# TIETOTURVAKULTTUURIN RAKENTUMINEN FINAVIAN VIESTINNÄSSÄ

Teemu Seppänen

Viestinnän maisterintutkielma

Kevät 2021

Kieli- ja viestintätieteiden laitos

Jyväskylän yliopisto

# JYVÄSKYLÄN YLIOPISTO

| | |
|---|---|
| Tiedekunta – Faculty<br>Humanistis-yhteiskuntatieteellinen | Laitos – Department<br>Kieli- ja viestintätieteiden laitos |
| Tekijä – Author<br>Teemu Seppänen | |
| Työn nimi - Title<br><br>Tietoturvakulttuurin rakentuminen Finavian viestinnässä | |
| Oppiaine – Subject<br>Viestintä | Työn laji – Level<br>Maisterintutkielma |
| Aika – Month and year<br>Toukokuu 2021 | Sivumäärä – Number of pages<br>95 |


Tiivistelmä – Abstract

Tutkielman tavoitteena on kuvata ja ymmärtää tietoturvaviestinnän yhteyttä organisaation tietoturvakulttuurin rakentumiseen. Tietoturva on organisaatioille kasvava prioriteetti ja työntekijöiden rooli tietoturvan toteutumisessa on merkittävä. Tutkielmassa ihmiskeskeisen tietoturvan vahvistamiseen etsittiin ratkaisua organisaation viestinnän ja tietoturvakulttuurin rakentumisen lähtökohdista. Tutkielmassa jäsennetty tietoturvaviestinnän käsite kuvaa tietoturvan johtamisviestinnän ja työyhteisön vuorovaikutuksen prosessien kokonaisuutta tietoturvan kontekstissa. Tutkielmaa varten teemahaastateltiin yhdeksää Finavian työntekijää. Aineistolähtöistä sisällönanalyysia hyödyntämällä aineistosta muodostettiin teemat, joiden mukaan tutkimuksen tulokset esiteltiin.

Tulosten mukaan tietoturvakulttuurin rakentumiseen on vahvasti yhteydessä organisaation toimintaympäristö. Finavialla turvallisuus on juurtunut arvo työntekijöiden päivittäisessä työssä, joka heijastuu tietoturvaan liittyviin asenteisiin ja suhtautumiseen sekä kokemukseen vastuusta. Tietoturvaa mahdollisesti heikentävinä tekijöinä mainittiin kiire ja inhimilliset virheet, kuten huolimattomuus tai tietämättömyys. Haastateltavien mukaan tietoturvan toteutumista edistävät tietoturvalliset laitteet ja järjestelmät, tuki ja tietoturvaviestintä.

Tietoturvaviestinnällä on merkittävä yhteys organisaation tietoturvakulttuurin rakentumiseen. Jatkuvaluontoisella tietoturvaviestinnällä voidaan perustella tietoturvan merkitystä toiminnalle, joka auttaa työntekijää tietoturvaan liittyvässä päätöksenteossa. Tietoturvan edistäminen edellyttää organisaatioilta suunniteltua muutoksen johtamista. Osana muutosprosessia työntekijöiden osallisuutta ja vaikuttamismahdollisuuksia tulee vahvistaa. Tietoturvakulttuurin rakentuminen tarvitsee palautetta ja innovaatioita ruohonjuuritasolta, jossa käytännön työtä tehdään.

Kehittämistä tietoturvaviestinnän osa-alueissa Finavialla on erityisesti eri viestintäkanavien roolien selkeyttämisessä, ohjeistusten saatavuudessa ja löydettävyydessä, viestinnän kohdentamisessa ja näkyvyyden lisäämisessä. Työntekijät kokivat, että tietoturvasta voidaan keskustella avoimesti ja matalalla kynnyksellä.

Tämä tutkielma on avaus viestinnän ja tietoturvan tutkimuksen yhdistämiselle. Tutkimus lisää ymmärrystä ihmiskeskeisen tietoturvan vahvistamisesta ja tietoturvakulttuurin rakentumisesta organisaatioissa. Tulokset ovat niin viestinnän- kuin tietoturva-asiantuntijoiden hyödynnettävissä ja tarpeellisen jatkotutkimuksen inspiraationa.



| |
|---|
| Asiasanat – Keywords<br>Tietoturva, tietosuoja, kyberturvallisuus, tietoturvakulttuuri, tietoturvaviestintä, viestintä, vuorovaikutus |
| Säilytyspaikka – Depository<br>Jyväskylän yliopisto / Jyväskylän yliopiston kirjasto |
| Muita tietoja – Additional information |

# SISÄLLYS

# 1 JOHDANTO

Tietoturvasta on tullut yksi organisaatioiden keskeisimmistä prioriteeteista. Syksyllä 2020 tapahtunut psykoterapiakeskus Vastaamon tietomurto näytti mihin heikko tietoturva voi pahimmillaan johtaa. Ylen (Hämäläinen 2021) mukaan arviolta lähes 33 000 ihmisen arkaluontoiset potilastiedot varastettiin tietomurron yhteydessä. Tietoja on jaettu ainakin kahdesti Tor-verkkoon, joka mahdollistaa käyttäjilleen anonyymin verkon käytön. Kyberhyökkäykset tuottavat myös merkittäviä taloudellisia kustannuksia organisaatioille ja vaikuttavat niin liiketoimintaan kuin organisaation maineeseenkin. Hyvä maine tietoturvaosaamisesta onkin nykypäivänä lähes edellytys liiketoiminnassa (Limba ym. 2017, 569). Tietoturvayhtiö McAfeen (Smith, Lostri & Lewis 2020, 3) mukaan kyberrikokset tuottavat globaalissa taloudessa jo yli miljardin dollarin tappioita vuosittain. Taloudellisten tappioiden lisäksi Vastaamon kaltaiset tietomurrot vaikuttavat yksilöiden hyvinvointiin, turvallisuuden tunteeseen sekä luottamukseen yhteiskuntaa ja sen järjestelmiä kohtaan.

Työntekijöiden rooli organisaatioiden tietoturvan toteutumisessa on merkittävä, koska jopa 91 prosenttia kaikista tietoturvauhkista alkaa työntekijöille saapuvien sähköpostien välityksellä (Bureau 2017). Traficom (2019) on listannut Kyberturvallisuuskeskuksen vuosikatsauksessa yleisimmät tietoturvauhkat yksilöille ja organisaatioille. Uhkia ovat esimerkiksi kiristyshaittaohjelmat, huijausviestit ja tietojenkalastelu, joiden tavoitteena on usein taloudellinen hyöty tai

liikesalaisuuksien tiedusteleminen. Työntekijöiden psykologiset ominaisuudet ovat usein kyberrikollisten hyödynnettävissä. Puhutaan inhimillisestä tekijästä, joka vastuussa jopa 95 prosenttisesti kaikista toteutuneista tietoturvauhkista (Gyunka & Christiana 2017). Työntekijöiden heikkoon tietoturvan hallintaan liittyvät usein esimerkiksi huonot ja toistuvat salasanat eri järjestelmissä (ks. Siponen, Puhakainen & Vance 2020). MTV:n (Egutkina 2020) uutisen mukaan Vastaamon tietomurto mahdollistui nimenomaan arvattavissa olevan oletussalasanan vuoksi. Tietoturvan suunnittelussa ja toteuttamisessa tulisi kiinnittää erityistä huomiota omiin työntekijöihin, jotta tietoturvauhkien toteutumisen mahdollisuus voidaan minimoida. (ks. Chmura 2018; Lehto 2019; Moinescu ym. 2019).

Siinä missä työntekijät voidaan nähdä tietoturvauhkana, toimivat he myös tietoturvan mahdollistajina (Forcepoint 2018, 20). Organisaation tietoturva on tiimityötä, joka yhdistää kaikkien työntekijöiden panoksen. Työntekijän rooli on edelleen merkittävä teknologian käytössä ja siihen liittyvässä päätöksenteossa, koska edes parhaat teknologiset järjestelmäratkaisut eivät takaa organisaatioille täyttä turvallisuutta (Abawajy 2012, 238). Hyökkäykset eivät kohdistu vain yksilöihin, joilla on pääsy luottamukselliseen tietoon, vaan jokainen organisaation työntekijä voi olla hyökkäyksen kohteena (Moinescu, Ciprian, Dragoş, Narcis-Florentin & Sergiu 2019). Ei tarvita kuin yksi työntekijä, joka lataa koko organisaation tietoverkon saastuttavan liitetiedoston sähköpostista. Toisaalta yksittäinen työntekijä voi myös torjua tietojenkalastelua, petoksia ja haittaohjelmia sisältäviä sähköposteja (Traficom 2019, 61).

Tutkielman tavoitteena on kuvata ja ymmärtää tietoturvaviestinnän yhteyttä organisaation tietoturvakulttuurin rakentumiseen. Kohdeorganisaationa tässä tutkielmassa toimii lentoasemayhtiö Finavia Oyj. Organisaation tietoturvaa voidaan vahvistaa rakentamalla organisaation laajuista tietoturvakulttuuria. Vroom ja Von Solms (2004) toteavat ideaalin tietoturvakulttuurin keskeisessä asemassa olevan tietoturvallisen toiminnan sulautuminen luonnolliseksi osaksi organisaation prosesseja. Määritelmässä korostuu työntekijöiden vapaaehtoinen ja itseohjautuva

tietoturvallinen toiminta. Viestinnän rooli tietoturvakulttuurin rakentumisessa on määritelty vahvasti osaksi johtamista (ks. esim. D'Arcy & Greene 2014). Viestinnän alle tietoturvan kontekstissa sijoitetaan usein koulutus ja opetus, joiden tavoitteena on kehittää työntekijöiden tietoturvaosaamista, sekä tiedotteet ja kampanjat, joiden tavoitteena on puolestaan lisätä tietoisuutta tietoturvasta sekä tehdä siitä näkyvä osa organisaation toimintaa. Tässä tutkielmassa esittelen uutena käsitteenä *tietoturvaviestinnän*, joka keskittyy kuvaamaan organisaation johtamisviestinnän ja työyhteisön vuorovaikutuksen prosessien yhteyttä tietoturvakulttuurin rakentumiseen.

Valon ja Mikkolan (2020, 3) mukaan työntekijöiden välinen vuorovaikutus ja viestintä ovat organisaation perusta. Organisaation vuorovaikutuksessa luodaan merkityksiä, jaetaan arvoja ja asetetaan yhteisiä tavoitteita. Inhimillisten toimijoiden lisäksi organisaatio muodostuu ja merkityksentyy materiaalisten, ei-inhimillisten toimijoiden välityksellä (ks. esim. Schoeneborn ym. 2014). Viestintä on osa kaikkea organisaation toimintaa, joten myös tietoturvakulttuurin rakentuminen perustuu organisaation viestintään ja vuorovaikutukseen. Tutkielmassa perehdytään *Finavian* työntekijöiden kokemuksiin ja käsityksiin tietoturvasta sekä siihen liittyvästä viestinnästä. Ymmärrystä pyritään lisäämään esimerkiksi siitä, millaista ja miten tietoturvaviestintää tulisi työntekijöille esittää, jotta tietoisuus ja ymmärrys tietoturvasta lisääntyisivät. Haasteena ei välttämättä ole tietoturvapolitiikan luominen, vaan siitä viestiminen tehokkaasti ja selkeästi (Moinescu ym. 2019). Toisaalta pelkkä tietoisuus tietoturvapolitiikasta ei yksittäisenä tekijänä riitä hyvän tietoturvakulttuurin rakentumiseen (Chen, Ramamurthy & Wen 2015).

Tässä tutkielmassa tietoturvakulttuuria ja sen rakentumista organisaatioissa tarkastellaan *ihmiskeskeisesti*. Tämä tarkoittaa pääosin tietoturvan ei-teknologisia tekijöitä, jotka ovat yhteydessä tietoturvan toteutumiseen organisaatioissa, pois lukien viestinnän toteuttamiseen käytettävä teknologia.

# 2 TIETOTURVA ORGANISAATIOISSA

## 2.1 Tietoturvan määrittely

Tietoturvaan sisältyy tietoturvan johtaminen, älylaitteiden, ohjelmistojen- ja datan turvallisuus, ja tietoliikenneturvallisuus. Tietoturvalla ja tietoturvallisuudella voidaan tarkoittaa oloja, joissa tietoturvariskit ovat hallinnassa. (Turvallisuuskomitea 2018, 15; Whitman & Mattord 2012, 8.) Tietoturva käsittää myös ne organisatoriset ja teknologiset järjestelyt, joilla suojataan ja varmistetaan tiedon 1. *luottamuksellisuus* (confidentiality), 2. *eheys* (integrity) ja 3. *saatavuus* (availability) sen varastoinnissa, prosessoinnissa tai lähettämisessä (Tietosuojavaltuutetun toimisto 2020; Whitman & Mattord 2012, 8). Kyberturvallisuuden sanastossa (Turvallisuuskomitea 2018, 15) luottamuksellisuus, eheys ja saatavuus määritellään seuraavasti:
"Luottamuksellisuus tarkoittaa, ettei kukaan sivullinen saa tietoa. Eheys tarkoittaa tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa ja saatavuus sitä, että tieto on hyödynnettävissä haluttuna aikana."

Nämä kolme ominaisuutta muodostavat C.I.A. -mallin, joka on tietoturvan yleinen perusta. Whitmanin ja Mattordin (2012, 8, 12, 15) mukaan malli ei kuitenkaan ole enää nykypäivän jatkuvasti muuttuvassa toimintaympäristössä ajan tasalla ja siihen on voitu lisätä uusia vahvistavia tekijöitä. Myös Raggad (2010, 22 - 23) lisää C.I.A. -malliin kolme muuta tavoitetta, jotka ovat 4. todentaminen (authentication), 5. kiistämättömyys (non-repudiation) ja 6. riskien hallinta (risk management). Todennus varmistaa sen, että vain oikeat ihmiset pääsevät käsiksi tietoon ja kiistämättömyys varmistaa sen, että tiedon lähettäjä ja tiedon saaja eivät voi kiistää saamaansa tai lähettämäänsä tietoa. Riskien hallinnalla tarkoitetaan kaikkien näiden tavoitteiden kokonaisuutta, joilla pyritään tunnistamaan, arvioimaan ja vähentämään riskejä.

