiotekniikkaa tarkastellaan salasanojen ja sähköpostin yhteydessä, se tarkoittaisi ristiriitaa henkilön sisäisten ja ulkoisten sosiaalisten kontrollien vaatimuksissa. Neutralisoimisteoriaa tulkintaa tässä yhteydessä niin, että henkilö ei noudattaisi organisaation ohjeita salasanakäytännöissä tai epäilyttävien sähköpostien avaamisen välttämisessä, vaan jokin muu sosiaalinen side, henkilökohtainen arvo tai periaate merkitsisi tietyssä tilanteessa enemmän.

Haastateltavat eivät tuoneet esille erityisesti juuri salasanoihin tai sähköpostiviesteihin liittyviä sosiaalisia siteitä, henkilökohtaisia arvoja tai periaatteita. Koska tutkimuksen teemat käsittelivät myös tietoturvakäyttäytymistä ja ohjeiden noudattamista, tarkastellaan tätä neutralisaatiotekniikkaa tässä yhteydessä kiireen kautta. Haastateltavat kertoivat muun muassa näin:

> ”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 salittua tehdä.”

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

> ”Esimies on käskenyt tehdä jotain, ja haluat tietenkin tehdä sen tietyssä ajassa ja järjestelmä ei toimi. Se on vaihe, jota perustellaan kiireellä.”

> ”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.”

Voidaan toki kysyä, onko kiire todellinen, mutta myös sitä, ketä kohtaan lojaliteetti kohdistuu, tai millainen arvo tai periaate koetaan korkeammaksi kuin tietoturvaohjeiden noudattaminen. Tässä kohdassa on otettava huomioon, että kohdeorganisaatiossa kyse voi olla todellisesta kiireestä, koska tilanteet saattavat muuttua nopeasti ja päätöksiä on kyettävä myös tekemään nopeasti.

Koska kiire voi siis olla todellinen, jolloin tehtävän suorittaminen vaikuttaa, erään haastateltavan sanoja lainaten, ”toiminnan jatkuvuuteen”, jolloin henkilön arvoissa tehtävän suorittaminen olisi korkeampi arvo tai periaate kuin tietoturvaohjeiden noudattaminen. Tällöin lojaliteetti kohdistuisi organisaatioon, eli toiminnan jatkuvuuden turvaamiseen. Haastateltavat kertoivat tässä kohtaa muun muassa näin:

> ”Mutta täytyy miettiä, mikä on itse tarkoitus. Eli mitä me tehdään ja mihin me halutaan sitä tietoa. Itseistarkoitus ei ole tiedon turvaaminen, vaan sen käyttäminen ja tuottaminen, ja sitä kautta tehtävät analyysit ja päätökset.”

> ”Tänä päivänä monelle organisaatiolle tuttu asia, 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.”

> ”Käytännön elämässä osa tehtävistä on täysin mahdottomia. Se järjestelmä ei taivu välttämättä kaikessa edes siihen tietoturvaohjeeseen.”

Kun tarkastellaan, millaisia periaatteita haastateltavat kokivat korkeammaksi kuin tietoturvaohjeiden noudattaminen, haastateltavat mainitsevat halun suorittaa jokin tehtävä tietyssä ajassa. Eräs haastateltava selittää asiaa näin:

> ”Ajattelen aina niin, että tietty asia ratkaisee tulevia asioita ja jos joku asia jää puolitiehen, niin se hidastaa myös muita asioita, eli näen niin, että asia ei kokonaisuutena etene, jos joku asia on pois eikä ole valmis.”

6.2.8 Oppiminen

Vaikka luvun alussa mainittiin, ettei oppiminen, siinä mielessä kuin Sykes ja Matza (1957) sen esittelevät, olisi relevanttia tietoturvarikkomusten yhteydessä, tuli haastatteluissa silti esille myös oppimiseen liittyviä tekijöitä. Haastateltavat kertoivat muun muassa näin:

> ”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.”

> ”Noudatetaan mallia, eli toimitaan samalla tavalla kuin toinenkin.”

6.2.9 Syyllisyys ja häpeä

Sykes ja Matza (1957) esittivät syyllisyyteen ja häpeään liittyvinä olettamuksina sen, että henkilö käyttää neutralisoimistekniikoita välttääkseen syyllisyyden ja häpeän tunteitaan. Tieteenalana psykologia lienee tutkinut eniten syyllisyyden ja häpeän tunteita. Tämän tutkimuksen tarkoitus ei ole perehtyä syvällisesti tuohon psykologian aihealueeseen, vaan esitellä vain lyhyesti noiden tunteiden luonne. Silfver-Kuhalammen ja Helkaman (2012) mukaan syyllisyys ja häpeä ovat moraalitunteita, jotka kohdistuvat pääasiassa yksilön omiin moraalisiin rikkomuksiin, heikkouksiin ja toimivat itsesäätelyn taustalla. Vaikka eri kielissä ja kulttuureissa sanoilla ”syyllisyys” ja ”häpeä” onkin vaihtelua, näyttäisi kuitenkin siltä, että syyllisyys liitetään huoleen toisten hyvinvoinnista ja haluun korjata aiheutunut vahinko. Häpeä puolestaan liitetään kokemukseen omien heikkouksien julkisesta paljastumisesta ja haluun vetäytyä tai piiloutua. (Silfver -Kuhalammen ja Helkaman , 2012.)

Luvun alussa olevaan taulukkoon (taulukko 3) on koottu tämän tutkimuksen tulkinnat neutralisoimisteorian olettamuksista. Henkilö olisi tulkinnan mukaan sitoutunut organisaation sosiaaliseen järjestykseen ja sisäistänyt tietoturvaohjeet sosiaalisena normina. Syyllisyys, häpeä ja itsesyytökset liittyisivät siten tietoturvarikkomukseen, jolloin yksilö suojelisi omaa minäkuvaansa käyttämällä neutralisoimistekniikoita poikkeavuuden oikeutukseen. Toisaalta yksilö ei kokisi syyllisyyttä ja häpeää, mikäli hän kokisi toimineensa moraalisesti oikein.

Haastatteluissakin käsiteltiin tilanteita, joissa syyllisyyttä ja häpeää tunnetaan. Haastatteluissa nousi esille erilaisia tilanteita, joissa tunnetaan syyllisyyttä ja häpeää, mutta myös tilanteita, jolloin syyllisyyden ja häpeän tunteita ei joko ole tai niitä ei osoiteta. Haastateltavat kertoivat häpeästä muun muassa näin:

> ”Jo pelkästään se aiheuttaa häpeää, että kuullaan jossain asiassa, eli ei kuulustella. En kyllä tiedä yhtään henkilöä, johon sillä ei olisi vaikutusta.”

> ”Koska ammattimaisuus on merkittävä organisaatio arvo ja virheettömyys on päivittäisessä työssä esillä ja sitä kautta varmasti sellaista häpeää tunnetaan, jos virhe tehdään. Yksilötasolla häpeä kyllä on tunnistettavissa ja näkyy.”

> ”Melkein kaikki tapaukset on suurimmaksi osaksi tapahtunut inhimillisestä virheestä ja kyllä niissä tapauksissa, mitä on ollut, huomaa henkilöistä, että on pahoillaan siitä asiasta, että näin nyt sattui käymään.”

> ”Kun usempi toimija toimisi virheellisesti, niin siinä tapauksessa sitä häpeää ei ehkä ole, koska silloin on tehty porukalla joku väärä toiminta, vaikka se olisi tiedettykin, niin siinä on sellainen tilanne, jossa sitä häpeää ei enää tulekaan, koska oltiin osana joukkoa ja toimittiin joukossa virheellisesti.”

> ”No en havainnut suoranaisesti, että henkilöä hävettäisi. Kun on täysin tiedostamattomasti tehnyt, niin se on tavallaan sen kautta, voiko sanoa, oikeutettu. Hän ei tiennyt sitä. Hän luuli tekevänsä oikein.”