Tietoturvan tavoitteena on varmistaa liiketoiminnan jatkuvuus ja minimoida myös mahdollisesti toteutuvien tietoturvauhkien aikaansaamat vahingot (Von Solms 1998).

Tietoturvauhka on mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku, joka kohdistuu tietoturvaan ja toteutuessaan vaarantaa sen (Turvallisuuskomitea 2018, 25). Tietoturva saavutetaan esimerkiksi tietoturvaohjeistusten noudattamisen, organisaation työntekijöiden koulutuksen, osaamisen ja tietoisuuden kehittämisen sekä teknologian avulla (Whitman & Mattord 2012, 8). Tietoturva sisältää niin teknologisen kuin sosiaalisen ulottuvuuden (Karyda, Kiontouzis & Kokolakis 2005, 246). Lehto (2019, 17) sekä Moinescu ja kumppanit (2019) antavat tietoturvan kehittämiselle lähtökohdaksi kyberpolitiikan tai tietoturvapolitiikan, jonka avulla ylin johto määrittelee organisaation tietoturvan tavoitteita, normeja ja hyväksyttäviä toimintatapoja.

Tietoturvasta puhuttaessa usein nousevat esille myös *tietosuojan* ja *kyberturvallisuuden* käsitteet. *Tietosuojalla* tarkoitetaan henkilötietojen käsittelyyn liittyviä toimenpiteitä, joten tietoturva voi täten olla yhtenä osana tietosuojan toteuttamista (Tietosuojavaltuutetun toimisto 2020). *Kyberturvallisuus* perustuu tietoturvallisuuden järjestelyihin eli kybertoimintaympäristössä toimivien tahojen tarkoituksenmukaisiin ja riittäviin tietojärjestelmien ja -verkkojen turvallisuusratkaisuihin (Lehto ym. 2018, 11). Kybertoimintaympäristö on yhdestä tai useammasta digitaalisesta järjestelmästä muodostuva toimintaympäristö. Turvallisuuskomitean (2018, 21, 31) määritelmän mukaan kyberturvallisuus on "tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan." Kyberturvallisuus tarkoittaa siis modernin digitaalisen ja verkottuneen yhteiskunnan turvallisuutta.

Kyberturvallisuus on tietojärjestelmien ja tietoliikenteen turvallisuutta, johon ovat kytköksissä myös *tietoturva* ja *tietosuoja*. Tiedon luottamuksellisuuden, eheyden ja saatavuuden ja tietosuojan varmistaminen ei ole kiinni ainoastaan tietojärjestelmien ja tietoliikenteen turvallisuudesta, vaan esimerkiksi kulkuluvat organisaation tiloissa voivat olla osana tietoturvaa. Van Solms ja Van Niekerk (2013) ovat havainneet, että kyberturvallisuuden ja tietoturvan käsitteitä käytetään usein synonyymeina. Tietoturva keskittyy lähtökohtaisesti vain tiedon turvaamiseen, kun taas kyberturvallisuus puolestaan keskittyy myös fyysisen maailman toimintojen

turvaamiseen. Yle (Heikkilä 2020) uutisoi tapauksesta, jossa kyberhyökkäyksen jumittama tietojärjestelmä saksalaisessa sairaalassa aiheutti naisen kuoleman. Sairaala ei pystynyt ottamaan naista vastaan, koska järjestelmät olivat jumittuneet kiristyshaittaohjelman vuoksi. Matkalla toiseen sairaalaan, oli nainen menehtynyt ambulanssissa. Tämä oli tiettävästi ensimmäinen kerta, kun ihmisen kuolema yhdistetään suoraan kyberhyökkäykseen. Terveydenhuollon lisäksi kyberhyökkäyksiä kohdistuu paljon valtiollisiin toimijoihin ja esimerkiksi kuljetus- ja ilmailualan toimijoihin (ks. Calvin 2018, 73; Van Solms & Niekerk 2013). Lentoasemilla kyberuhkat voivat potentiaalisesti vaarantaa ihmishenkiä, aiheuttaa vahinkoja infrastuktuuriin ja epäsuorasti tuottaa taloudellisia sekä yhteiskunnallisia haittoja (ks. Matta & Cantelli-Forti 2019, 286).

## 2.2 Ihmiskeskeinen tietoturva

### 2.2.1 Tietoturvan inhimillinen ulottuvuus

Finavian yli tuhannella työntekijällä on merkittävä rooli tietoturvan toteutumisessa, koska jopa 80 prosenttia kaikista tietoturvauhkista toteutuu johtuen inhimillistä tekijöistä, kuten huolimattomuudesta tai tietämättömyydestä (ks. Grobler, Gaire & Nepal 2021). Teknologia on suunniteltu ihmisen hallittavaksi. Schultz (2005) on pohtinut työntekijöiden psykologisia ominaisuuksia sekä arvaamattomuutta teknologisten turvallisuusratkaisujen hallinnassa. Yksilöt ovat jossain määrin aina osa joko teknologian suunnittelua, käyttöä, huoltoa tai asentamista. Tämä mahdollistaa työntekijöiden tahattomat tai tahalliset virheet, osaamattomuuden, huolimattomuuden, välinpitämättömyyden, hyväksikäytön tai muun haitallisen toiminnan myös organisaatioiden tietoturvan hallinnassa. Vuoden 2020 Digibarometrissä havaittiin kuluttajien kohdalla piittaamattomuutta omien tietojen käytössä, vaikka osaamisen taso tietoturvalliseen toimintaan olisi yltänyt. On yleisesti tiedossa, että ihmistä pidetään kyberturvallisuudessa heikoimpana lenkkinä (Calvin 2018). Puhutaan siis inhimillisestä tekijästä (human factor), joka on yksi organisaatioiden isoimmista tietoturvahaasteista.

Yksittäinen työntekijä voi olla tietoturvauhka, mutta toisaalta myös tietoturvan mahdollistaja.

Helsingin Sanomien uutisessa (Tiainen 2020) käsitellään tietoturvaväsymystä ja hällväliä-ajattelua. Tietoturvaväsymyksen perusideana on se, että ihmiset eivät esimerkiksi koe jaksavansa lukea yksityisyydensuojan ehtoja verkkosivuilla tai muodostaa vahvoja salasanoja eri palveluihin, koska se koetaan vaivalloiseksi. ”Hällväliä” -ajattelulla voidaan perustella laiskaa käytöstä ajattelemalla, että mitä kukaan minun tiedoillani tekisi. Muun muassa edellä mainitusta syystä ihmiset ajattelevat olevansa turvassa kyberhyökkäyksiltä ja harvalla myöskään on kokemusta toteutuneen hyökkäyksen uhriksi joutumisesta (ks. Grobler ym. 2021, 4). Työntekijät voivat myös kokea tietoturvaohjeistusten noudattamisen usein ylimääräisenä työnä, kuten monimutkaisten salasanojen muistamisena, yksinkertaisten sijaan. Ylimääräiseksi koettu työ voidaan nähdä perusteluksi olla noudattamatta ohjeistuksia (ks. Barlow ym. 2018).

Vaikka organisaatiolla olisi käytössään kaikista edistyksellisimmät suojausjärjestelmät, voivat inhimilliset tekijät mahdollistaa tietoturvauhkien toteutumisen (Grobler, Gaire & Nepal 2021). Toisaalta Groblerin ja kumppaneiden (2021, 13) mukaan inhimilliset tekijät eivät itse asiassa ole isoin haaste, vaan haasteena ihmisten ja järjestelmien välisen yhteyden katkos. Tällä tarkoitetaan sitä, että järjestelmiä ei ole suunniteltu riittävän ihmiskeskeisesti, jolloin inhimillisten virheiden todennäköisyys kasvaa. Tietoturvan tarkastelussa tulisi kiinnittää huomiota sekä teknologiseen että inhimilliseen ulottuvuuteen (Grobler ym. 2021; Karyda, Kiontouzis & Kokolakis 2005, 246). Tässä tutkielmassa inhimillistä tekijää pidetään kuitenkin merkittävänä tietoturvan toteutumiseen vaikuttavana tekijänä ja painotus on ihmiskeskeisyydessä ja inhimillisessä ulottuvuudessa.

### 2.2.2 Organisaation työntekijät tietoturvauhkana

On luonnollista ajatella, että tietoturvauhka tulee organisaation ulkopuolelta. Monet voivat mieltää tietoturvauhkan taitavana ja salaperäisenä hakkerina, joka murtautuu

organisaation tietojärjestelmään kannettavalla tietokoneella, jonka näytössä virtaa numeroita ja dataa. Populaarikulttuuri rakentaa osaltaan näitä mielikuvia, josta hyvänä esimerkkinä on todella suosittu ja arvostettu tv-sarja Mr. Robot. Sarjan päähahmona toimii nuori ja hieman omalaatuinen hakkeri, joka perustaa anarkistisen haktivistiryhmän. Osittain mielikuva taitavista hakkereista pitää paikkansa: Verizonin (2019, 5) selvityksessä 52 prosenttia kaikista tarkastelluista tietomurroista sisälsi hakkerointia ja 69 prosenttia oli ulkopuolisten aikaansaamia.

Uhkia organisaatiolla voi olla ulkoisia (external), sisäisiä (internal) tai kolmas osapuoli (partner). Verizonin (2019, 5) raportin mukaan 34 prosenttia tietomurroista oli osallisena sisäpiiriläinen ja IBM:n selvityksessä vuonna 2017 arvioitiin sisäpiiriläisten tehneen jopa 60 prosenttia kaikista hyökkäyksistä. Sisäpiiriläisiä voivat olla esimerkiksi nykyiset ja entiset työntekijät, liiketoiminta- tai sopimuskumppanit ja konsultit sekä asiakkaat (Lehto ym. 2017, 19). Sisäpiiriläiset ovat merkittävä tietoturvauhka, koska heillä on mahdollisesti pääsy organisaation tietojärjestelmiin ja parempi tietoisuus organisaation turvallisuusmenettelyistä ja -heikkouksista

Kuuluisa esimerkki sisäpiiriläisen toteuttamasta tietomurrosta on Edward Snowdenin tapaus vuodelta 2013 (BBC 2014). Snowden latasi ja vuoti eri lähteiden mukaan satoja tuhansia salaisia tiedostoja Yhdysvaltojen kansalliselta turvallisuusvirastolta työntekijän asemasta. Sisäpiiriläisten tietoturvauhkien toteuttaminen voi olla tahallista, mutta inhimillinen tekijä mahdollistaa myös tahattomien uhkien muodostumisen ja toteutumisen. Erityisen haastavaa sisäpiiriläisten aiheuttamien uhkien valvonnasta voi tehdä vahva luottamus organisaation omiin työntekijöihin ja järjestelmiin. Työntekijät voidaan nähdä tietoturvalle uhkana, mutta ennen kaikkea työntekijät tulisi tunnistaa tietoturvan mahdollistajina.

### 2.2.3 Käyttäjän manipulointi

Organisaation työntekijöiden psykologisia ominaisuuksia ja naiiviutta pyritään käyttämään hyödyksi eri kyberhyökkäysmenetelmissä. Joissain tilanteissa työntekijän

käytös voi poiketa normaalista käytöksestä, joka voi johtaa huonoihin päätöksiin, joita normaalitilanteissa harkittaisiin huolellisemmin. Työntekijöihin voi kohdistua kiristystä tai uhkailua, mutta suurin osa kyberhyökkäyksistä toteutetaan käyttäjää manipuloimalla (social engineering). Käyttäjän manipuloinnin roolina on usein mahdollistaa muiden tietoturvauhkien toteutuminen, kuten haittaohjelmien asentaminen organisaation järjestelmiin.

Työntekijöihin voidaan vaikuttaa manipuloimalla (esim. tunteisiin vetoamalla) tai valehtelemalla (esim. imitointi), jotta työntekijä saadaan suorittamaan jokin vahingollinen teko. (ks. Ghafir ym. 2018; Moinescu ym. 2019.) Turvallisuuskomitea (2018, 19) määrittelee käyttäjän manipuloinnin "toiminnaksi, jonka tavoitteena on hankkia luottamuksellista tietoa tekeytymällä tiedon käyttöön oikeutetuksi ja käyttämällä hyväksi tiedon käyttöön oikeutettuja henkilöitä." Hyökkääjän on saavutettava työntekijän luottamus eri keinoja hyödyntäen. Inhimillisen tekijän hyödyntäminen tietoturvallisuuden heikkoutena mahdollistaa suurimman osan kyberrikoksista, johtuen monesti ihmisten huonosta tietoturvatietoisuudesta ja osaamisesta (Europol 2020, 15–16). Tutkimusten mukaan tietojenkalastelua ja käyttäjän manipulaatiota opitaan tunnistamaan koulutuksen avulla, jolloin tietojenkalastelu jää vain yritykseksi (Traficom 2020, 7).