6.2.10 Poikkeavan käyttäytymisen mahdollistaja

Sykes & Matza (1957, 666) mainitsevat näin: ”But there is also reason to believe that they precede deviant behavior and make deviant behavior possible.” Marunan ja Copesin (2005) ovat tulkinneet lauseen siten, että teorian mukaan poikkeava käyttäytyminen etenee kronologisessa järjestyksessä. Eli neutralisoimistekniikat edeltävät tekoa ja toimivat poikkeavan käyttäytymisen mahdollistajana. Teorian voi tulkita tässä kohtaa niin, että ilman neutralisoimistekniikoita tietoturvarikkomusta ei olisi edes mahdollista tehdä. Haastatteluiden perusteella tietoturvarikkomus on mahdollinen ilman, että henkilö hyödyntää neutralisoimistekniikoita.

Toisaalta mahdollistajan voi tulkita myös niin, että jos henkilö on kerran hyödyntänyt jotakin neutralisoimistekniikka ja todennut sen toimivaksi, hän hyödyntäisi sitä jatkossakin. Tässä kohdassa eräs haastateltava totesi näin:

> ”Kun jotakuta on moitittu jostakin asiasta, en ole törmännyt, että asia olisi enää toista kertaa tullut esille saman henkilön kohdalla. Kyllä se niin isoa häpeä on, jos joutuu keskustelemaan siitä, mitä on tapahtunut, että ei sitä toista kertaa tee.”

6.3 Muita havaintoja

Vaikka haastateltavat eivät suoranaisesti kyseenalaistaneet salasanojen ympärillä käytyä keskustelua, välittyi silti toiveita teknisistä ratkaisuista, joiden avulla käyttäjällä olisi vähemmän mahdollisuuksia tietoturvarikkomuksiin. Toinen vahvasti esille nostettu asia oli palveluiden ulkoistaminen ja sen mukanaan tuomat ongelmat. Käyttäjät joutuvat tekemään asetuksia ja määrityksiä yhä enemmän ja käyttäjille kohdistuva ohjeiden ja sääntöjen tietotulva on kasvanut. Vaikka organisaation luonteesta johtuen ihmiset ovat tottuneet omaksumaan uusia asioita nopeasti, silti muun muassa tietoturvaohje on vain yksi monista työntekijään kohdistuvista vaatimuksista, joka kilpailee muiden lukemattomien ohjeiden kanssa. Toisaalta haastatteluissa tuli esille palveluiden ulkoistamisesta johtuva toisenlainenkin huolenaihe. Ulkoistaminen oli lisännyt epäluottamusta muun muassa organisaation tietojen turvallisesta säilyttämisestä.

Haastatteluissa tuli esille myös johtavassa tai esimiesasemassa olevien välinpitämättömyys tietoturvaohjeiden noudattamiseen. Haastateltavana ei ollut yhtään ylimmän johdon edustajaa, mutta muutama esimiesasemassa oleva. Haastateltavat muotoilivat aiheesta muun muassa näin:

> ”Johto ei aina kunnostaudu tietoturvan noudattamisessa.”

> ”Suurin tietoturvariski organisaatiossa on asenne kysymys, eli se kuinka paljon siihen oikeasti asennoidutaan, eli otetaan tosissaan se asia.”

Haastatteluissa aiheena sivuttiin myös tietoturvakoulutusta. Vaikka kohdeorganisaatiossa järjestetään haastatteluiden mukaan vuosittaista sekä pakollista että vapaaehtoista tietoturvakoulutusta, koulutus ei välttämättä huomio erilaisten käyttöympäristöjen eroavaisuuksia käytännön tarpeisiin eikä yksilöiden erilaista tapaa oppia ja sisäistää asioita.

7 TARKASTELU

Tässä luvussa esitellään tutkimuksen päälöydökset sekä verrataan tutkimuksen tuloksia aikaisempiin tutkimuksiin ja kirjallisuuteen. Luvussa kerrotaan myös tutkimuksen käytännön hyödynnettävyydestä. Lisäksi luvun lopussa arvioidaan tutkimuksen luotettavuutta sekä esitellään jatkotutkimusaiheita.

7.1 Löydökset

Tutkimustulosten perusteella tehdyt löydökset esitellään samassa järjestyksessä kuin tutkimustulokset edellisessä luvussa. Ensin vertaillaan lakia ja tietoturvaa sekä tietoturvan rinnastusta sosiaaliseen normiin. Aiheet on tässä kohtaa yhdistetty, koska niiden ympärillä käydyt keskustelut liittyvät löydösten osalta hyvin läheisesti yhteen. Näiden jälkeen käydään läpi kukin neutralisoimistekniikka sekä teorian olettamuksia.

7.1.1 Vertailu lakiin ja rinnastus sosiaaliseen normiin

Laki vs tietoturva: Haastatteluiden perusteella tietoturvapolitiikkaan ja sen noudattamisohjeisiin ei suoranaisesti liity samankaltaista kunnioitusta ja uskoa kuin lakiin. Suhtautuminen vaihteli sekä henkilön taustan ja aseman että myös työtehtävien mukaan. Haastatteluiden perusteella myös tietoturvaohjeiden ymmärtämisessä on eroavaisuuksia, eikä henkilö välttämättä ymmärrä oman toimintansa merkitystä. Toisaalta tietoturvaohjeisiin liittyvää kunnioitusta näyttäisi heikentävän se, ettei työntekijä välttämättä koe ohjeiden vastaavan hänen todellisia työtehtäviään, vaan saattaa kokea tietoturvaohjeiden kirjaimellisen noudattamisen hankaloittavan työn tekemistä. Vaikka lakia voidaankin tulkita hyvin eri tavoin, eikä kaikkia lakeja kohtaan välttämättä tunneta kunnioitusta, voidaan silti olettaa, että henkilö lakia rikkoessaan ymmärtää toimivansa lain vastaisesti, ja että toiminnasta mahdollisesti seuraa myös jokin rangaistus. Haastatteluiden perusteella tietoturvarikkomusten seuraukset olivat epäselviä.

Tämä voi osaltaan vaikuttaa tietoturvapolitiikan noudattamisen arvostukseen heikentävästi.

Tietoturvan noudattaminen sosiaalisena normina: Voiko tietoturvaa rinnastaa sosiaaliseen normiin? Luvussa kolme viitataan Ewaldin (2003) toteamukseen, kuinka tekniset normit saattavat noudattaa erilaista aikataulua muihin normeihin verrattuna. Silti nekin voivat muuttua vain hitaasti, koska muutos on sidoksissa teknisen innovaation lisäksi myös ympäristön vastaanotto- ja omaksumiskykyyn. (Ewaldin, 2003, 67.) Vaikka organisaatiolla olisi pitkät perinteet tietoturvasta jo ajalta ennen tietojärjestelmiä, se ei välttämättä tarkoita, että tietoturvakäytännöt olisivat saavuttaneet sosiaalisen normin aseman myös nykypäivän tietojenkäsittely-ympäristössä. Schein (1991, 54-55) on kirjoittanut jo yli kolme vuosikymmentä sitten, eli vuonna 1985 julkaistussa teoksessaan siitä, 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. Neutralisoimisteoriassa viitataan useassa kohtaa yhdenmukaisuuden vaatimukseen, joka edellyttää yhteisön jäsenten yhteistä toimintatapaa ja yhdenmukaista tapaa ajatella (Laine, 2007), eli sisäistettyä normia (Suoninen, 1997).

Koska haastateltavina oli sekä tietoturva-alan asiantuntijoita että niin sanottuja loppukäyttäjiä, oli kohdeorganisaatiossa haastatteluiden perusteella havaittavissa, tietoturvan pitkästä perinteestä huolimatta, Scheinin (1991) esille tuoma väittämä erilaisista tarkastelutavoista. Vaikka haastateltavat kertoivatkin tietoturvan liittyvän vahvasti jokapäiväiseen työhön, se ei välttämättä tarkoittanut kaikille haastateltaville yhteistä sosiaalista normia nimenomaan tietojärjestelmien osalta. Kun henkilö esimerkiksi kertoi tuntevansa tietoturvaohjeistuksen ja tietävänsä toimintatavat, mutta ei siltikään kokenut jotain asiaa merkityksellisenä, kyse voi olla aidosta ymmärtämättömyydestä, mutta kyse voi olla myös välinpitämättömyydestä. Toki organisaation tarjoamiin tietoturvaratkaisuihin pitää voida luottaa, mutta tietoturvaohjeet sisältävät käyttäjän tietoturvakäyttäytymistä ohjaavia ohjeita, jolloin käyttäjän voisi olettaa ymmärtävän, ettei esimerkiksi pelkkä tilaturvallisuus voi turvata järjestelmään mahdollisesti kohdistuvaa organisaation ulkopuolelta tulevaa tunkeutusmisyritystä. Toisaalta haastatteluiden perusteella ymmärtämättömyys oli myös täysin aitoa, eli vaikka käyttäjä ymmärsi tietoturvan merkityksen, hän ei pystynyt sisäistämään ohjeiden ja teknisten ratkaisujen yhteyttä todellisiin työtehtäviinsä. Jos tietoturvaohjeiden ymmärtämisessä ja sisäistämisessä on suurta vaihtelua, silloin tietoturvaohjeiden noudattaminen ei välttämättä ole rinnastettavissa sosiaaliseen normiin. Siitä saattaa silloin puuttua muun muassa Suonisen (1997) mainitsema toimintaa ohjaava merkitys. Toisaalta tietoturvapolitiikka ja sen noudattamisohjeet eivät välttämättä voi tarjota sosiaaliseen normiin rinnastettavaa joustoa ja tilannesidonnaisuutta, ja toimia siten vain suuntaa antavina. Vaikka haastatteluissa viitattiinkin siihen, että ohjeita on pakko voida soveltaa, sillä ei kuitenkaan viitattu sosiaalisen normin sisältämään joustavuuteen. Enemmän

soveltaminen liittyi yksittäisen henkilön tekemään ohjeeseen, jossa ei oltu osattu tai voitu ennakoida kaikkia eteen tulevia tilanteita. Yksittäinen henkilö ei siis välttämättä voi asettaa sosiaalista normia, jonka yhteisö tai ryhmä olisi valmis sellaisenaan sisäistämään. Jos tutkimukseen valittuja käytäntöjä tarkastellaan rinnastuksena sosiaaliseen normiin, jolloin tietoturvaohjeiden noudattamattomuuden voi tulkita poikkeavuutena, vain yhden aiheen voi rinnastaa sosiaaliseksi normiksi. Se on epäilyttävien sähköpostiviestien avaamisen välttäminen. Kuten haastateltavat kertoivat, asiasta on keskusteltu paljon ja vaikutteet käyttäytymiseen on saatu sekä organisaation sisältä että ulkopuolelta.

Vaikka aikaisemmissa neutralisoimisteoriaa tietoturvan yhteydessä soveltaneissa tutkimuksissa täysin vastaavaa vertailua ei ole tehty, on muissa aikaisemmissa tutkimuksissa viitattu joihinkin samoihin huomioihin, eli tietoturvaohjeiden ja työtehtävien väliseen ristiriitaisuuteen sekä vaikeuteen ymmärtää tietoturvaohjeita. Muun muassa Puhakainen ja Siponen (2010) käsittelevät tätä aihetta. Aiemmissa neutralisoimisteoriaa tietoturvan yhteydessä soveltaneissa tutkimuksissa Siponen ja Vance (2010), Willison ym., (2016) ja Bauer ja Bernroider (2017) ovat huomioineet sosiaalisen kontrollin, sosiaalisen järjestyksen, sosiaaliset säännöt tai sosiaalisen normin, mutta tutkimuksissa tietoturvarikkomus rinnastetaan ikään kuin itsestäänselvänä sosiaalisen normin rikkomisena, eli poikkeavuutena. Tässä tutkimuksessa vain epäilyttävien sähköpostiviestien avaamisen välttämisen voi rinnastaa sosiaaliseen normiin, koska haastatteluiden perusteella asia oli sisäistetty niin hyvin, että se ohjasi toimintaa. Yhtenä selityksenä tälle tutkimustuloksen eroavaisuudelle voi olla se, että tässä tutkimuksessa tutkimusmenetelmä erosi aiemmista tutkimuksista, jolloin tutkimuksen otanta oli pienempi. Toisaalta selitys voi liittyä myös Bauerin ja Bernroiderin (2017) päätelmään, jonka mukaan yksilön henkilökohtaiset moraaliarvot ja –normit ovat olennaisen tärkeitä tietoturvakäyttäytymisessä ja neutralisoimistekniikoiden hyödyntämisellä puolestaan on heikko yhteys tietoturvakäyttäytymiseen. Tämän tutkimuksen tutkimustehtävänä eivät olleet henkilökohtaiset arvot ja normit, joten tässä tutkimuksessa haastateltavien henkilökohtaisia arvoja ja normeja sivuttiin vain yhdessä kohdassa, vetoaminen korkeampiin lojaliteetteihin –neutralisoimistekniikan yhteydessä. Siitä syystä haastatteluiden perusteella ei voida tehdä johtopäätöksiä niiden vaikutuksesta tietoturvakäyttäytymiseen. Aiheena tietoturvan rinnastus sosiaaliseen normiin edellyttäisi kuitenkin lisätutkimusta, jotta tietoturvan merkityksestä yksilön toimintatapoihin saataisiin lisätietoa.

7.1.2 Neutralisaatiotekniikat

Vastuun kieltäminen (engl. *denial of responsibility*). Jos teoriaa verrataan siihen, kuinka haastateltavat perustelevat itselleen sitä, etteivät vaihda salasanoja säännöllisesti, jos järjestelmä ei pakota, tai eivät valitse riittävän vahvaa salasanaa, jos sitä ei ehdottomasti vaadita, ei haastatteluiden perusteella voi suoraan päätellä uhriutumista, tai avuttomana tilanteesta toiseen ajautumista. Enemmän kyse on ihmisen muistijärjestelmän rajallisuudesta. Aikaisemmissa neutralisaa-

tioteoriaa tietoturvakontekstissa soveltaneissa tutkimuksissa tämän tutkimustehtävän aihetta ei ole käsitelty, mutta havainto on sopusoinnussa muiden aikaisempien tutkimusten kanssa. Muun muassa Brown ym., (2004) kirjoittavat, että ongelma on hyvin tiedossa ja ongelmaan on pyritty tekniikan avulla löytämään uusia mahdollisuuksia, mutta vie kuitenkin luultavasti vielä vuosia ennen kuin tekniikka on täysin syrjäyttänyt salasanojen käytön. Myös Woods (2016) tuo väitöskirjassaan esille salasanojen muistamiseen liittyvän ongelman sekä siihen liittyvän turvallisuusriskin.

Vahingon kieltäminen (engl. *denial of injury*). Haastatteluiden perusteella organisaatiokulttuuri näyttäisi vaikuttavan vahingon kieltämiseen, eli haastatteluiden perusteella tietoturvarikkomuksia ei ole mitään syytä kieltää tai salailla, eikä siten kiistää aiheuttamaansa vahinkoa. Toisaalta haastatteluiden perusteella oli havaittavissa, että salasanojen vaihtamattomuuden liittyy ristiriita. Haastatteluiden perusteella vahvaan salasanaan liittyvää ohjeistusta noudatettiin, mutta vahvan salasanan käyttö aiheutti sen, ettei salasanaa vaihdettu. Kun haastateltava oli siis oppinut muistamaan vahvan salasanan, siitä ei haluttu luopua. Kuten edellisen vastuun kieltäminen -neutralisaatiotekniikan yhteydessä mainitaan, salasanojen vaihtamattomuus näyttäisi liittyvän ihmisen muistijärjestelmän rajallisuuteen. Vaikka haastateltavat eivät esimerkiksi perustelleet salasanojen vaihtamattomuutta sillä, ettei siitä seuraa harmia tai se ei aiheudu mitään vahinkoa, asian merkityksettömyyden voi tulkita joko ymmärtämättömyytenä tai välinpitämättömyytenä. Näitä tulkintoja käsiteltiin jo aiemmin sosiaalisen normin yhteydessä. Vahingon kieltäminen –neutralisaatiotekniikkaa ei siis välttämättä liity salasanojen vaihtamattomuuteen. Vaikka kaikissa, luvussa neljä esitellyissä, aikaisemmissa tutkimuksissa vahingon kieltäminen –neutralisaatiotekniikka on huomiotu, toteavat muun muassa Bansal ja Shin (2016) sekä Barlow ym., (2013) tutkimustulostensa perusteella, että neutralisoimistekniikan merkitys vaihtelee riippuen siitä, millainen tietoturvarikkomus on kyseessä.