Kevin Mitnick (2003) on entinen käyttäjien manipuloija. Hän on luonut perustaa käyttäjän manipuloinnin käsitteelle sekä kertoo teoksessaan kyberhyökkääjän näkökulman työntekijöiden huijaamiseen. Hänen mukaansa hyökkääjä valmistautuu aina kohtaamaan vastarintaa ja epäluottamusta, sekä on suunnitellut siirtonsa kuin shakkipelissä. Kun työntekijän luottamus on saavutettu, hyökkääjä saa usein haluamansa tiedon. Luottamuksen saavuttamisessa voi onnistua yhdellä sähköpostilla, tai viikkojen ja jopa kuukausien yhteydenotoilla, jotka askel askeleelta vievät kohti haluttua lopputulosta. Yleisimpiä huijausmetodeja Mitnickin (2003) mukaan ovat esimerkiksi kollegana, auktoriteettina tai virkavaltana esiintyminen sekä sähköpostien kautta lähetettävät vahingolliset sovellukset, linkit ja liitetiedostot. Kesäaikaan yleistyvät *toimitusjohtajahuijaukset* ovat hyvä esimerkki auktoriteettina esiintymisestä: huijari

tekeytyy johtoportaan henkilöksi ja voi pyytää esimerkiksi sähköpostin välityksellä pikaista rahasiirtoa tai luottamuksellista tietoa kesäsijaiselta, joka ei välttämättä vielä tunne organisaation johtoa (Halonen 2020; Traficom 2020).

Moinescu ja kumppanit (2019) listaavat käyttäjän manipuloinnin yleisimmiksi muodoiksi peitetarinan kehittämisen (pretexting) ja tietojenkalastelun (phishing). Peitetarinan kehittämisen lisäksi pyritään esimerkiksi luomaan työntekijälle kiireen tunne, jolloin toiminta voi olla epärationaalista. Käyttäjän manipulointi voi kohdistua tyytymättömiin ja katkeroituneisiin työntekijöihin, jotka eivät esimerkiksi ole saaneet palkankorotusta tai ovat kokeneet saavansa epäoikeudenmukaista kohtelua organisaatiossa. Työntekijä voi siis mahdollisesti katkeroitua ja "pettää" oman organisaationsa, eli vaikuttaa tiedon luottamuksellisuuteen, eheyteen ja saatavuuteen, esimerkiksi taloudellista hyötyä tavoittelemalla. (Moinescu ym. 2019; Virvilis ym. 2014.) On olennaista, että työntekijä viihtyy työssään ja voi hyvin, jotta hän on motivoitunut noudattamaan turvallisuusohjeistuksia.

Kansainväliset tietoturvayhtiöt, kuten Verizon, tuottavat vuosittaisia raportteja tietoturvatapahtumista. Verizonin (2018) raportin mukaan 93 prosenttia kaikista käyttäjän manipulointia hyödyntävistä hyökkäyksistä sisälsi tietojenkalastelua. Tietojenkalastelu on kaikista tehokkain tapa manipuloida käyttäjiä, esimerkiksi luomalla sähköposteihin vahingollisia linkkejä tai liitetiedostoja.

Esimerkkinä tietojen kalastelusta on Hillary Clintonin kampanjapäällikkö John Podestan tapaus vuodelta 2016. Podesta sai sähköpostin "Googlelta", jossa varoitettiin, että hänen tiliään käytettiin ulkomailta ja salasana tulisi vaihtaa mahdollisimman nopeasti. Podesta vaihtoi linkin kautta salasanan väärennetyllä verkkosivulla ja hyökkäävät saivat näin Podestan tunnukset käyttöönsä. (Moinescu ym. 2019.) On sanomattakin selvää, että tällaiset tapaukset vaikuttavat niin organisaation toimintaan kuin hyökkäyksen kohteeksi joutuneen työntekijän henkilökohtaiseen elämään. Vaikka käyttäjän manipuloinnin tekniikat eivät ole uusia, ihmisen toiminta on aina altista vaikutuksille. Teknologia ei vielä nykypäivänä pysty tunnistamaan käyttäjän

manipulointia, joten myös Finavialla työntekijöiden tietoturvaosaamisen ja -tietoisuuden kehittäminen on kriittinen tekijä tietoturvan ylläpitämisessä organisaatioissa.

Tietoturvayhtiö Verizonin (2019) raportissa työntekijöiden haavoittuvuus kuvataan hyvin yhdellä lauseella: Tietokonetta ei voi huijata, mutta ihmistä voi, ja hänen tietokoneelleen voi asentaa haittaohjelman. Raportissa kyberrikolliset kuvataan saalistajina, jotka etsivät inhimillisiä tekijöitä ja teknologisia puutteita sekä haavoittuvuuksia. Raportissa tarkastelluista kaikista tietomurroista 33 prosenttia oli sosiaalisten hyökkäysten aikaansaamia (esim. tietojenkalastelu). Vuosien 2013 ja 2019 vertailussa käyttäjän manipulointi ja muu inhimillisen tekijän hyödyntäminen on ollut selkeässä kasvussa. Hyökkääjien yleisimpänä motiivina toimii taloudellinen hyöty tai liikesalaisuuksien paljastaminen. Inhimillisten tekijöiden ja sosiaalisten hyökkäysten muodostamaa tietoturvauhkaa voidaan hallita organisaation tietoturvakulttuuria vahvistamalla.

# 3 TIETOTURVAKULTTUURI

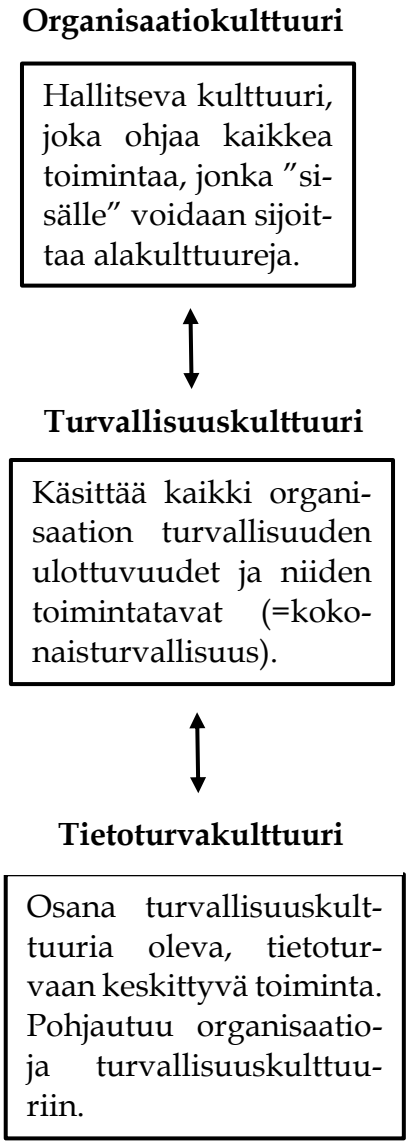
## 3.1 Organisaatiokulttuuri ja turvallisuuskulttuuri

Tietoturvakulttuurin määritelmää on hyvä pohjustaa esittelemällä lyhyesti organisaatiokulttuurin ja turvallisuuskulttuurin käsitteitä. Jokaisella organisaatiolla on omanlaisensa organisaatiokulttuuri. Organisaatiokulttuurin käsitettä esitellään perinteisesti Scheinin (1999, 2017) jäsennyksen mukaan, jossa organisaatiokulttuuri sisältää kolme eri syvyyden tasoa: 1. artefaktit eli organisaation näkyvät tekijät (esim. viestintä, käytetty kieli, viralliset prosessit), 2. julkilausutut arvot (esim. filosofiat, normit, tavoitteet) ja 3. perusoletukset eli käsitykset, uskomukset ja näkemykset organisaation toiminnasta (esim. "itsestäänselvyydet", tehokkaat ja toimivat käytänteet).

Organisaatiokulttuuri on merkitysjärjestelmä, jota rakennetaan ja ylläpidetään työyhteisön viestinnässä ja vuorovaikutuksessa (Reiman, Pietikäinen & Oedewald 2008, 14; Valo & Mikkola 2020, 9). Turvallisuuskulttuuria voidaan pitää organisaatiokulttuurina, joka korostaa turvallisuutta, tai vaihtoehtoisesti yhtenä organisaatiokulttuurin osana (Reiman, Pietikäinen & Oedewald 2008). Voidaan pohtia, että Scheinin (1999, 2017) esittämät organisaatiokulttuurin kolme tasoa ovat kaikki yhteydessä organisaation työntekijöiden tietoturvalliseen toimintaan: esimerkiksi 1. viestintä tietoturvasta, 2. tietoturvaan liittyvät normit ja 3. merkitykset tietoturvasta. Chen, Ramamurthy ja Wen (2015) tarkastelivat tietoturvakulttuurin jäsentymistä myös Scheinin (1999, 2017) jaottelun mukaan ja havaitsivat, että tietoturvakoulutukset- ja tietoisuusohjelmat (SETA-ohjelmat), julkilausut arvot tietoturvasta ja turvallisuuden monitorointi ovat yhteydessä organisaation perusoletuksiin tietoturvasta.

Scheinin jäsennyksen voidaan siis nähdä ulottuvan myös tietoturvakulttuuriin, koska tietoturva toimii yhtenä turvallisuuskulttuurin osa-alueena (ks. YTNK 2005). Tässä tutkielmassa organisaatiokulttuuri todetaan hallitsevaksi kulttuuriksi, jonka yhtenä osa-alueena on turvallisuuskulttuuri. Hallitsevan kulttuurin kontekstissa suurin osa

työntekijöistä jakaa samat arvot, normit ja tottumukset, kun taas alakulttuureissa pienempi ryhmä voi omata esimerkiksi omaan työympäristöön tai maantieteelliseen sijaintiin mukautuneet arvot ja toimintatavat (Da Veiga & Martins 2017, 73). Osana organisaation turvallisuuskulttuuria on puolestaan tietoturvakulttuuri. Kulttuurien tasot on havainnollistettu kuviossa 1. Jokaisella organisaatiolla voidaan ajatella olevan jonkin tasoinen turvallisuuskulttuuri ja tietoturvakulttuuri, mutta ne eivät välttämättä saavuta organisaation (tieto)turvallisuuden näkökulmasta riittävää tasoa, ilman niihin tietoisesti suunnattua toimintaa ja resursseja.




**Kuvio 1 Kulttuurien tasot**

Turvallisuuskulttuurin käsitteen juuret juontavat ydinvoimalaonnettomuuksien (esim. Tšernobylin ydinonnettomuus vuonna 1986) jälkipuinteihin, jossa todettiin huonon turvallisuuskulttuurin mahdollistaneen onnettomuuden toteutumisen (ks. esim. Cooper 2000). Turvallisuuskulttuurin voidaan katsoa alun perin keskittyneen perinteiseen työturvallisuuteen, kuten työtapaturmien ja onnettomuuksien ehkäisyyn. Nykyään organisaatioiden turvallisuus on moniulotteinen ilmiö, johon tietoturvan lisäksi sisältyy esimerkiksi ympäristöturvallisuus, pelastustoiminta ja rikosturvallisuus (YTNK 2005). Finavialla turvallisuuden osa-alueita on yhteensä kuusi, jotka ovat yritysturvallisuus, lentoturvallisuus, siviili-ilmailun turvaaminen, työturvallisuus, kyberturvallisuus ja *tietoturvallisuus* (Finavia 2020). Organisaation turvallisuuskulttuurin rakentumiseen ovat yhteydessä yksilöiden ja ryhmien arvot, asenteet, motivaatio, taidot, ja käyttäytyminen (Reiman, Pietikäinen & Oedewald 2008, 11).

Reimanin ja kumppaneiden (2008) turvallisuuskulttuurin määritelmässä korostuvat turvallisuuden strateginen suunnittelu ja toteutus, organisaation kyky ja tahto ymmärtää turvallisuuskulttuuria ilmiönä sekä kaikki ne toimet, joilla turvallisuutta pyritään edistämään ottamalla huomioon työntekijöiden näkemykset ja organisaation sosiaaliset prosessit. He kuvaavat turvallisuuskulttuurin sisältävän kolme ulottuvuutta, jotka ovat 1. organisatorinen ulottuvuus, 2. psykologinen ulottuvuus ja 3. sosiaalisten prosessien ulottuvuus. Organisatoriseen ulottuvuuteen sisältyy esimerkiksi viestintä, johtaminen, organisaation oppiminen ja osaaminen. Psykologinen ulottuvuus sisältää työn hallittavuuden, turvallisuusmotivaation, systeemisen turvallisuusnäkemyksen, vastuun turvallisuudesta ja vaaratietoisuuden. Sosiaalisia prosesseja ovat muun muassa merkitysten yhteensovittaminen ja identiteettien hallinta. Tässä tutkielmassa sosiaalisista prosesseista puhutaan työyhteisön vuorovaikutuksen prosesseina, koska se on viestinnän tutkimukseen perustuen tarkempi käsite.

Turvallisuuskulttuuri on koko organisaation yhteisen toiminnan lopputulos, joka sisältää monia eri osa-alueita ja ulottuvuuksia. Tässä tutkielmassa organisatorista ulottuvuutta sekä viestinnän ja vuorovaikutuksen prosessien roolia tarkastellaan myös

turvallisuuskulttuurin rakentumisen näkökulmasta, koska tietoturvakulttuuri rakentuu määritelmäni mukaan osana organisaation turvallisuuskulttuuria.

## 3.2 Tietoturvakulttuurin käsite

Tietoturvakulttuurilla ei ole yhtä universaalia määritelmää, joten tämän luvun tavoitteena on antaa yleiskuvaa siitä, mitä kaikkea tietoturvakulttuuri voi pitää sisällään ja millaisia lähtökohtia käsitteellä on. Lähtökohtana organisaation tietoturvakulttuurille voidaan pitää ihmiskeskeisyyttä. Vroom ja Von Solms (2004) määrittelevät ideaalia tietoturvakulttuuria, jossa keskeisessä asemassa on työntekijöiden tietoturvallisen toiminnan ja käytöksen sulautuminen luonnolliseksi osaksi organisaation toimintakulttuuria. Määritelmässä korostuu myös työntekijöiden vapaaehtoinen ja itseohjautuva tietoturvallinen toiminta. Tietoturvakulttuurin tavoitteena on siis vahvistaa ja ylläpitää mahdollisimman hyvää tietoturvan tasoa organisaatiossa sekä vähentää ylhäältä päin tulevaa työntekijöiden kontrollointia ja valvontaa.

Tietoturvan toteutuminen organisaatiossa on koko työyhteisön yhteisen panoksen lopputulos, jota voi hyvin havainnollistaa kyberhygienian (cyber hygiene) käsitteellä. Kuten terveydenhuollossa hyvällä hygienialla pyritään torjumaan bakteereja ja viruksia, torjutaan kybermaailmassa myös viruksia ja sosiaalisia hyökkäyksiä. Finavian työntekijöille tämä voi tarkoittaa esimerkiksi sovellusten päivittämistä ja pätevien salasanojen kehittämistä. Monilla työntekijöillä tuntuu kuitenkin olevan heikko kyberhygienia, mikä mahdollistaa tietoturvauhkien toteutumista (Cain, Edwards & Still 2018, 36). Kyberhygienia kuvaa hyvin sitä lopputulosta, johon tietoturvakulttuurin rakentamisella pyritään: työntekijät noudattavat yhteisiä pelisääntöjä, jotta virukset eivät pääse tarttumaan tai leviämään.

Tietoturvan vahvuuden taso organisaatioissa on yhteydessä työntekijöiden valveutuneisuuteen (Traficom 2019, 61). Siponen (2000) on tarkastellut tietoturvatietoisuuden (information security awareness) käsitettä, jolla viitataan tilaan, jossa työntekijät ovat

tietoisia tietoturvasta ja ideaalissa tilanteessa noudattavat tietoturvaohjeistuksia. Työntekijöiden tietoturvatietoisuuden vahvistamisella tavoitellaan muutosta tietoturvalliseen toimintaan ja käyttäytymiseen (Abawajy 2012, 238). Työntekijöille tulisi olla selvää, että miksi tietoturvaohjeistuksia tulee noudattaa (Siponen 2000). Tietoturvatietoisuutta voidaan parantaa esimerkiksi viestintäkampanjoilla, joiden tarkoituksena on luoda organisaatiolle turvallisuuskeskeistä kulttuuria. Tietoturvatietoisuus on siis yksi osa-alue organisaation tietoturvakulttuurin rakentumisessa. (ks. Siponen 2000, 39; Abawajy 2012, 238–239.)

Da Veiga ja kumppanit (2020) ovat kirjallisuuskatsauksen pohjalta luoneet kokoavan määritelmän tietoturvakulttuurista, jota käytetään myös tässä tutkielmassa: Organisaation tietoturvakulttuuri pohjaa työntekijöiden toimintaan ja käyttäytymiseen. Tietoturvapolitiikka ja tietoturvaohjeistusten noudattaminen yhdessä viestinnän ja työntekijöiden koulutuksen kanssa ovat tietoturvakulttuurin tukipilareita. Tietoturvallisesta toiminnasta tulee muodostua organisaation laajuisesti normaali ja luonnollinen tapa tehdä töitä, joka on yhteydessä työntekijöiden oletuksiin, arvoihin, uskomuksiin, tietoisuuteen ja asenteisiin sekä näkemyksiin tiedon turvaamisesta. Organisaation johdon ja johtamisen rooli korostuu tietoturvakulttuurin rakentamisessa, kuten myös tarkoituksenmukaisen tieto- ja viestintäteknologian saatavuus. Merkittävään asemaan nousee myös luottamus niin työntekijöiden kuin sidosryhmien välillä, joka mahdollistaa tiedon luottamuksellisuuden, eheyden ja saatavuuden. Tässä tutkielmassa on oleellista saavuttaa ymmärrystä Finavian tietoturvakulttuurista, jotta viestinnän roolia ja yhteyttä tietokulttuurin rakentumiseen voidaan tarkastella Finavian kontekstissa.

Hyvänä esimerkkinä organisaation tietoturvakulttuurin vahvistamisesta toimii Microsoftin uusi lähestymistapa turvallisuuskoulutuksen uudistamisessa. Microsoftin uutisen (Ansari 2020) mukaan turvallisuuskoulutusten johtaja Ken Sexsmith on asettanut tavoitteeksi “liikkeen” aloittamisen, jossa jokainen työntekijä haluaa olla osa organisaation turvallisuustarinaa. Tavoitteena on tehdä tietoturvasta henkilökohtaista, kiinnostavaa, samaistuttavaa, mutta myös tehokasta. Sitouttava ja osallistava

tietoturvakoulutus, joka käyttää tosielämän esimerkkejä tietoturvauhkista motivoi henkilöstöä ja sai työntekijät innostumaan tietoturvasta. Uuden oppimisen lisäksi Microsoftilla on tavoitteena ylläpitää jo opittuja taitoja, jotka helposti unohtuvat, ellei niitä säännöllisesti kerrata. Uutisen mukaan, riippumatta keinoista millä henkilöstöä kouluttaa tietoturvasta, koulutuksen tulisi olla aina vastavuoroista. Työntekijöiden kuuleminen ja heidän lähtökohtansa sekä tarpeidensa ymmärtäminen on ensiarvoisen tärkeää. Työntekijöiden asenteet ja suhtautuminen, motivaatio ja kiinnostus, arvot, avoimuus ja luottamus sekä työhyvinvointi ja tuki ovat kaikki tekijöitä, jotka ovat yhteydessä työntekijöiden tietoturvalliseen toimintaan (esim. Alavi ym. 2016).

## 3.3 Viestintä tietoturvakulttuurin lähtökohtana

Organisaation toiminta perustuu ihmisten väliselle vuorovaikutukselle (Valo & Mikkola 2020, 3). Vuorovaikutuksessa organisaation työntekijät tuottavat ja muokkaavat sosiaalisia rakenteita ja toimintaa, eli käsityksiä todellisuudesta (Berger & Luckmann 1967). Tietoturvakulttuurin rakentumista organisaatioissa voidaan tarkastella tämän kaltaisen sosiaalisen tai viestinnällisen rakenteistumisen (esim. Giddens 1984) lähtökohdista. Giddensin (1984) mukaan viestinnässä ja vuorovaikutuksessa muodostetaan sekä muokataan sosiaalisia rakenteita, jotka ohjaavat ja vaikuttavat ihmisten toimintaan.

Valon ja Mikkolan (2020) mukaan viestintä on toimivan organisaation kannalta välttämätöntä, koska se on työntekijöiden välisen yhteistyön edellytys. Organisaation viestinnässä ja vuorovaikutuksessa luodaan merkityksiä, jaetaan arvoja ja asetetaan yhteisiä tavoitteita, eli tuotetaan ja muokataan sosiaalista todellisuutta. Työntekijöiden arjessa viestintä voi olla sisäistä tiedottamista, johtamisviestintää, tiimien ongelmanratkaisua ja päätöksentekoa tai esimerkiksi kahvihuonekeskusteluja. Pohjimmiltaan työntekijöiden välinen vuorovaikutus on viestien tuottamista ja tulkintaa, sekä sosiaalisen todellisuuden ja eri tilanteiden ymmärtämistä. Näin ollen myös

organisaation erilaiset kulttuurit rakentuvat työntekijöiden välisessä vuorovaikutuksessa, eli organisaation viestinnässä (ks. Valo & Mikkola 2020).

Yhtenä viestinnällisen rakenteistumisen lähtökohtana on CCO-näkökulma (Communicative constitution of organizations / organisaation viestinnällinen rakenteistuminen). CCO-näkökulma tarkastelee kuinka viestintä määrittää ja rakentaa sosiaalista todellisuutta (Baxter 2004, 3). CCO-näkökulman on alun perin esitellyt James Taylor ja hänen kollegansa (ks. Taylor, Cooren, Giroux & Robichaud 1996), joka tunnetaan nimeltä Montreal School CCO. Schoenebornin ja kumppaneiden (2014) mukaan organisaatio rakentuu viestinnässä kahdella eri tapaa: 1. artefakteista ja materiaaleista (non-human agency) ja 2. vuorovaikutuksessa ymmärrettynä (human agency). Ensimmäinen tapa käsittää artefaktat ja materiaalit, joilla on suuri merkitys organisaation rakentumiseen: esimerkiksi tilat, logot, politiikat, ohjeistukset ja muistiot voidaan käsittää toimijoiksi, jotka merkityksentävät organisaatiota, sen tavoitteita, arvoja ja asemaa. Inhimillisten toimijoiden, työyhteisön vuorovaikutuksen lisäksi, myös näillä ”ei-inhimillisillä” toimijoilla on merkittävä roolinsa organisaation rakentumisessa viestinnässä ja vuorovaikutuksessa. Hyödyntäen sosiaalisen ja viestinnällisen rakenteistumisen lähtökohtia, määrittelen tässä tutkielmassa viestinnällisen lähtökohdan seuraavasti:

*Organisaatio on viestinnällisten prosessien verkosto, jossa rakennetaan, määritetään ja ylläpidetään sosiaalista todellisuutta. Organisaatiot ovat dynaamisia sekä jatkuvasti muuttuvia, ja niiden olemassaolo perustuu viestinnälle ja vuorovaikutukselle, sekä inhimillisiin että ei-inhimillisiin toimijoihin.* (Schoeneborn ym. 2014; Wilhoit 2018; Valo & Mikkola 2020)

Työntekijöiden rooli organisaation tietoturvan toteutumisessa on merkittävä (Moinescu ym. 2019). Viestinnän lähtökohdat korostavat työyhteisön vuorovaikutuksen prosessien merkitystä tietoturvakulttuurin rakentumiselle. Vuorovaikutuksessa luodaan ja muokataan organisaation kulttuureja (Valo & Mikkola 2020, 9). Tietoturvaan keskittyvä viestintä ei voi olla ainoastaan yksisuuntaista, vaan sen täytyy olla vuorovaikutteista ja työntekijöiden lähtökohdat huomioonottavaa. Täytyy kuitenkin

ymmärtää, että sosiaalisten rakenteiden muuttaminen ei tapahdu hetkessä, koska juurtuneilla arvoilla ja normeilla on usein pitkä historia (ks. Valo & Mikkola 2020).

Näkemykseni mukaan tietoturvakulttuurin rakentuminen lähtee liikkeelle siitä, että työntekijöiden merkityksiä, arvoja ja tavoitteita tietoturvasta sovitetaan yhteen. Isossa organisaatiossa, kuten Finavialla, jossa työntekijät toimivat hajautetusti ja hyvin erilaisissa työtehtävissä, merkitysten yhteensovittaminen voi näyttäytyä haasteelliselta. Tässä tutkielmassa ratkaisuja sekä työkaluja tietoturvakulttuurin rakentumiseen haetaan *tietoturvaviestinnästä*, jota ohjaavat käsitykset organisaation viestinnällisestä rakenteistumisesta.

# 4 TIETOTURVAVIESTINTÄ

Tässä tutkielmassa muodostan ja esittelen uutena käsitteenä *tietoturvaviestinnän*. Käsitteellä lisätään ymmärrystä tietoturvakulttuurin rakentumisesta organisaation viestinnässä.

Organisaatiokulttuuri sisältää monipuolisia viestinnän ja vuorovaikutuksen lähtökohtia: viestintäkäytänteitä interpersonaalisissa suhteissa, tiimeissä, tapaamisissa ja muissa kohtaamisissa työpaikoilla, interpersonaalisia käyttäytymismalleja (esim. tuki, luottamus), johtamisviestintää sekä työntekijöiden osallistamista ja vaikuttamista (Valo & Mikkola 2020, 9). Myös tietoturvakulttuurin rakentumisessa nojataan näihin viestinnän ja vuorovaikutuksen lähtökohtiin. Tässä luvussa tietoturvaviestinnän käsitettä rakennetaan turvallisuuden johtamisen, turvallisuusviestinnän, tietoturvakulttuurin ja tietoturvan johtamisen sekä muutosviestinnän kirjallisuudesta ja julkaisuista. Käsitteen jäsennystä tehdään yhdistämällä viestinnän ilmiöitä turvallisuuden kontekstissa saatuihin tuloksiin.

## 4.1 Turvallisuusviestinnästä tietoturvaviestintään

Perinteiseen turvallisuusviestintään organisaatioissa kuuluu "johdon turvallisuuden eteen tekemien asioiden kertominen henkilöstölle, tapaturmista ja muista vaaratilanteista informoiminen sekä turvallisuuteen liittyvien päätösten perusteluiden viestiminen (Reiman ym. 2008, 53)." Esimerkiksi Finavia (2019, 39) kehitti vuoden 2019 aikana turvallisuusviestintää jakamalla henkilöstölle safety alert -viestejä ja turvallisuuskoosteita ajankohtaisista turvallisuusaiheista. Hofmannin ja Morgesonin (1999, 293) mukaan turvallisuuteen keskittyvä viestintä on yhteydessä turvallisuuteen sitoutumiseen ja onnettomuuksien määrään. Tietoturvaviestinnän voidaan ajatella omaavan organisaatioissa samoja tavoitteita kybertoimintaympäristössä fyysisen maailman sijaan: miten tietoturvauhkia ennaltaehkäistään ja miten tietoturvauhkan toteutuessa toimitaan? Barlowin ja kumppaneiden (2013, 146) mukaan hyvin suunniteltu viestintä voi vähentää työntekijöiden tekemien tietoturvarikkeiden määrää.

Tässä tutkielmassa hyödynnetään aikaisempaa tutkimusta viestinnästä osana turvallisuuskulttuurin rakentumista, koska tietoturva on yksi organisaation turvallisuuden ulottuvuuksista.