Uhrin kieltäminen (engl. *denial of victim*). Haastatteluiden perusteella uhrin kieltäminen ei olisi enää luokiteltavissa tietoturvarikkomukseksi, vaan se kategorioitiin rikollisuudeksi. Haastatteluissa tällaista rikosta ei tullut esille, mutta tietoturvarikkomuksen tulkitseminen rikollisena toimintana eroaa havaintona aiemmista tutkimuksista. Willison ym., (2016) tutkimuksen mukaan uhrin kieltäminen liittyi prosessuaaliseen epäoikeudenmukaisuuteen ja tietoturvarikkomus aikeisiin. Cheng ym., (2014) ja Li ym., (2013) tutkimustuloksissa tutkijoiden mukaan uhrin kieltäminen –neutralisoimistekniikka yhdessä muiden neutralisaatiotekniikoiden kanssa ennustaa työntekijän työhön liittymättömän internetin käytön aikomusta. Mahdollinen selitys havaintojen eroavaisuudelle voi olla se, että haastatteluiden perusteella nimenomaan organisaatiota kohtaan suunnattu kosto koettiin rikolliseksi. Bennett ja Robinson (2000) esittävät, että organisaatiokäyttäytymisessä, organisatorisiin normeihin liittyvissä poikkeavuuksissa on eroja riippuen siitä, suuntautuuko poikkeava käyttäytyminen itse organisaatiooon vai organisaation jäseneen. Toinen selitys voi olla se, että tutkimustehtävän rajauksessa uhrin kieltäminen olisi ollut hankala

suunnata yksittäiseen organisaation jäseneen. Lisäksi haastateltavien ilmaukset voivat kertoa myös organisaatiokulttuurin perusoletuksista. Koska aikaisemmissa neutralisaatioteoriaa tietoturvakontekstissa soveltaneissa tutkimuksissa aihetta on käsitelty vähän, aihe edellyttäisi lisätutkimusta muun muassa siihen, vaikuttaako poikkeavan käyttäytymisen suuntaus (organisaatio vai organisaation jäsen) uhrin kieltämisen –neutralisoimisteknikkaan.

Tuomitsijoiden tuomitseminen (engl. *condemnation of the condemners*). Jos teoriaa verrataan haastateltavien kertomiin näkemyksiin, kokemuksiin ja asenteisiin tietoturvapolitiikkaa ja sen noudattamisohjeita kohtaan, eivät haastateltavat suoranaisesti kyseenalaistaneet niitä, vaikkakin joitakin ristiriitaisuuksia haastatteluissa tuli esiin. Haastateltavat kertoivat tuntevansa tietoturvaohjeet, ja ohjeetkin olivat, niiden löydyttyä, haastateltavien mielestä ainakin osittain selkeitä, mutta ehkä tietoturvaohjeita ei täysin oltu sisäistetty, koska keskusteltaessa ohjeiden sisällöstä, ilmeni ristiriitaisuuksia, kuinka ohjeiden mukaisesti pitäisi toimia. Koska kohdeorganisaatiossa on erilaisia tietojärjestelmien käyttöympäristöjä sekä taidoiltaan erilaisia käyttäjiä, käyttöympäristöihin suhtautumisessa oli havaittavissa eroja. Haastatteluiden perusteella tietoturvapolitiikan ja sen noudattamisohjeiden ei koettu olevan epäoikeudenmukaisia, vaan enemmänkin liian laajoja, jotta niistä löytyisi nopeasti apua eri tilanteisiin. Haastatteluissa tuli esille myös Bauerin ja Bernroiderin (2017) tutkimuksessa esille nostama aihe, eli tietoturvatietoisuuden parantaminen edellyttää erilaisia ulkoisia ja sisäisiä viestintäkanavia. Vaikka muun muassa Cheng ym., (2014) ja Li ym., (2013) tulivat tutkimustuloksissaan siihen johtopäätökseen, että neutralisoimistekniikat ovat merkittävästi yhteydessä tietoturvarikkomus aikeisiin, tämän tutkimuksen tutkimustuloksen perusteella voi päätellä, että myönteisestä asenteesta huolimatta, nykypäivän työelämän realiteetti on, että tietoturvaohje joutuu kilpailemaan yhdessä kaikkien muiden ohjeiden kanssa työntekijän ajasta, jolloin tietoturvaohjeen sisäistämiseen ei välttämättä jää aikaa yhtään sen enempää kuin muidenkaan ohjeiden.

Vetominen korkeampiin lojaliteetteihin (engl. *appeal to higher loyalties*). Tämän neutralisoimistekniikan monitulkintaisuuden vuoksi, haastatteluista pyritään päättelemään, millainen sosiaalinen side, henkilökohtainen arvo tai periaate koettaisiin niin sanotusti korkeammalle sijalle kuin tietoturvapolitiikan mukaisten ohjeiden noudattaminen. Päätelmässä tarkastellaan ensin, mitä tarkoittaisi, jos lojaliteetti kohdistuisi henkilöön, kuten vaikkapa esimieheen. Teko oikeutettaisiin silloin esimerkiksi halulla suojella esimiestä mahdollisilta vaikeuksilta, mikäli jokin tehtävä jäisi suorittamatta, jolloin henkilö perustelisi, ettei tehnyt tietoturvarikkomusta itsensä vuoksi. Edellä mainitun kaltainen suojelu saattaisi edellyttää jo alaisen ja esimiehen välillä emotionaalisesti ystävyyssuhteeseen tai intiimiin suhteeseen rinnastettavaa suhdetta. Haastatteluiden perusteella edellä mainitun kaltaista esimies-alaissuhdetta ei ilmennyt, vaan kunnioitus esimiestä kohtaan näytti perustuvan enemmän organisaatiohierarkiaan, eikä välttämättä esimieheen henkilönä. Myöskään muunlainen sosiaalinen side ei haastatteluiden perusteella asettunut arvoltaan korkeammaksi kuin tietoturvaohjeiden noudattaminen. Haastatteluissa ei myöskään tullut esille syitä,

joita voisi tulkita henkilökohtaisina arvoina. Tietoturvaohjeiden noudattamattomuuteen ei siten liittynyt esimerkiksi vetoamista työmotivaation lisäämiseen tai työssä jaksamiseen. Haastatteluiden perusteella lojaliteetti kohdistui enemmän toiminnan jatkuvuuteen turvaamiseen. Tällöin lojaliteetti kohdistuu itseasiassa organisaatiota kohtaan, joten voidaan kysyä, ketä vastaan silloin oikeastaan rikotaan, jos tietoturvapolitiikkaa rikotaan. Tilanteesta voi tulla johtopäätökseen, että tietoturvapolitiikka ja sen ohjeet eivät ole linjassa todellisten työtehtävien kanssa. Vaikka muun muassa Siponen ja Vance (2010) viittaavat Puhakaisen (2006) tutkimustuloksiin, joita Puhakainen ei liitä neutralisoimisteoriaan, mutta joista Siponen ja Vance päättelevät, että suuresta työmäärästä johtuva kiire, tai töiden priorisointi voidaan nähdä työntekijöiden keinoina hyödyntää neutralisoimistekniikoita, tämän tutkimuksen kohdeorganisaatiossa kiire voi olla todellinen eikä pelkkä selitys, silloin kun kyse on nimenomaan toiminnan jatkuvuuden turvaamisesta. Vetoaminen korkeampiin lojaliteetteihin ei siten välttämättä selitä tietoturvarikkomuksia. Myös aikaisemmissa neutralisoimisteoriana tietoturvakontekstissa soveltaneissa tutkimuksissa muun muassa Nykänen (2011) ja Silic ym., (2017) eivät kyenneet osoittamaan vetominen korkeampiin lojaliteetteihin –neutralisoimistekniikan ja tietoturvarikkomusten välillä merkittävää yhteyttä.

Oppiminen: Jos oppimista vertaa neutralisoimisteorian olettamuksiin tietoturvaohjeiden noudattamattomuudessa, ei haastatteluista tullut esille erityisesti motivaation tai myönteisen asenteen oppimista tietoturvarikkomuksia kohtaan. Kuitenkin oppimiseen liittyen tuotiin esille eräs seikka. Haastatteluiden perusteella omien henkilökohtaisten laitteiden ja organisaation tarjoamisen laitteiden käyttötavoissa on eroavaisuuksia. Vaikka omia laitteita ei käytettäisikään töiden tekemiseen, saattaa vapaa-ajan viihdepainotteinen käyttötapa olla ristiriidassa organisaation tapoihin verrattuna, jolloin vapaa-ajalla opittu toimintatapa saattaa siirtyä myös työympäristöön. Aikaisemmissa neutralisoimisteoriaa tietoturvan yhteydessä soveltaneissa tutkimuksissa sekä Haag ym., että Silic ym., (2017) sivuavat aihetta tarkastellessaan neutralisoinnin roolia niin sanottuihin varjo-it:n käyttäjiin saaden kuitenkin keskenään ristiriitaiset tutkimustulokset. Kumpikaan tutkimuksista ei suoraan keskittynyt siihen, miten vapaa-ajalla opitut tavat vaikuttavat työympäristön toimintatapohin. Aihe vaatisi lisätutkimusta muun muassa siitä, kuinka merkittävä ristiriita eri laitteiden vapaa-ajan käytössä opituilla toimintatavoilla on työympäristön toimintatapoihin.

Syyllisyys ja häpeä: Syyllisyyden ja häpeän tunteet liittyivät haastatteluiden perusteella virheettömyyden vaatimuksessa epäonnistumiseen. Tietoturvan kustannuksella tehty toiminnan jatkuuden turvaaminen sitä vastoin ei haastatteluiden perusteella aiheuttanut syyllisyyden ja häpeän tunteita, kuten ei myöskään esimerkiksi salasanojen vaihtamattomuus. Haastatteluiden perusteella henkilö voi jättää muun muassa salasanansa vaihtamatta ilman, että käy itsensä kanssa minkäänlaista sisäistä keskustelua tai tuntisi toiminnastaan syyllisyyttä tai häpeää. Tätä havaintoa tukee muun muassa Silic ym., (2017) tutkimustuloksen perusteella esittämä väite, ettei häpeä ole merkittässä yhteydessä

tietoturvarikkomuksiin. Haastatteluiden perusteella voi tulla johtopäätöksen, joka tukee myös aikaisemmin esiteltyä havaintoa. Jos yksilö ei koe häpeää eikä syyllisyyttä, ei hänen silloin välttämättä tarvitse suojella itseään itsesyytöksiltä, välttää syyllisyyttä eikä oikeuttaa tekojaan neutralisoimistekniikoiden avulla. Toisaalta se, ettei toiminnan jatkuvuuden turvaamisen kustannuksella tehdyistä tietoturvarikkomuksista koeta syyllisyyttä ja häpeää, voi tarkoittaa, että henkilö kokee toimivansa moraalisesti oikein. Aihe vaatisi kuitenkin lisätutkimusta siitä, onko moraalisesti oikeaksi koetussa teossa kyse yksilön henkilökohtaisista arvoista vai organisaation perusoletusten kautta sisäistetyistä normeista. Kuten jo aiemmin on mainittu, muun muassa Bauer ja Bernroider (2017) viittaavat tutkimustuloksessaan siihen, että henkilökohtaiset arvot voisivat olla yhteydessä tietoturvakäyttäytymiseen. Vaikka tämän tutkimuksen haastatteluissa sivuttiinkin organisaatiokulttuuria, ei haastatteluiden perusteella voi tehdä kovin syvällisiä johtopäätöksiä, millaisia alitajuisia, näkymättömiä ja itsestäänselvyyksiksi muodostuneita perusoletuksia kohdeorganisaatio pitää sisällään.

Poikkeavan käyttäytymisen mahdollistaja: Haastatteluiden perusteella tietoturvarikkomus on täysin mahdollinen ilman, että henkilö hyödyntää neutralisoimistekniikoita. Se, että mahdollistaminen tarkoittaisi jatkuvaa toimintaa, ei haastatteluiden perusteella tullut kohdeorganisaatiossa esille. Myös muun muassa Silic ym., (2017) tutkimustuloksessa alkuperäisen neutralisoimisteorian neutralisoimistekniikoilla ei ollut yhteyttä varjo-it:n käyttämiseen, eli tietoturvarikkomus on mahdollinen ilman neutralisoimistekniikoita.

7.1.3 Merkittävin löydös

Tutkimuksen merkittävin löydös on se, etteivät neutralisoimisteorian keskeiset olettamukset välttämättä pädekään tietoturvallisuuden alueella. Muun muassa tietoturvaohjeiden noudattamista ei välttämättä voida rinnastaa sosiaaliseen normiin. Löydöstä voidaan pitää uutena, koska aikaisemmissa tutkimuksissa ei tiettävästi ole huomioitu kaikkia neutralisoimisteorian keskeisimpiä olettamuksia yhtä kattavasti kuin tässä tutkimuksessa. Vaikka sosiaalinen järjestys ikään kuin edellyttää jonkinlaista selitystä, miksi joku toimii sopimattomasti tai väärin, neutralisoimistekniikat eivät välttämättä selitä tietoturvarikkomuksia. Haastatteluiden perusteella selitykset voisivat viitata, ainakin osittain, Scottin ja Lymanin (1968) esittämiin pahoitteleviin selontekoihin. Se, että henkilö myöntää tehneensä sopimattomasti, mutta kiistää vastuun, näyttäisi haastatteluiden perusteella selittävän tietoturvarikkomuksia enemmän kuin se, että henkilö muun muassa kokisi itsensä uhrina tai kieltäisi aiheuttamansa vahingon tai kokisi tietoturvarikkomuksen laillisena kostona. Tietoturvapolitiikkaa ja sen noudattamisohjeita ei välttämättä haluta kyseenalaistaa tai kiistää niiden mielekkyyttä, vaan tietoturvarikkomus halutaan tehdä ymmärrettäväksi.

7.1.4 Muita löydöksiä

Suonisen (1997) mukaan sosiaalinen status vaikuttaa oikeuttamisen tekniikoihin. Eli hierarkisesti ylempi ei koe edes tarvetta selitellä toimintaansa samoin kuin hierarkisesti alempi. Haastatteluiden perusteella sosiaalinen asema näyttäisi vaikuttavan sekä tietoturvatoimintaan että myös oikeuttamisen tekniikoiden hyödyntämiseen. Haastatteluiden perusteella hierarkisesti korkeampi institutionaalinen rooli yhdistettynä pitkään työsuhteeseen ei välttämättä näyttänyt vaikuttavan myönteisesti suhtautumisessa tietoturvapolitiikaan ja sen noudattamisohjeisiin. Tämä havainto on linjassa Bansal ym., (2016) tutkimuksen kanssa, jonka yhtenä hypoteesina oli, että pitkä vakituinen työsuhde vähentäisi henkilökohtaisten ja organisaation arvojen välistä eroa, jolloin todennäköisyys vilpilliseen toimintaan pienenisi, mutta tutkimus ei tukenut tätä oletusta. Muun muassa Nykäsen (2011, 268) mukaan ilman johdon ja esimiesten aktiivista tietoturvatoimintaa, ei organisaation tietoturvakaan voi kehittyä.

7.2 Käytännön hyödynnettävyys

Tämän tutkimuksen havaintoja voidaan hyödyntää eri organisaatioiden tietoturvatoiminnan kehittämiseen ja tietoturvatietoisuuden parantamiseen. Pelkkä tietoturvapolitiikka ja sen noudattamisohjeet eivät vielä sellaisenaan välttämättä ohjaa työntekijää toimimaan siten, että tietoturva olisi sisäistetty itsestäänselvyytenä tämän päivän tietojenkäsittely-ympäristössä. Seuraavaksi esitellään muutamia suosituksia.