Viestinnällä on merkittävä rooli tietoturvan toteutumisessa ja tietoturvakulttuurin rakentumisessa organisaatioissa (ks. Barlow, Warkentin, Ormond & Dennis 2018; D'Arcy & Greene 2014; Hsu, Shih, Hung & Lowry 2015; McEvoy & Kowalski 2019). Vahva turvallisuuskulttuuri pohjautuu viestintään ja vuorovaikutukseen, joilla rakennetaan luottamusta ja yhteisiä merkityksiä turvallisuudesta (ks. esim. Cooper 2000). Turvallisuuden ja tietoturvan tutkimuksessa viestinnän tarkastelu painottuu johtamiseen (ks. esim. D'Arcy & Greene 2014; McEvoy & Kowalski 2019; Reiman, Pietikäinen & Oedewald 2008), vaikuttamaan pyrkivään viestintään (ks. esim. Boss ym. 2015; Johnston ym. 2015; Siponen ym. 2020) ja työyhteisön vuorovaikutuksen ilmiöihin (ks. esim. Hofmann & Stetzer 1998; Hsu ym. 2015; Kath, Marks & Ranney 2010; Wilson-Donnelly, Priest, Burke & Salas 2004). Seuraavissa alaluvuissa jäsennän tietoturvaviestinnän käsitettä teoreettisesti pohjautuen muun muassa mainittuun kirjallisuuteen.

## 4.2 Tietoturvan johtamisviestintä

Tietoturvakulttuuria ohjaa johdon näkemys (Da Veiga ym. 2020) ja johtamisen rooli on merkityksellinen myös tietoturvaviestinnän kokonaisuudessa. D'Arcyn ja Greenen (2014) mukaan johdon tulisi selkeästi viestiä ja osoittaa toiminnallaan, että tietoturva on organisaatiossa keskeisessä asemassa. Tämän viestin tavoitteena on saada työntekijät kokemaan vastuuta tietoturvan toteutumisesta, koska mikään teknologinen ratkaisu ei suojaa organisaatiota kyberhyökkäyksiltä yhtä vahvasti kuin osaava ja tietoinen henkilöstö. Johdon tehtävänä on edistää positiivia asenteita ja asennoitua sekä toimia itse esimerkillisesti (Kath, Marks & Ranney 2010, 649; Reiman, Pietikäinen & Oedewald 2008, 53; Wilson-Donnelly ym. 2004, 26). Käytännössä tämä tarkoittaa turvallisuuden arvon osoittamista viestinnässä ja päätöksenteossa (Reiman &

Oedelwald 2008, 144), mikä auttaa osaltaan työntekijöitä ymmärtämään tietoturvan roolia organisaation päivittäisessä toiminnassa. Tietoturva-asioista viestimisen voidaan nähdä olevan johdon vastuulla, kuten myös tietoturvaan liittyvien näkemysten ja käsitysten hallinnan organisaatiossa. Organisaation johtoportaan ja lähijohtajien tulisi sitoutua kannustamaan organisaation oppimista tietoturvan teemoista ja mahdollistaa oppimiselle hyvät lähtökohdat avoimella viestinnällä ja vuorovaikutuksella (Littlejohn, Lukic & Anoush 2015, 289).

Tietoturvalle kohdistetut viestintäkanavat (Alavi ym. 2016; Harrison & Jurjens 2017) parhaimmillaan vahvistavat tietoturvatietoisuutta, koska ne helpottavat oikea-aikaisen tiedon löytämistä ja saatavuutta. Viestintä tulee myös kohdentaa eri kohderyhmille organisaatioissa – suorittavaa työtä tekevän ei välttämättä tarvitse saada tietoa tietojärjestelmäpäivityksistä, mutta tietotyöläiselle tämä tieto voi olla tärkeä. Johnston ja kumppanit (2019, 270) toteavat työntekijöiden omaavan motivaatiopulaa tietoturvaa koskevien viestien prosessoinnissa, koska niitä ei koeta henkilökohtaisella tasolla merkittäviksi ja relevanteiksi. Mikäli tietoturvaohjeistukset ja -toimenpiteet on suunniteltu tukemaan työn tavoitteita ja toteuttamaan velvollisuuksia, työntekijät todennäköisemmin hyödyntävät niitä osana päivittäisiä työtehtäviään (Karyda, Kiountouzis & Kokolakis 2005, 257).

Tietoturvakoulutukset ja -harjoitukset voidaan myös nähdä osana organisaation johdon suunnittelemaa viestintää. Niillä pyritään esimerkiksi lisäämään työntekijöiden ymmärrystä tiedonhallintaan liittyvistä riskeistä ja laajemmin organisaation tietoturvapolitiikasta. Chenin ja kumppaneiden (2015) mukaan SETA (opetus, harjoitus ja tietoisuus) ohjelmia käytetään nostamaan työntekijöiden tietoturvatietoisuuden tasoa, kehittämään tietoturvataitoja ja -tietoja päivittäisen työn tueksi, viestimään velvollisuudesta ja vastuusta sekä seurauksista (Wilson & Hash 2003). Da Veiga ja kumppanit (2020) vahvistavat näkemystä viestinnän tärkeästä roolista tietoturvaa koskevassa muutoksenhallinnassa, joka on erityisen korostunutta ottaen huomioon digitaalisen maailman nopean muutostahdin.

Tietoturvatietoisuutta voidaan parantaa esimerkiksi viestintäkampanjoilla, joiden tarkoituksena on luoda organisaatiolle turvallisuuskeskeistä kulttuuria. (ks. Abawajy 2012, 238–239; Siponen 2000, 39.) Samoin myös sisäiseen viestintään tuotetut tiedotteet ja uutiset lisäävät tietoturvan näkyvyyttä organisaatiossa. Tietoturvaan liittyvät ohjeistukset ovat myös osana tietoturvan johtamisviestintää ja CCO-näkökulman mukaisesti ohjeistukset voivat olla toimijoita, jotka osaltaan rakentavat merkityksiä tietoturvasta. Hedströmin ja kumppaneiden (2011, 374) mukaan tietoturvaohjeistukset ovat organisaation ilmaisuja tietoturvallisen toiminnan arvoista.

Tietoturvakäytänteitä ei voida kehittää ilman vastavuoroista viestintää työntekijöiden välillä. Suositusten, palautteen ja huolien jakaminen auttaa johtoa kehittämään organisaation tietoturvakulttuuria (ks. Hsu, Shih, Hung & Lowry 2015). Koska tietoturva vaatii pitkäjänteistä jatkuvuuden hallintaa, on palautteen saaminen kriittistä sujuvan muutostahdin ylläpidossa (ks. Lewis 2006, 24). Vastavuoroisuutta voidaan kehittää tukemalla ja kannustamalla työntekijöitä avoimeen viestintään. Kath ja kumppanit (2010, 644) toteavat työntekijöiden nostavan turvallisuuteen liittyviä asioita helpommin keskusteluun, mikäli he kokevat organisaation välittävän työntekijöistään. Tietoturvan kohdalla voidaan ajatella tämän mallin toimivan samalla tavalla: kun organisaatio tukee työntekijöidensä hyvinvointia ja viihtyvyyttä, lisää se työntekijöiden motivaatiota toimia yhteiseksi hyväksi sekä vähentää mahdollista sisäpiiriläisten muodostamaa uhkaa. Tämä voi tarkoittaa esimerkiksi sitä, että alaiset ilmoittavat tietoturvaan liittyvistä huolista suuremmalla todennäköisyydellä lähijohtajille, jonka on perinteisen työturvallisuuden kohdalla todettu vähentävän tapaturmia (ks. Hofmann & Morgeson 1999, 293; Hofmann & Stetzer 1998). Vahvat lähijohtaja-alaissuhteet mahdollistavat pienienkin epävarmuuksien ja huolien nostamisen lähijohtajien tietoisuuteen (Kath ym. 2010, 649), eli rima keskustella tietoturvaa koskevista asioista madaltuu.

Johdon tuki on tärkeää työntekijöiden tietoturvallisen käyttäytymisen toteutumisessa ja tietoturvaohjeistusten noudattamisessa. Sen sijaan, että työntekijöitä pakotettaisiin väkisin noudattamaan tietoturvaohjeistuksia tai sanktioiden uhalla, tulisi

tietoturvallisen käyttäytymisen olla vapaaehtoista ja itseohjautuvaa (ks. Vroom ja Von Solms 2004). Kun työntekijät kokevat olevansa itse vastuussa omasta osallistumisestaan, koetaan viestintä vähemmän pakottavana ja enemmän suostuttelevana (Lewis 2006, 32), mikä voi heijastua esimerkiksi tietoturvaohjeistusten parempaan noudattamiseen. Merkittävään asemaan tietoturvakulttuurin rakentumisessa asettuvat johtotehtävissä olevat työntekijät, joiden omat asenteet tietoturvasta ja käyttäytymismallit heijastuvat organisaation muiden työntekijöiden näkemyksiin ja käsityksiin tietoturvan tärkeydestä.

## 4.3 Tietoturvan vaikuttamisviestintä

Vaikuttamaan pyrkivä viestintä voidaan mieltää organisaation johdon keinoksi tietoturvan vahvistamiseen. Yhtenä tehokkaana keinona tietoturvaohjeistusten noudattamiseen on todettu erilaisten sanktioiden hyödyntäminen ja niistä viestiminen (esim. Boss ym. 2015; Johnston, Warkentin & Siponen 2015). Tämä lähestysmistapa on tuttu kriminologian ja terveystieteiden tutkimuksesta, kuten esimerkiksi tupakan terveysriskeistä viestiminen ja sen seurauksena toivottu käyttäytymisen muutos terveellisimpiin elämäntapoihin. Tietoturvan kontekstissa haasteeksi osoittautui se, että uhkat koskettavat tietoa ja tietojärjestelmiä, eivätkä suoraan työntekijää (Johnston ym. 2015). Tässä tutkielmassa olen osoittanut, seuraukset tiedon hallinnoijalle tai omistajalle voivat olla merkittäviä, koska tieto on nykypäivänä jokaiselle tärkeä pääoma.

Siponen ja kumppanit (2020) ovat tarkastelleet tietoturvaan liittyvää viestintää vaikuttamisen lähtökohdista hyödyntämällä Sykesin ja Matzan (1957) esittelemien neutralisaatiotekniikoiden vastaista viestintää, eli antineutralisaatio-viestintää. Antineutralisaatio-viestintä voi esimerkiksi sisältää sanoman, jonka mukaan on väärin ajatella, ettei salasanojen jakamisesta koidu harmia ja salasanojen jakaminen on kaikissa tilanteissa väärä tapa toimia (Barlow, Warkentin, Ormond & Dennis 2018, 693). Barlow ja kumppanit (2013) toteavat antineutralisaatio-viestinnän olevan yhtä tehokasta, ellei tehokkaampaa kuin sanktioista viestimisen tietoturvaohjeistusten parempaan

noudattamiseen. Neutralisaatiotekniikoiden tavoitteena on oikeuttaa sääntöjen vastaista toimintaa ja estää syyllisyyden tunnetta sekä negatiivista minäkuvaa. Siponen ja Vance (2010) totesivat neutralisaatiotekniikoiden ennustavan merkittävästi yksilöiden aikeita olla noudattamatta tietoturvaohjeistuksia.

Lisäksi niin sanottujen pelkoilmauksien (fear appeals) käyttöä on hyödynnetty vaikuttamaan pyrkivässä viestinnässä, kun tietoturvaan liittyvää viestintää on tehostettu muokkaamaan työntekijöiden näkemyksiä potentiaalisista uhkista ja toivotusta käyttäytymisestä suojaamaan kyseiseltä uhkalta (Johnston ym. 2015). Yksinkertaistettuna pelkoilmaukset ovat vaikuttamaan pyrkivää viestintää, jotka ovat suunniteltu "säikäyttämään" yksilö noudattamaan ohjeistuksia kertomalla mahdollisista pelottavista ja vakavista seurauksista, mikäli ohjeistusta laiminlyödään (Witte 1992, 329). Pelkoilmauksiin yhdistettynä viestintä mahdollisista sanktioista on todettu keinoksi tehostaa tietoturvaohjeistusten noudattamista. Erityisesti epäviralliset sanktiot, kuten mahdollinen itsensä nolaaminen kollegoiden edessä, koettiin vahvaksi motivaatiotekijäksi tietoturvallisen käyttäytymisen toteutumiseen (Johnston ym. 2015). Vaikuttamaan pyrkivästä viestinnästä tietoturvan kontekstissa on tehty huomattavasti tutkimusta. Tässä tutkielmassa vaikuttamisviestintää hyödynnetään tietoturvaviestinnän kokonaisuuden hahmottamisessa. Aikaisemmalla tutkimuksella tuetaan uusia näkökulmia viestinnän hyödyntämisestä tietoturvakulttuurin rakentumisessa.

Barlowin ja kumppaneiden (2018, 701) tulokset osoittavat, että tietoturvaviestintä voi lisätä tietoturvaohjeiden noudattamista paremmin kuin asetetut sanktiot, erityisesti niissä tilanteissa, joissa työntekijä pohtii noudattamatta jättämisen hyötyjä. Kuten Siponen (2000) huomauttaa, että työntekijöiden tulisi ymmärtää miksi ohjeistuksia tulisi noudattaa, myös Barlowin ja kumppaneiden (2018) tutkimuksesta käy ilmi, että lyhyetkin perusteluviestit vahvistavat ohjeiden noudattamista, koska ne tukevat työntekijää tietoturvaa koskevassa päätöksenteossa. Vaikuttamaan pyrkivä viestintä ja erityisesti pelkoilmauksien sekä sanktioiden käyttö ajautuvat kuitenkin ristiriitaan Vroomin ja Von Solmsin (2004) tietoturvakulttuurin määritelmän keskeisten lähtökohtien kanssa. Määritelmässä korostuvat työntekijöiden vapaaehtoinen ja

itseohjautuva tietoturvallinen toiminta. Voidaan pohtia edistävätkö sanktiot ja pelottelu vapaaehtoiseen ja itseohjautuvaan toimintaan parhaiten - tavoitellaanko muutosta ainoastaan käyttäytymisessä vai myös asenteissa, arvoissa ja näkemyksissä? Työntekijöiden päivittäisen toiminnan ymmärtämiseen avain saattaa löytyä niistä arvoista, jotka heidän toimintaansa ohjaavat (Hedström ym. 2011, 374).