Koska pelkät tekniset ratkaisut eivät yksin voi varmistaa tietoturvaa muun muassa salasanojen muistettavuuteen liittyen, tulisi käyttäjiä ohjata ja opastaa muistettavien salasanojen muodostamisessa. Muun muassa Woods (2016) tuo tutkimustuloksissaan esille, että ainutlaatuiset (uniikit) salasanat ovat muistettavampia kuin kierrätetyt tai muokatut salasanat. Ymmärtämättömyyteen voidaan vaikuttaa muun muassa koulutuksella. Kun tähdätään asioiden ymmärtämiseen, liittyy muun muassa konstruktivistiseen oppimiskäsitykseen näkemys, jonka mukaan oppija on aktiivinen toimija koko oppimisprosessin ajan (Rauste-von Wright, Wright ja Soini 2003, 162–166). Eri ihmiset oppivat eri tavoin, jolloin esimerkiksi luentotyyppinen koulutus tai sähköinen, valmiit vaihtoehdot sisältävä testi ei välttämättä edistä kaikkien oppimista. Kuvaavien esimerkkien kertominen, eli virheellisten toimintatapojen mahdolliset konkreettiset seuraukset, saattaa myös edistää oppimista. Kun ymmärtämättömyys on aitoa, se edellyttää, että asetutaan koulutettavan asemaan, eli kouluttajan olisi pyrittävä ymmärtämään, millainen koulutettavien tieto-taitotaso on ja suhteuttaa koulutus sen mukaisesti. Jotta koulutus välttyisi Scheinin (1991, 54-55) kuvailemalta tietojenkäsittelyn veljeskunnan sanaston käytöltä, tulisi kouluttajan pyrkiä välttämään tarpeetonta erityissanaston käyttöä. Myös ohjeiden laatimisessa tulisi asettua ohjeita käyttävän asemaan ja havainnollistaa ohjetta esi-

merkiksi kuvien avulla ja välttää monitulkintaisia ilmaisuja. Kuten jo johdannossa mainittiin, tietoturvallisuus syntyy sosioteknisessä ympäristössä. Tutkimus havainnollistaa myös sen, kuinka tietojärjestelmien kehittämisessä tulisi pyrkiä huomioimaan tietoturvallisuuden lisäksi myös järjestelmän käytettävyys.

Vaikka tietoturvaa voidaan parantaa monenlaisten teknisten ratkaisujen avulla, valitettavasti tekniikka yksin ei kykene pureutumaan asenteisiin. Asenteiden muutokseen voi kuitenkin vaikuttaa muun muassa ymmärrystä lisäämällä, jolloin aihetta ei enää koeta merkityksettömänä. Tämän tutkimuksen käytännön hyöty tiedeyhteisölle on se, että tutkimus tarjoaa sekä uutta tietoa että lukuisia jatkotutkimusaiheita.

7.3 Luotettavuuden arviointi

Hirsjärven ym., (2004) mukaan, kaikissa tutkimuksissa pyritään arvioimaan toteutetun tutkimuksen luotettavuutta. Vaikka kvalitatiivisissa tutkimuksissa reliaabelius ja validius voidaan tulkita eri tavoin, tulisi tutkimuksen luotettavuutta ja pätevyyttä silti arvioida. (Hirsjärvi ym., 2004, 216-217.) Saaranen-Kauppinen ja Puusniekan (2010) mukaan laadullisen tutkimuksen reliabiliteettia arvioitaessa voidaan tarkastella käytetyn metodin luotettavuutta sekä johdonmukaisuutta, tutkimustuloksen pysyvyyttä sekä tulosten johdonmukaisuutta. Saaranen-Kauppinen ja Puusniekka (2010) tuovat esille myös sen, että luotettavuuden arvioinnissa on otettava huomioon se, että esimerkiksi tutkittava saattaa vastata johonkin haastattelukysymykseen enemmän sen mukaan, kuinka sosiaalisesti hyväksyttävä vastaus on, eikä sen mukaan, kuinka todellinen vastaus on. Myös Alasuutarin (2012, 74) mukaan emme aina voi olla varmoja edes omia tekojamme ohjaavista motiiveista, joten ei ole olemassa metodia, joka takaisi varman pääsyn totuuden luo. Tässä tutkimuksessa anonyymiteettiyden avulla pyrittiin saamaan todellisia vastauksia. Toisaalta myös oheisviestinnän avulla pyrittiin tulkitsemaan haastateltavan kertoman todenmukaisuutta. Tutkimusmenetelmä soveltui tähän tutkimukseen ja saavutti sille asetetun tavoitteen. Mikäli menetelmäksi olisi valittu kvantitatiivinen tutkimusmenetelmä, olisi sillä ikään kuin toistettu aikaisempia tutkimuksia.

Saaranen-Kauppisen ja Puusniekan (2010) mukaan laadullisen tutkimuksen validiteetti tarkoittaa tutkimuksen uskottavuutta, eli sitä kuinka hyvin tutkija pystyy vakuuttamaan lukijan tutkimuksen rakentumisesta, omasta ajatusprosessistaan sekä ajatusten myötä tulleesta tutkimustuloksesta. Totuus kuitenkin on, että mikään tutkimus ei tuo täydellistä ymmärrystä. (Saaranen-Kauppinen ja Puusniekka, 2010.) Hirsjärven ym., (2004) mukaan laadullisen tutkimuksen luotettavuutta voi lisätä kertomalla tarkasti tutkimuksen toteutukseen liittyvät olosuhteet, kuten paikat ja haastatteluihin käytetty aika. Tässä tutkimuksessa tutkimuksen toteutus on kerrottu niin tarkasti, kuin se kohdeorganisaation toiveita kunnioittaen on ollut mahdollista. Hirsjärvi ja Hurme (2001, 18) mainitsevat totuuden, että tutkijan subjektiiviset näkemykset vaikuttavat koko tutkimusprosessissa. Tässäkään tutkimuksessa ei ole voitu irrottautua tut-

kijan subjektiivisista näkemyksistä. Teorian tutustumiseen käytettiin runsaasti aikaa ja aihepiirinä tietoturvarikkomukset olivat tutkijalle entuudestaan tuttu. Aihepiirin tuntemus auttoi haastatteluteemojen valinnassa.

7.4 Tutkimuksen rajoitteet

Kuten jokaiseen tutkimukseen, myös tähän tutkimukseen liittyy rajoitteita. Vaikka muun muassa Maruna ja Copes (2005) mainitsevat, että neutralisaatiotekniikoiden hyödynnettävyyttä on hankala todistaa ilman pitkittäistutkimusta, ei tälle tutkimukselle varattu aika mahdollistanut pitkittäistutkimusta. Pitkittäistutkimus olisi siten voinut antaa tälle tutkimukselle erilaisen tutkimustuloksen. Toinen rajoite on se, että tutkimus rajattiin yhteen kohdeorganisaatioon. Kolmantena rajoitteena voidaan mainita myös sen, että tutkimus keskittyi vain alkuperäisen neutralisoimisteorian mukaisiin neutralisoimistekniikoihin, joten on mahdollista, että jokin tai jotkin muut neutralisoimistekniikat voivat selittää enemmän tai syvällisemmin tietoturvarikkomusten mekanismia.