## 4.4 Työyhteisön vuorovaikutuksen prosessit tietoturvan kontekstissa

Näen tietoturvan toteutumisen organisaatioissa yhtenä työyhteisön vuorovaikutuksen lopputuloksena. Työntekijöiden välisessä vuorovaikutuksessa luodaan merkityksiä, jaetaan arvoja ja asetetaan yhteisiä tavoitteita (Valo & Mikkola 2020). Reiman, Pietikäinen ja Oedewald (2008, 50, 78) kuvaavat organisaation työyhteisön vuorovaikutuksen prosessien ulottuvuutta keskeisenä tekijänä turvallisuuskulttuurin rakentumisessa. Heidän mukaansa sosiaalisten ilmiöiden tarkastelussa on otettava huomioon ”organisaatioiden ajallinen ja jatkuvasti muuttuva luonne”, jossa työyhteisön päivittäinen vuorovaikutus muokkaa käsityksiä ja merkityksiä. Työyhteisön vuorovaikutuksessa rakennetaan yhteistä ymmärrystä organisaation tietoturvasta, minkä määrittelen yhdeksi tietoturvaviestinnän tärkeimmistä lähtökohdista. Organisaatiokulttuuri, turvallisuuskulttuuri ja tietoturvakulttuuri ovat opittuja toimintamalleja. Reiman ja kumppanit (2008, 10) kiteyttävät opitun kulttuurin vaikuttavan siihen, miten työyhteisössä ollaan vuorovaikutuksessa keskenään, mitä asioita organisaatiossa arvostetaan ja pidetään tärkeinä, sekä miten tavoitteet ja niiden saavuttaminen hahmotetaan.

Organisaation monimutkaiset ja vaativat tehtävät korostavat yhteistyön merkitystä työyhteisön vuorovaikutuksessa (Valo & Mikkola 2020, 7). Yhteistyössä näille tehtäville haetaan ymmärrystä ja merkityksiä. Organisaatioiden tehtäväkeskeinen luonne luo tarvetta esimerkiksi tiedonhallinnalle, tiedonjakamiselle ja päätöksenteolle, jotka ovat keskeisessä asemassa organisaation viestintää ja työyhteisön vuorovaikutusta. Työtyytyväisyyttä tarkasteltaessa työntekijät kokevat erityisen tärkeänä tiedon

saatavuuden, sen oikea-aikaisuuden ja hyödyllisyyden (Lewis 2006, 31). Littlejohnin ja kumppaneiden (2015) tutkimuksessa oppimiskulttuurin ja turvallisuuskulttuurin nähtiin tukevan toisiaan. Hyvä turvallisuuskulttuuri edellyttää siis organisaatiolta myös hyvää oppimiskulttuuria. Molemmat näistä kulttuureista pohjautuvat avoimeen viestintään ja vuorovaikutukseen työyhteisössä, mikä tarkoittaa esimerkiksi sujuvaa viestintää johdon ja alaisten välillä sekä kannustamista keskusteluun turvallisuuteen liittyvistä teemoista. Työntekijöitä tulisi osallistaa päätöksentekoon ja sitouttaa osaksi turvallisuuden kehittämisprosesseja. Tämä vaatii selkeitä viestintäkanavia ja ohjeistuksia palautteen sekä kehitysideoiden jakamiseen.

Tietoturvaviestinnän lähtökohtana on ihmiskeskeisyys. Kun tietoturvaa kehitetään ihmiskeskeisestä lähtökohdasta, merkittävässä asemassa on työntekijöiden näkemysten ja merkitysten hallinta. Organisaation vahva tietoturva rakentuu osaavien, motivoituneiden, hyvinvoivien ja sitoutuneiden työntekijöiden varaan, jotka ovat jokainen osana organisaation tietoturvaviestintää. Tietoturvaviestintä on organisaation suunniteltua ja strategista viestintää tietoturvasta, kuten tiedotteita, viestintäkampanjoita, koulutuksia ja ohjeistuksia. Lisäksi tietoturvaviestintä on työyhteisön vuorovaikutuksen ja sosiaalisten prosessien hallintaa, kuten merkitysten yhteensovittamista tietoturvasta. Tietoturvaviestintä tulee nähdä kokonaisuutena, joka lävistää organisaation kaikki tasot ja tavoittaa kaikki työntekijät kohdennetusti, oikea-aikaisesti ja ymmärrettävästi. Tietoturvaviestintä perustuu yhteistyölle ja oikein toteutettuna se rakentaa organisaation tietoturvakulttuuria.

## 4.5 Tietoturvan muutosviestintä

Kybermaailman nopeasta muutostahdista johtuen organisaatiot elävät jatkuvassa muutoksessa myös tietoturvan hallinnassa. Kun teknologian hyödyntäminen lisääntyy ja erilaiset uhkat kybermaailmassa kehittyvät, täytyy organisaation myös kehittyä ja muuttua. Muutosta luodaan, ylläpidetään ja hallitaan viestinnällä, jossa keskeisessä asemassa on yhteisen ymmärryksen rakentaminen (ks. Ford & Ford 1995).

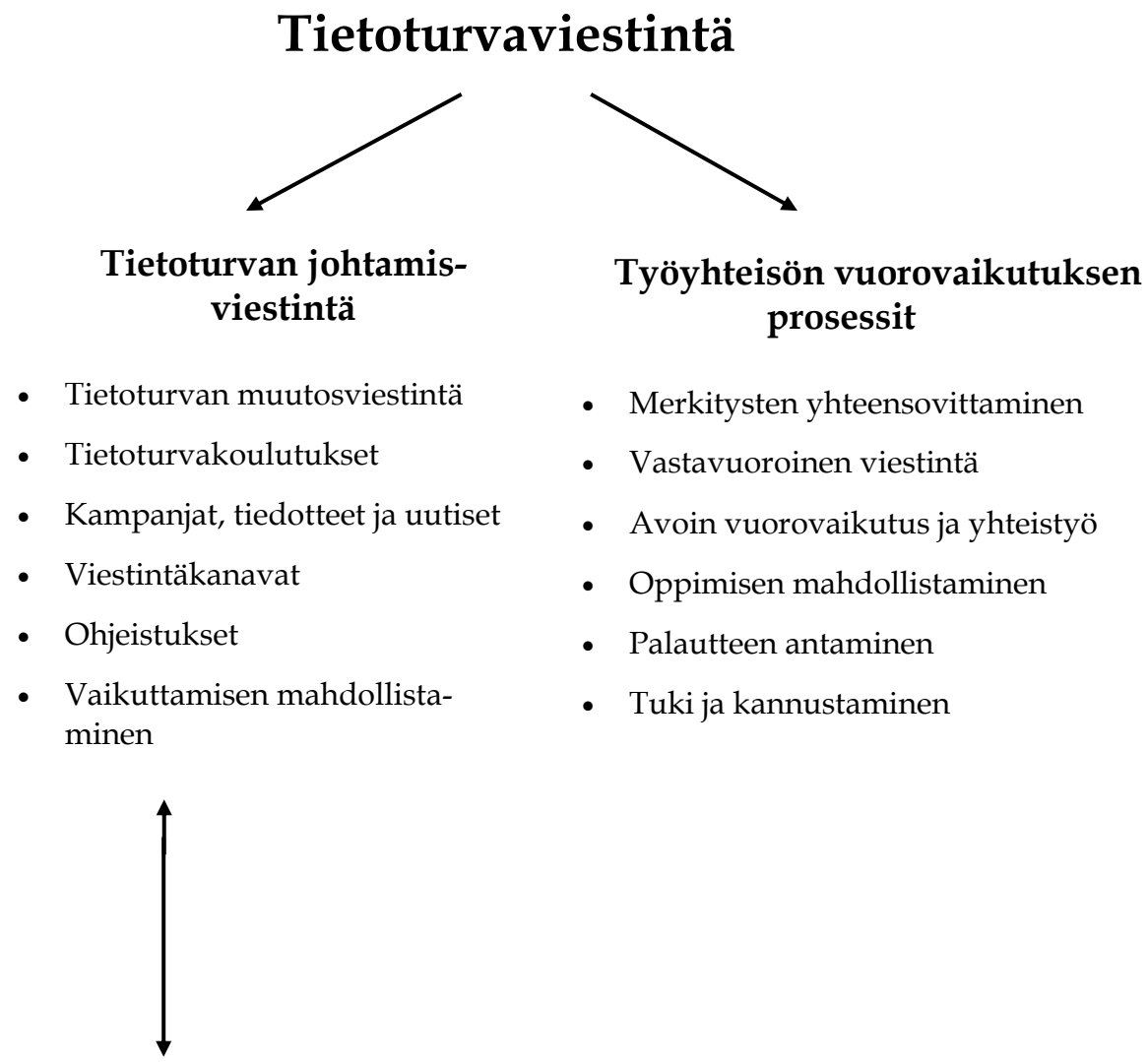
Tietoturvaviestinnän kokonaisuus voi vahvasti hyötyä muutosviestinnän lähtökohdista osana tietoturvaan liittyvää muutoksenhallintaa. Muutosviestintä on tässä tutkielmassa tietoturvaviestinnän käsitteen jäsentämistä ohjaava tekijä.

Johtamisen merkitys muutosviestinnässä on olennainen, koska johtajat lähtökohtaisesti toimivat muutoksen käynnistäjinä ja rakentavat visiota sekä toteuttavat viestintää. Muutosta täytyy siis johtaa suunnitelmallisesti (ks. esim. Pádár, Pataki & Sebestyén 2017) ja monesti muutosprojektille valitaan muutoksen johtaja tai johtajia, joiden roolina on muun muassa edustaa projektin tavoitteita ja arvoja sekä huolehtia tarvittavista resursseista (Harrison 1999; Schroeder 2015, 2). Muutoksen onnistuminen on aina jossain määrin riippuvainen johdon muutosviestinnän laadusta (ks. esim. Luo, Song, Gebert, Zhang & Feng 2016). Laadukkaiden johtaja-alaissuhteiden nähdäänkin olevan merkittävä tekijä muutoksen onnistumisessa, jonka puolesta puhuu myös se, että muutosviestinnän toteuttajien tulee tietää milloin, miten ja mitä tietoa työntekijöille viestitään (Lewis 2006, 26–27). Muutoksen toimivuuteen vaikuttavat työntekijöiden aiemmat, niin hyvät kuin huonotkin, kokemukset muutoksista. Näistä aikaisemmista muutosprosesseista tulisi pystyä analysoimaan toimivia käytänteitä ja soveltaa niitä tietoturvaviestinnän suunnittelussa. Muutosviestinnässä merkittävää onkin työntekijöiden näkemysten arviointi, koska työntekijöiden omat näkemykset ennustavat usein heidän asenteitaan muutoksia kohtaan ja niihin sopeutumista. (ks. Lewis 2006.)

Työyhteisön vuorovaikutuksen prosessien rooli tietoturvakulttuurin rakentumisessa korostuu myös muutoksenhallinnassa. Arviot kollegoiden asenteista, kahvipöytäkeskustelut ja epäviralliset vuorovaikutustilanteet eivät näy lähijohtajille tai muutoksen toteuttajille. (Lewis 2006, 27–29.) Muutosviestintä nähdään enemmänkin dialogisena prosessina (esim. merkitysten hallinta ja yhteensovittaminen) kuin yhdensuuntaisena viestintänä. Työntekijät haluavat kokea osallistuvansa muutokseen ja tuntea, että heidän ajatuksiaan ja ideoitaan arvostetaan muutosprosessissa (Lewis 2006, 41). Pakotettu muutos ei siis ole ratkaisu myöskään tietoturvakulttuurin rakentumisessa,

koska se herättää vastustusta. Tietoturvaviestintä toimii tärkeänä elementtinä muutoksen ja jatkuvuuden hallinnassa.

Kuviossa 2 on hahmoteltuna tietoturvaviestinnän kokonaisuutta. Kokonaisuus on jaoteltu Tietoturvan johtamisviestintään ja Työyhteisön vuorovaikutuksen prosesseihin. Molempien osa-alueiden alle on lueteltu niitä viestinnällisiä tekijöitä, jotka ovat osana tietoturvaviestintää. Lisäksi tietoturvan vaikuttamisviestintä on omana kokonaisuutenaan osana Tietoturvan johtamisviestintää.




**Kuvio 2 Tietoturvaviestinnän kokonaisuus**

# 5 TUTKIMUKSEN TOTEUTUS

## 5.1 Tutkimuksen kohdeorganisaatio

### 5.1.1 Finavian kuvaus

Tämä tutkielma toteutettiin yhteistyössä Finavian kanssa siten, että tutkielmaa varten haastatellut henkilöt olivat Finavian työntekijöitä. Tutkielma ei ollut toimeksianto, vaan ehdotin yhteistyömahdollisuutta oma-aloitteisesti aiheen parissa. Osana kriittistä infrastruktuuria toimiva lentoasemayhtiö (20 lentoasemaa) soveltuu tietoturvakulttuurin näkökulmasta relevantiksi kohdeorganisaatioksi, koska turvallisuus on yksi Finavian keskeisimmistä arvoista ja kaiken tekemisen perusta (Finavia 2019). Muita arvoja Finavialla ovat asiakaslähtöisyys, uudistuminen ja vastuullisuus. Lentoasemien ylläpitäjänä Finavia on Suomen lentoliikenteelle arvokas ja erityisesti Helsinki-Vantaan lentoasema toimii keskeisenä solmupisteenä Finnairin reittiverkostolle (Pöllänen ym. 2014). Kokonaismatkustajamäärä Finavian lentoasemilla oli vuonna 2019 jopa 26 miljoonaa matkustajaa. Henkilöstöä Finavia-konsernilla on noin 2700, jotka ovat eri alojen osaajia palvelumuotoilijoista konekalustoasiantuntijoihin ja projektipäälliköihin.