7.5 Jatkotutkimusaiheet

Vaikka tietoturva aiheena tarjoaa lukuisia jatkotutkimusaiheita, esitellään seuraavaksi muutamia tämän tutkimuksen myötä esille tulleita aiheita. Jotta saataisiin lisätietoa tietoturvan merkityksestä yksilön elämään, niin työ- kuin vapaa-aikana, olisi tärkeä tutkia tietoturvan rinnastusta sosiaaliseen normiin enemmän ja monipuolisemmin. Voisiko tietoturvassa olla kyse esimerkiksi siitä, ettei tietoturva ole saavuttanut normin asemaa, koska tietoturvaohjeet saattaa laatia yksittäinen henkilö, vaikka muun muassa Ewaldin (2003) mukaan normia ei julisteta eikä ryhmän ulkopuolinen voi siitä päättää? Siinä merkityksessä, jonka Ewald normista antaa, tietoturva ei välttämättä ole vielä saavuttanut normin varsinaista merkitystä, eli kukaan yksittäinen ihminen ei voi laatia lakiin rinnastettavaa ohjetta, jota jokainen ryhmän tai yhteisön jäsen olisi valmis noudattamaan. Aiheesta voisi tarkastella muun muassa, vaikuttaako organisaatiokulttuuri siihen, että tietoturvasta tulisi sosiaalisen normin kaltainen kirjoittamaton sääntö vai vaikuttaako henkilökohtaiset arvot siihen, että tietoturvan voisi rinnastaa sosiaaliseksi normiksi. Koska yksilön henkilökohtaiset arvot kulkevat mukana myös työelämässä, voisi jatkotutkimusaiheena tutkia myös henkilökohtaisten arvojen merkitystä ja vaikutusta tietoturvakäyttäytymiseen.

Kuten aiemmin jo esiteltiin, voisi yhtenä tutkimusaiheena olla se, vaikuttaako poikkeavan käyttäytymisen suuntaus (organisaatio vai organisaation jäsen) uhrin kieltämisen –neutralisoimisteknikkaan. Jos siis tietoturvarikkomus tehdään halusta kostaa tai rangaista, millaisia erot ovat, kun tietoturvarikkomus suunnataan organisaatiota kohtaan tai kun se suunnataan organisaation jäsentä kohtaan.

8 YHTEENVETO

Tietoturvaa uhkaavat haavoittuvuudet syntyvät sosioteknisessä ympäristössä, jolloin ihminen voi omalla toiminnallaan kumota teknologian mahdollistamat tietoturvaratkaisut. Usein sanotaankin, että ihminen on tietoturvan heikoin lenkki. Organisaatioympäristössä työntekijöiden asenteet ja toimet vaikuttavat tietoturvallisuuteen. Työntekijöiden tietoturvapolitiikan mukaisten ohjeiden noudattamattomuus muodostaa organisaation toiminnalle merkittävän tietoturvauhkan. Arviolta puolet tietoturvarikkomuksista tai –loukkauksista tapahtuu työntekijöiden toimesta joko tahallisesti tai tahattomasti. Tutkimalla, miten työntekijät selittävät tietoturvarikkomuksiaan, voidaan tietoturvaohjeiden noudattamattomuuteen löytää selittäviä tai ennustavia syitä. Aikaisemmissa tutkimuksissa tietoturvarikkomusten aikomuksia ja tietoturvarikkomuksia on selitetty muun muassa neutralisoimisteorian avulla. Neutralisoimisteorian mukaan yksilö puolustelee tai selittelee normeista poikkeavaa käyttäytymistä erilaisten neutralisoimistekniikoiden avulla.

Tässä tutkimuksessa teemahaastatteluiden avulla kerättyä aineistoa verrattiin neutralisoimisteorian oletuksiin ja tekniikoihin. Tutkimuksen merkittävin löydös on se, etteivät neutralisoimisteorian keskeiset olettamukset välttämättä pädekään tietoturvallisuuden alueella. Vaikka sosiaalinen järjestys ikään kuin edellyttää jonkinlaista selitystä, miksi joku toimii sopimattomasti tai väärin, neutralisoimistekniikat eivät välttämättä selitä tietoturvarikkomuksia. Tutkimus havainnollistaa muun muassa sen, etteivät tietoturva ja sen noudattamisohjeet ole välttämättä saavuttaneet sosiaalisen normin asemaa.

Tekniikka ei yksin voi pureutua asenteisiin, joiden kautta työntekijä ymmärtäisi ja omaksuisi roolinsa organisaation tietoturvallisuuden yhtenä tärkeänä ja merkittävänä osatekijänä. Teknologian innovaatioiden vastaanotto- ja omaksumiskyky saattaa vaihdella eri ihmisillä, jolloin asenteiden muutokseen voidaan vaikuttaa muun muassa ymmärrystä lisäämällä.

LÄHTEET

Aaltola, J. & Valli, R. (2001). *Ikkunoita tutkimusmetodeihin –näkökulmia aloittelevalle tutkijalle tutkimuksen teoreettisiin lähtökohtiin ja analyysimenetelmiin*. Jyväskylä: PS-kustannus.

Alasuutari, P. (2012). *Laadullinen tutkimus 2.0*. Tampere: Vastapaino. E-kirja.

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

Bansal, G., Hodorff, K., & Marshall, K. (2016). Moral Beliefs and Organizational Information Security Policy Compliance: The Role of Gender. *Proceedings of the Eleventh Midwest United States Association for Information Systems, 1-6.*

Bansal, G., & Shin, S. I. (2016). Interaction Effect of Gender and Neutralization Techniques on Information Security Policy Compliance: An Ethical Perspective. (*Twenty-second Americas Conference on Information Systems, San Diego, 2016)*

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.

Bauer, S., & Bernroider, E. W. (2017). From Information Security Awareness to Reasoned Compliant Action: Analyzing Information Security Policy Compliance in a Large Banking Organization. Data Base for Advances in Information Systems (2017), forthcoming.

Bennett, R. J., & Robinson, S. L. (2000). Development of a measure of workplace deviance. *Journal of applied psychology*, *85*(3), 349.

Black, D. (1983). Crime as social control. *American sociological review*, 34-45.

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

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., and Boss, R. W. (2009). "If Someone Is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security," *European Journal of Information Systems* (18:2), pp. 151-164.

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.

Brown, A. S., Bracken, E., Zoccoli, S., & Douglas, K. (2004). Generating and remembering passwords. *Applied Cognitive Psychology*, 18(6), 641-651.

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: 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.

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.

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.

D'arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems*, 20(6), 643-658.

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

Da Viega, A. & Eloff, J.H.P. (2010), "A framework and assessment instrument for information security culture", *Computer & Security*, Vol. 29 No. 2, pp. 196-207.

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 (pp. 49-61). Springer International Publishing.

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

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

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

Eskola, J., & Suoranta, J. (2008). *Johdatus laadulliseen tutkimukseen.* 8. painos. Tampere: Vastapaino.

Franzese, R. J. (2015). *The Sociology of Deviance : Differences, Tradition, and Stigma*. Springfield : Charles C Thomas. 2015. E-kirja.

Garza, V., & Guo, X. (2015). Securing BYOD: A Study of Framing and Neutralization Effects on Mobile Device Security Policy Compliance.

Gouglidis, A., Green, B., Busby, J., Rouncefield, M., Hutchison, D., & Schauer, S. (2016). Threat awareness for critical infrastructures resilience. In Resilient Networks Design and Modeling (RNDM), 2016 8th International Workshop on (pp. 196-202). IEEE.

Gruber, V., & Schlegelmilch, B. B. (2014). How techniques of neutralization legitimize norm-and attitude-inconsistent consumer behavior. *Journal of business ethics*, 121(1), 29-45.

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.

Hinduja, S. (2007). "Neutralization Theory and Online Software Piracy: An Empirical Analysis," *Ethics and Information Technology* (9:3), pp. 187-204.

Hirsjärvi, S., & Hurme, H. (2001). *Tutkimushaastattelu*. *Teemahaastattelun teoria ja käytäntö.* Helsinki: Yliopistopaino.

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2004). *Tutki ja kirjoita* (10. osin uud. painos). Helsinki: Tammi.

Hu, Q., West, R., & Smarandescu, L. (2015). The role of self-control in information security violations: insights from a cognitive neuroscience perspective. *Journal of Management Information Systems*, 31(4), 6-48.

Höne, K., & Eloff, J. H. P. (2002). Information security policy—what do international information security standards say?. *Computers & Security*, 21(5), 402-409.

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.

Ingram, J.R. and Hinduja, S. (2008). Neutralizing music piracy: An empirical examination. *Deviant Behavior*, 29 (4), 334-366.

Innes, M. (2003). *Understanding Social Control : Deviance, Crime and Social Order.* Open University Press. E-kirja.