Vastuullisuusraportin (Finavia 2019) mukaan vuonna 2019 panostettiin kyber- ja tietoturvallisuuden kehittämiseen. Finavia tähtää uskottavaan ja tulokselliseen turvallisuuskulttuuriin, jota kehitettiin esimerkiksi kirkastamalla turvallisuusohjeistuksia henkilöstölle sekä järjestämällä infotilaisuuksia ja harjoituksia. Raportin mukaan Finavian turvallisuuskulttuuri on vahvistunut ja henkilöstö kokee turvallisuuden edistämisen tärkeänä. Kansainvälisen tutkimuksen (Immuniweb 2020) Helsinki-Vantaan lentoasema oli teknologisilta järjestelmiltään maailman toiseksi kyberturvallisin lentoasema. Turvallisuus Finavialla rakentuu yhteistyölle viranomaisten ja sidosryhmien kanssa, joiden välillä käydään aktiivista vuoropuhelua. Yhtenä Finavian turvallisuushallintajärjestelmän periaatteena nostetaan esille johdon sitoutuminen turvallisuuteen, jolle on asetettu tavoitteita ja säännöllinen seuranta.

Finaviaa voidaan kuvailla myös HRO-organisaatioksi (high reliability organization / korkean luotettavuuden organisaatio) (ks. esim. Sutcliffe 2011). HRO ajattelutapa kehittyi alunperin lentoalan- ja ydinvoimayhtiöiden operaatioiden havaittujen yhtäläisyyksien lähtökohdista. HRO toimii sosiaalisesti ja poliittisesti herkässä tilassa, teknologia on riskialtista ja vaarallisten onnettomuuksien mahdollisuus on tunnistettua. Lisäksi HRO:lla on monimutkainen hallinta- ja toimintajärjestelmä. (ks. Sutcliffe 2011.) HRO:lta vaaditaan turvallisuuden suhteen täydellisyyttä, ja kuten tietoturvan kontekstista tiedetään, täyttä turvallisuutta kybermaailmassa ei voida taata teknologisilla järjestelmillä (ks. esim. Limba 2017). Reimanin ja kumppaneiden (2008, 70) mukaan HRO:n henkilöstön tulee olla tietoinen tyypillisistä vaaroista ja niistä mekanismeista, jotka voivat mahdollistaa uhkien toteutumisen. Osana Suomen kriittistä infrastruktuuria Finavian tietoturva (teknologinen ja ihmiskeskeinen) asettuu merkittävään rooliin.

Tietoturvakulttuurin rakentumista Finavian viestinnässä oli mielekästä tarkastella, koska turvallisuuden tulisi olla juurtunut arvo ja näkyä vahvasti Finavian työntekijöiden päivittäisessä toiminnassa. Vaikka Finavialla turvallisuus on kaiken toiminnan keskeinen periaate, on HRO-ajattelun mukaisesti turvallisuutta arvioitava ja kehitettävä jatkuvasti (Sutcliffe 2011). Tämä tutkielma toimii myös osana Finavian turvallisuuden kehittämistä.

### 5.1.2 Asiantuntijahaastattelu

Tämän tutkielman tavoitteena on kuvata ja ymmärtää tietoturvaviestinnän yhteyttä organisaation tietoturvakulttuurin rakentumiseen. Tavoitteeseen pääsemisen tueksi toteutin asiantuntijahaastattelun Finavian tietoturvajohtaja Timo Laakson kanssa. Asiantuntijahaastattelua hyödynnettiin tässä tutkielmassa lisäämään ymmärrystä kohdeorganisaatiosta ja tietoturvaan liittyvistä arvoista, toimenpiteistä sekä tavoitteista. Laakson kanssa hyödynnettiin samaa haastattelurunkoa (ks. Liite 1) kuin muiden haastateltavien kanssa, mutta tulokulma kysymyksiin oli erilainen. Esittelen asiantuntijahaastattelun havaintoja kahdessa osassa, 1. Tietoturva Finavialla ja 2.

Tietoturvaviestintä Finavialla. Molemmissa osissa sisältö pohjautuu Timo Laakson vastauksiin haastattelutilanteessa syksyllä 2020.

**Tietoturva Finavialla.** Finavian kaiken toiminnan perusta on turvallisuus. Lentoasemilla on korkea riskiprofiili ja ne ovat komplekseja sekä kriittisiä kokonaisuuksia, niin sosiaalisesti kuin teknologisestikin. Tietoturva on osa kokonaisuusturvallisuutta, jossa yhteistyötä tehdään monien toimijoiden kesken. Tietoturvan rooli on Finavialla toimia tukifunktiona, joka mahdollistaa lentoaseman toimintaa. Tietoturvaa ja sen tavoitteita ohjaavat lentoasemilla vahvasti erilaiset lait ja säännökset. Tavoitteena on varmistaa ilmailuturvallisuus sekä toiminnan häiriöttömyys ja jatkuvuus. Tavoitteita tukevat muun muassa oma tietoturvanhallintajärjestelmä, poliitikat ja ohjeistukset sekä käytännön teknologinen toteutus. Laakson mukaan tietoturvakulttuuri on keskeinen tekijä tietoturvan edistämisessä. Turvallisuus on lentoasemilla ”sisään rakennettua” toiminnassa, koska reguloituna toimijana turvallisuuden kokonaisuus on tarkasti määritelty ja työntekijät ovat tähän tottuneet. Tietoturvaa edistää myös aktiivinen riskienhallintatyö.

**Tietoturvaviestintä Finavialla.** Tietoturvasta viestimiseen hyödynnetään Intranettiä, jonka sisältöä ovat ohjeet, dokumentit, tiedotteet, uutiset ja blogitekstit. Microsoft Teamsissa IT:llä on oma kanavansa ja Teamsista löytyy myös avoin kanava kyberturvallisuudelle. Teamsin kanavien tavoitteena on kehittää vuorovaikutteisuutta. Teamsissa voidaan esittää kysymyksiä ja kommentteja matalalla kynnyksellä kyberaiheista. Teamsin hyödyntäminen myös keventää intranetin sisältöjen määrää. Sähköpostia käytetään aktiivisesti, ja kohdennusta viesteissä on jonkin verran (esim. esimieskirjeet). Tilannekuvasovelluksen kautta viesti saadaan tarvittaessa koko henkilöstölle puhelimiin. Tavoitteena on selkeyttää eri viestintäkanavien roolia, jotta kanavilla olisi selkeät ja toisistaan erottuvat funktiot.

Laakson mukaan tavoitteena on, että tietoturvaan liittyvät ohjeistukset ja toimintamallit olisi rakennettu suoraan työohjeisiin. Tavoitteena on, että erilliset ohjeet kerätään yhdeksi kokonaisuudeksi: ”esimerkiksi projekteilla ei tarvitse olla erilliset

projektiohjeet ja projektin tietoturvaohjeet, vaan ne olisivat sama ohje.” Intrassa halutaan jakaa yleisohjeet tietoturvaan liittyen. Perinteisen turvallisuuden ympärille on jo rakentunut toimintakulttuuri, jossa ohjeita noudatetaan ja niitä jopa kaivataan, mikäli niitä ei ole saatavilla.

Tietoturvaan liittyvän viestinnän näkyvyyttä voidaan parantaa ja tavoitteena on suosia visualisoituja esimerkkejä tekstitiedostojen sijaan. Kaikki ohjeistukset halutaan pitää tiiviinä ja selkeinä. Laakso tunnistaa, että eri työntekijöillä on eri tietoturvaosaamisen tarpeet. Tähän yhtenä työkaluna on tietoturvaosaamisen ja ohjeiden rakentaminen suoraan työnkuvaan tai työtehtävään.

Tietoturvakoulutus on Finavialla monimuotoista. Kaikille tutuin koulutus on e-learning tietoturvakoulutus, jossa koulutetaan perusasiat tietoturvasta koko henkilöstölle (esim. yleisimmät uhkat ja niihin reagointi). Koulutuksia on ollut myös luokkamuotoisina. Koulutukseksi voidaan laskea erilaiset muistutukset ja infot tiimipalavereissa tai muissa yhteyksissä. Koulutuksilla halutaan edistää tietoturvaa positiivisen kautta, jolloin ohjeistetaan ja kannustetaan oikeanlaiseen toimintaan, sen sijaan että viesti olisi ”älä tee noin, älä tee näin.” Lisäksi Finavialla on ollut pidempiä koulutuksia ja harjoituksia, kuten hyökkäys-puolustuspäiviä teknisille asiantuntijoille.

Laakso haluaa jalkauttaa sellaista viestinnän mallia, että henkilöstö voisi ottaa yhteyden suoraan tietoturvatiimiin, ettei asiaa tarvitsisi käyttää monen eri henkilön kautta. Yhteys työntekijöihin tietoturva-asioissa halutaan mahdollisimman ketteräksi ja avoimeksi. Tätä edistää muun muassa hierarkiarakenteiden tietoinen purkaminen

Laakson mainitsemista tavoitteista ja toimintamalleista on tunnistettavissa monia tietoturvaviestintää edistäviä ja tietoturvakulttuuria rakentavia tekijöitä, kuten viestintäkanavien kehittäminen ja vuorovaikutteisuuden lisääminen. Asiantuntijahaastattelu ja työntekijöiden haastattelut antavat hyvän kokonaiskuvan Finavian nykyisestä tietoturvakulttuurista ja sen rakentumisesta organisaation viestinnässä.

## 5.2 Tutkimuksen tavoite ja tutkimuskysymykset

Tutkielman tavoitteena on kuvata ja ymmärtää tietoturvaviestinnän yhteyttä Finavian tietoturvakulttuurin rakentumiseen. Tavoitetta lähestytään pureutuen Finavian työntekijöiden käsityksiin ja kokemuksiin tietoturvakulttuurista sekä tietoturvaviestinnästä. Tutkimuksen tulosten pohjalta luodaan käytännön suosituksia ja ohjeita Finavian tietoturvakulttuurin vahvistamiseen.

Tavoitteiden saavuttamiseksi asetin kaksi tutkimuskysymystä:

1. Millaisia käsityksiä ja kokemuksia työntekijöillä on tietoturvasta Finavialla?

2. Millaista tietoturvaviestintä on Finavialla työntekijöiden käsitysten ja kokemusten mukaan?

Ensimmäisen tutkimuskysymyksen avulla pyritään ymmärtämään, miten tietoturvakulttuuri määrittyy työntekijöiden näkemysten mukaan. Tutkimuskysymys tarkastelee sitä, millaisia merkityksiä tietoturvalle annetaan ja mitä eri tekijöitä tai toimijoita siihen yhdistetään. Näkemyksiä haetaan myös työntekijöiden kokemasta vastuusta ja asenteista tietoturvaa kohtaan sekä tarkastellaan tekijöitä, jotka heikentävät tai vahvistavat tietoturvaa. Olennaista on se, että merkitykset kohdennetaan Finavian toiminnan kontekstiin. Ensimmäinen tutkimuskysymys lisää ymmärrystä Finavian tietoturvakulttuurin lähtökohdista ja nykytilasta.

Toinen tutkimuskysymys pyrkii kuvaamaan millainen viestintä ja vuorovaikutus voivat rakentaa sekä vahvistaa tietoturvakulttuuria. Työtekijöiden näkemyksiä haetaan nykyisistä tietoturvaviestinnän toimintamalleista, kuten käytetyistä viestintäkanavista, tiedottamisesta ja koulutuksista. Lisäksi tarkastellaan työyhteisön vuorovaikutuksen prosesseja, kuten johtaja-alaissuhteita. Toinen tutkimuskysymys lisää ymmärrystä tietoturvaviestinnän kokonaisuudesta Finavialla ja yleisesti organisaatioissa.

## 5.3 Tutkimusmenetelmä

Reiman, Pietikäinen ja Oedewald (2008, 78) kuvaavat lähtökohtia turvallisuuskulttuurin kaltaisen ilmiön laadulliseen tutkimukseen:

> ”Prosessimaisten ja moniulotteisten ilmiöiden tavoittaminen esimerkiksi kyselytutkimuksen keinoin haastavaa. Näiden ilmiöiden tarkastelussa on huomioitava organisaatioiden ajallinen ja jatkuvasti muuttuva luonne, jossa niin toimintatavat kuin käsitykset ja merkitykset muokkautuvat vähitellen päivittäisessä vuorovaikutuksessa työyhteisössä. Keskeistä on kiinnittää huomiota tapoihin, joilla organisaation työntekijät ovat vuorovaikutuksessa keskenään.”

Laadullinen tutkimusote mahdollistaa sisäpiiriläisten käsitysten ja kokemusten tarkastelun (Strauss & Corbin 2008, 12) tutkimuksen tavoitteiden mukaisesti. Tutkielman tavoitteena on kuvata ja ymmärtää tietoturvaviestinnän yhteyttä organisaation tietoturvakulttuurin rakentumiseen tarkastelemalla aikaisempaa tutkimusta sekä työntekijöiden käsityksiä ja kokemuksia tietoturvasta. Tarkoituksena ei siis ole testata muuttujia vaan löytää mahdollisesti uusia keinoja tietoturvan vahvistamiseen Finavialla ja muissa organisaatioissa. Tämä lähtökohta tukee laadullisen tutkimusasetelman valintaa (ks. Strauss & Corbin 2008).