Jauho, M. (2003). Normaalin genealogiaa. *Tiede & edistys* 28 (2003): 1.

Johnston, M. S., & Kilty, J. M. (2016). "It's for their own good": Techniques of neutralization and security guard violence against psychiatric patients. *Punishment & Society*, 18(2), 177-197.

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.

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.

Kielitoimiston sanakirja. (2017). Rikkomus. Helsinki: Kotimaisten kielten keskus. Haettu 7.5.2017 osoitteesta http://www.kielitoimistonsanakirja.fi/netmot.exe?ListWord=rikkomus&SearchWord=rikkomus&dic=1&page=results&UI=fi80&Opt=1.

Kielitoimiston sanakirja. (2017). Uhka. Helsinki: Kotimaisten kielten keskus. Haettu 7.5.2017 osoitteesta http://www.kielitoimistonsanakirja.fi/netmot.exe?ListWord=uhka&SearchWord=uhka&dic=1&page=results&UI=fi80&Opt=1.

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.

Kivivuori, J. (2008). *Rikollisuuden syyt*. Helsinki: Kustannusosakeyhtiö Nemo.

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.

Li, W., & Cheng, L. (2013). Effects of Neutralization Techniques and Rational Choice Theory on Internet Abuse in the Workplace. In PACIS (p. 169).

Lowry, P. B., Zhang, J., Wang, C., & Siponen, M. (2016). Why do adults engage in cyberbullying on social media? An integration of online disinhibition and deindividuation effects with the social structure and social learning model. *Information Systems Research*, 27(4), 962-986.

Maruna, S., & Copes, H. (2005). What have we learned from five decades of neutralization research?. *Crime and justice*, 221-320.

Metsämuuronen, J. (2011). *Tutkimuksen tekemisen perusteet ihmistieteissä 2*. Opiskelijalaitos. International Methelp Oy.

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and organization*, 17(1), 2-26.

Nicho, M., & Kamoun, F. (2014). Multiple case study approach to identify aggravating variables of insider threats in information systems. *Association for Information Systems*.

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

Peltier, T. (2014). *Information Security Fundamentals.* Second Edition. CRC Press. E-kirja.

Piacentini, M. G., Chatzidakis, A., & Banister, E. N. (2012). Making sense of drinking: the role of techniques of neutralisation and counter-neutralisation in negotiating alcohol consumption. *Sociology of health & illness*, 34(6), 841-857.

Puhakainen, P. (2006). A design theory for information security awareness. Väitöskirja. Oulun Yliopisto. Haettu 6.11.2016 osoitteesta http://herkules.oulu.fi/isbn9514281144/isbn9514281144.pdf.

Puhakainen, P. & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly*, 34(4), 757-778.

Raggad, B. G. (2010). Information security management. New York : CRC Press.

Rauste - von Wright L., von Wright J. & Soini T. (2003). *Oppiminen ja koulutus*. Helsinki: WSOY.

Riekkinen, J. (2016). Dissonance and Neutralization of Subscription Streaming Era Digital Music Piracy: An Initial Exploration. In PACIS 2016: Proceedings of the 20th Pacific Asia Conference on Information Systems, ISBN 9789860491029. Association for Information Systems.

Saaranen-Kauppinen, A., & Puusniekka, A. (2006). KvaliMOTV - Menetelmäopetuksen tietovaranto. Tampere: Yhteiskuntatieteellinen tietoarkisto. Haettu 17.4.2017 osoitteesta http://www.fsd.uta.fi/menetelmaopetus/

Salmivalli, C., & Voeten, M. (2004). Connections between attitudes, group norms, and behaviour in bullying situations. *International Journal of Behavioral Development, 28*(3), 246-258.

Schein, E.H. (1991). *Organisaatiokulttuuri ja johtaminen*. 3. painos. Helsinki: Weilin+Göös. Ekonomia-sarja.

Scott, M.B. & Lyman, S. M. (1968). Accounts. *American sociological review*, 46-62.

Silfver-Kuhalampi, M., & Helkama, K. (2012). Syyllisyys, häpeä ja arvot erilaisissa kulttuureissa. *Psykologia* 47 (05-06), 2012.

Silic, M., Barlow, J. B., & Back, A. (2017). A new perspective on neutralization and deterrence: Predicting shadow IT usage. *Information & management*.

Siponen, M. (2006). Information security standards focus on the existence of process, not its content. *Communications of the ACM*, *49*(8), 97-100.

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., Vance, A., & Willison, R. (2012). New insights into the problem of software piracy: The effects of neutralization, shame, and moral beliefs. *Information & Management*, 49(7), 334-341.

Siponen, M., Willison, R., & Baskerville, R. (2008). Power and practice in information systems security research. *ICIS 2008 Proceedings*, 26.

Sommestad, T., Hallberg, J., Lundholm, K., and Bengtsson, J. (2014). "Variables influencing information security policy compliance," *Information Management & Computer Security* (22:1), pp 42-75.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security*, 24(2), 124-133

Suoninen, E. (1997). Selonteot ja oman toiminnan ymmärrettäväksi tekeminen. *Sosiologia* : Westermarck-seuran julkaisu 34 (1997) : 1, 3. artikkeli.

Sutherland, E. H. (1955). Principles of Criminology, revised by D. R. Cressey, Chicago: Lippincott, pp. 77-80.

Sykes, G. & Matza, D. 1957. Techniques of Neutralization: A Theory of Delinquency. *American Sociological Review*, 22 (6), 664–670.

Tieteen termipankki. (2015). Oikeustiede:normi. Haettu 12.1.2017 osoitteesta: http://www.tieteentermipankki.fi/wiki/Oikeustiede:normi.

Tieteen termipankki. (2015). Filosofia:normi. Haettu 19.2.2017: osoitteesta http://www.tieteentermipankki.fi/wiki/Filosofia:normi.

Tieteen termipankki. (2015). Oikeustiede:poikkeava käyttäytyminen. Haettu 17.2.2017 osoitteesta: http://www.tieteentermipankki.fi/wiki/Oikeustiede:poikkeava käyttäytyminen.

Tietotekniikan termitalkoot. (2016). Sanastokeskus TRK ry. Haettu 3.5.2017 osoitteesta http://www.tsk.fi/tsk/termitalkoot/fi/node/266, Haavoittuvuus.

Tietotekniikan termitalkoot. (2015). Sanastokeskus TRK ry. Haettu 3.5.2017 osoitteesta http://www.tsk.fi/tsk/termitalkoot/fi/node/266, Tietoturva; tietoturvallisuus.

Topalli, V. (2005). When being good is bad: An expansion of neutralization theory. *Criminology*, 43(3), 797-836.

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. (2006). *Laadullinen tutkimus ja sisällönanalyysi*. Helsinki; Tammi.

Vacca, J. (2014). *Managing information security*. Waltham, MA : Syngress 2014. E-kirja.

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, *29*(4), 476-486.

Watkins, S. (2013). *An Introduction to Information Security and ISO27001* : 2013. Ely: IT Governance Publishing. E-kirja.

Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security*. Fourth edition. Cengage Learning. E-kirja.

Willison, R. & Warkentin, M. (2013). Beyond deterrence: an expanded view of employee computer abuse. *MIS Quarterly* Vol. 37 No. 1, pp. 1-20.

Willison, R., Warkentin, M., & Johnston, A. C. (2016). Examining employee computer abuse intentions: insights from justice, deterrence and neutralization perspectives. *Information Systems Journal*.

Woods, N. (2016). Improving the security of multiple passwords through a greater understanding of the human memory. Väitöskirja. Jyväskylä: Jyväskylän yliopisto, informaatioteknologian tiedekunta. Haettu 30.4.2017 osoitteesta https://jyx.jyu.fi/dspace/bitstream/handle/123456789/51882/978-951-39-6846-5_vaitos26112016.pdf?sequence=1.

Zhang, S., Yu, L., Wakefield, R. L., & Leidner, D. E. (2016). Friend or Foe: Cyberbullying in Social Network Sites. ACM SIGMIS Database, 47(1), 51-71.