Aineistonkeruun menetelmäksi valikoitui puolistrukturoitu teemahaastattelu. Puolistrukturoidulla tarkoitetaan tässä tutkielmassa haastattelua, jossa on selkeä rakenne ja valmiita esimerkkikysymyksiä, mutta keskustelua voidaan käydä myös haastattelujen aikana nousevista aiheista. Haastattelumetodilla voidaan hakea ymmärrystä haastateltavan näkemyksiin ilmiöistä (ks. esim. Kvale 1996) ja rakentaa yhteisiä merkityksiä tutkittavasta ilmiöstä (Tracy 2013). Erityisen hyvin haastattelua voidaan hyödyntää mielipiteiden, motivaatioiden ja kokemusten tarkasteluun (Tracy 2013, 132). Tässä tutkielmassa ymmärrystä haettiin työntekijöiden käsityksistä ja kokemuksista tietoturvasta. Tracyn (2013, 141) mukaan haastattelut tarjoavat myös mahdollisuuden samankaltaisuuksien ja eroavaisuuksien tarkasteluun. Tietoturvakulttuurin rakentumisen näkökulmasta työntekijöiden tulisi omata samoja käsityksiä ja

merkityksiä tietoturvasta, joten samankaltaisuuksien ja eroavaisuuksien tarkastelu on tarkoituksenmukaista.

Haastattelurunko (liite 1) muodostui pohjautuen aikaisempaan tutkimukseen aiheista ja tutkimuskysymysten ohjaamana. Runko sisälsi neljä eri teemaa:

1. Työn kuvaaminen (työntekijöiden soveltuvuus tietoturvakulttuurin tarkasteluun tutkielmassa)
2. Näkemykset tietoturvasta Finavialla (tietoturvakulttuurin tarkastelu)
3. Strateginen ja suunniteltu viestintä tietoturvasta (tietoturvan johtamisviestintä)
4. Työyhteisön vuorovaikutuksen prosessit (vuorovaikutuksen ilmiöt tietoturvan kontekstissa)

Albrechtsen (2007) sekä Posey, Roberts, Lowry ja Hightower (2014) ovat tarkastelleet työntekijöiden käsityksiä ja kokemuksia tietoturvasta laadullisesti haastattelumetodia hyödyntäen. Albrechtsen (2007) haastatteli Norjalaisen IT-yhtiön ja pankin työntekijöitä, joita ennen hän kävi keskusteluja tietoturva-asiantuntijoiden kanssa saavuttaakseen ymmärrystä organisaatioiden toimintatavoista ja asiantuntijoiden näkemyksistä. Tässä tutkielmassa asiantuntijahaastattelua hyödynnettiin samalla tavalla. Koin asiantuntijahaastattelun ja muut tapaamiset tietoturvajohtajan kanssa merkityksellisinä työntekijöiden haastattelujen toteuttamiselle, koska lentoala ja lentoalan tietoturva eivät olleet entuudestaan tuttuja. Posey ja kumppanit (2014) vertailivat tietoturva-asiantuntijoiden ja muiden työntekijöiden näkemyksiä tietoturvasta, mutta tässä tutkielmassa asiantuntijahaastattelua hyödynnetään vain organisaation nykyisen tietoturvakulttuurin ja -viestinnän kuvaamisessa tietoturvajohtaja Timo Laakson näkökulmasta.

## 5.4 Haastateltavat ja haastattelujen toteutus

Haastateltaviksi hain Finavian työntekijöitä mahdollisimman laajasti eri työtehtävistä, koska yksipuolinen vastaajajoukko ei pysty kuvaamaan kokonaisvaltaisesti

organisaation kulttuuria ja toimintatapoja. Mahdollisimman monipuolisella vastaajajoukolla pyrin mahdollistamaan tulosten yleistettävyyttä. Finavian työntekijöiden sähköpostilistoille ja intranettiin lähetettiin tiedote tutkimuksesta, joka sisälsi lyhyen kuvauksen tutkielmasta ja tutkimuksesta, motivoi osallistumaan sekä kuvasi henkilötietojen käsittelyä tutkimuksen aikana. Haastateltaville toimitettiin tutkimuksen suostumuslomake, tietosuojailmoitus ja tiedote tutkimuksesta. Suostumukset haastatteluun annettiin suullisesti tallenteelle. Työntekijät saivat vapaaehtoisesti ja omaaloitteisesti ottaa yhteyttä opinnäytetyön tekijään halutessaan osallistua haastatteluun. Otantaa voidaan kuvata satunnaisotannaksi, koska jokaisella työntekijällä oli yhtäläinen mahdollisuus osallistua tutkimukseen (ks. Tracy 2013, 133).

Vapaaehtoisia osallistui haastatteluihin yhteensä yhdeksän kappaletta ja näiden lisäksi toteutettiin asiantuntijahaastattelu tietoturvajohtaja Timo Laakson kanssa. Kaikki haastattelut toteutettiin etäyhteyksin Microsoft Teamsin välityksellä. Haastattelut tallennettiin myöhempää litterointia varten ja lisäksi tein muistiinpanoja haastattelun aikana. Haastattelujen kesto oli yhteensä 7 tuntia ja 10 minuuttia. Lyhyin haastattelu kesti 36 minuuttia ja pisin haastattelu 1 tunnin 10 minuuttia. Keskiarvoltaan haastattelut olivat noin 47 minuuttia. Viisi haastateltavaa luonnehti asemaansa johtajaksi tai lähijohtajaksi, kolme toimi alaisasemassa ja yksi haastateltava luonnehti olevansa vahvasti molempia. Haastateltavat työskentelivät lentoasemilla ympäri Suomea ja olivat olleet Finavialla töissä noin 1–20 työvuotta erilaisissa työtehtävissä, suorittavan työn tekijöistä tietotyöläisiin. Työtehtävät vaihtelivat haastateltavien mukaan esimerkiksi ”numeroiden pyörittelystä” isojen kokonaisuuksien hallintaan, sopimusten käsittelyyn ja asiakaspalvelutehtäviin. Suurin osa haastateltavista kuvaili työskentelevänsä pääosin tiimeissä tai vahvasti toisten työntekijöiden kanssa yhteistyössä, mutta myös itsenäistä työtä kuului osaksi jokaisen työnkuvaa.

Haastattelut käytiin keskustelunomaisesti, koska monet kysymyksistä vaativat havainnollistamista esimerkein. Microsoft Teams toimi sujuvana alustana haastatteluille ja haastateltavat tuntuivat myös olevan tottuneita etäyhteyksien käyttöön. Kaikki haastateltavat eivät halunneet laittaa web-kameraa päälle, mutta

haastattelijana pidin kamerani jokaisessa haastattelussa päällä. Teknologiavälitteistä haastattelua arvioidaan tarkemmin tutkielman arviointi -luvussa.

## 5.5 Aineiston käsittely ja analyysi

Tallennettu haastatteluaineisto litteroitiin tekstimuotoon analyysia varten. Litterointi tehtiin asiatarkasti, jolloin täytesanat ja toistot jätettiin litteroimatta. Lisäksi litteroimatta jätettiin haastattelujen alkuosuus, jossa haastateltavat kertoivat työkokemuksestaan ja työtehtävistään, joita käytettiin kuvaamaan haastateltavien monipuolisuutta tietoturvakulttuurin tarkastelun kannalta.

Litteroitua aineistoa tuli yhteensä 52 sivua (fontti Calibri, pistekoko 12 ja riviväli 1,5). Aineistosta välittyy monipuolisesti haastateltavien omakohtaisia käsityksiä ja kokemuksia tietoturvasta sekä siihen liittyvästä viestinnästä. Haastateltavat merkittiin aineistoon pseudonyymeillä H1 – H9.

Laadullisen aineiston analyysiin löytyy erilaisia lähtökohtia, mutta ei tiettyä mallia, jota täytyisi noudattaa; lähtökohdat ovat suuntaa antavia, mutta lopputulos riippuu aina tutkijan tulkinnoista (Patton 2015, 1033–1034). Analyysin tavoitteena on siis muuttaa haastatteluista saatu data löydöksiksi, tuloksiksi. Koska aineistosta tehtävät tulkinnat ovat subjektiivisia, pyrin avaamaan mahdollisimman tarkasti analyysiprosessia, ja eri päätöksiin yhteydessä olleita tekijöitä, jotta voin perustella pätevyyttäni tämän aineiston tulkitsijana.

Analyysin lähtökohdaksi valitsin piirteitä Glaserin ja Strausin (1967) Grounded theorysta ja Tracyn (2013) kuvaamasta iteratiivisesta analyysista. Analyysin tavoitteena on järjestää eli teemoitella haastatteludata. Tämä prosessi alkaa usein muodostamalla aineistosta ylätason kategorioita, joita lähdetään syventämään askel kerrallaan (Strauss & Corbin 1998, 19). Datan järjestämiseen yleinen keino on aineiston koodaaminen, joka käytännössä tarkoittaa aineiston tulkitsemista ja merkitsemistä.

Koodaus aloitetaan usein ylätason koodauksella, eli laajempien kokonaisuuksien merkitsemisellä, jonka jälkeen kokonaisuuksia aletaan pilkkoa yksityiskohtaisemmin alatason koodeilla (Tracy 2013, 186, 189, 194).

Analyysini on sekä deduktiivinen että induktiivinen. Patton (2015) kuvailee tätä lähestymistapaa analyyttiseksi induktioksi, jolloin analyysi alkaa usein deduktiivisesti ja jatkuu induktiivisesti. Deduktiivisessa analyysissa dataa analysoidaan taustateoriaan peilaten ja induktiivisessa analyysissa tutkija keskittyy puhtaasti aineistolähtöiseen datan järjestämiseen ja korostaa avointa lähestymistä dataan (ks. Braun & Clark 2006, 86; Patton 2015, 1079). Voidaan pohtia, että induktiivista analyysia ohjaa kuitenkin jossain määrin aina tutkijan aikaisempi tieto aiheesta. Aikaisemman tutkimuksen tai hypoteesien perusteella muodostetut haastattelukysymykset ohjaavat haastateltavan vastauksia, joten on oletettavaa, että myös vastauksia koodataan enemmän tai vähemmän perustuen aikaisempaan tietoon aiheesta. Joka tapauksessa analyysia voidaan kuvata Grounded theoryn mukaisesti aineistolähtöiseksi sisällönanalyysiksi, joka sisältää datan koodaamista ja teemoittelua.

Tracyn (2013, 184) kuvaaman iteratiivisen analyysin piirteitä ovat myös induktiivisen ja deduktiivisen analyysin yhdistäminen. Tracy korostaa, että aineistosta tulkittavia merkityksiä voidaan peilata aikaisemman tiedon ja tutkimuksen tavoitteiden mukaisesti. Voidaan pohtia, että Tracyn (2013) iteratiivisen analyysin mallin yhtenä tavoitteena on laajentaa käsitystä sisällönanalyysin monipuolisista toteuttamismahdollisuuksista, ja keventää Grounded theoryn (Glaser & Strauss 1967) tuomaa perustaa aineistolähtöiselle analyysille. Aineistolähtöinen analyysi on toimiva työkalu uuden käsitteen, kuten tietoturvaviestinnän tarkasteluun. Koska ilmiöstä ei vielä aikaisemman tutkimuksen perusteella tiedetä kaikkea, täytyy dataa lähestyä avoimesti ja antaa mahdollisuus uusien havaintojen löytämiseen.

Tämän tutkielman analyysin vaiheet ovat sovellettu Tracyn (2013) iteratiivisen analyysin vaiheista, joita ovat muun muassa aineistoon tutustuminen ja sen järjestäminen. Analyysi muodostui täten kolmesta vaiheesta:

1. Aineistoon tutustuminen
2. Aineiston koodaus
3. Aineiston teemoittelu

Analyysi alkoi tutustumalla aineistoon lukemalla sitä läpi ja merkitsemällä aineistoon alustavia ajatuksia sekä huomioita. Samalla tutkimuksen kannalta epärelevantit kokonaisuudet voidaan poistaa. Aineisto tuli tutuksi jo litterointivaiheessa, mutta sen läpikäynti toiseen kertaan mahdollisti analyysin seuraavassa vaiheessa, eli koodauksessa, yhtenäisempää merkitysten tulkintaa tekstiin merkittyjen havaintojen tuella. Analyysiyksiköksi valitsin merkityskokonaisuuden, joka on haastateltavan puheenvuoro tai puheenvuoron osa, kuten yksittäinen lause tai lausahdus.

Iteratiiviseen analyysin mukaisesti toteutin aineistolle kahden eri tason koodausta, eli ylätason ja alatason koodausta. Avoimet tutkimuskysymykset mahdollistivat merkityskokonaisuuksien induktiivista koodausta (Braun & Clark 2006, 84), mutta ylätason koodauksessa koodien nimeäminen pohjautui pääosin aikaisempaan tietoon aiheesta. Koodaus oli varsinkin alkuvaiheessa hyvin teorialähtöistä. Ylätason koodit ovat kuvailevia ja kertovat merkityskokonaisuuksien aihealueen, mutta eivät kuvaa vielä tarkemmin aineiston sisältämiä merkityksiä (Tracy 2013, 189). Ylätason koodeja jäsentyi yhteensä 20 kappaletta, joita olivat esimerkiksi Tietoturva työtehtävissä ja Viestintäkanavat. Toisella koodauskierroksella ylätason koodeja tarkennettiin ja järjestettiin uudelleen. Alatason koodeja jäsentyi yhteensä 59, joita olivat esimerkiksi Inhimillinen tekijä ja Tietoturvaviestinnän näkyvyys. Osa merkityskokonaisuuksista sai useampia ylätason ja alatason koodeja.

Ylätason ja alatason koodaus mahdollistivat aineiston systemaattisen järjestämisen teemoihin, joiden mukaan tämän tutkielman tulokset esitellään. Teemat muodostettiin tutkimuskysymysten ohjaamana, teoria- ja aineistolähtöisesti, vastaamaan tutkimukselle asetettuun tavoitteeseen. Teemoja muodostettaessa ylätason ja alatason koodeja yhdistettiin sekä järjesteltiin uudelleen muodostamaan yhtenäisiä

kokonaisuuksia. Yläteemoja muodostui yhteensä kolme, joista ensimmäinen Näkemyksiä tietoturvasta Finavialla sisältää kahdeksan alateemaa. Tämä kokonaisuus vastaa ensimmäiseen tutkimuskysymykseen ”Millaisia käsityksiä ja kokemuksia työntekijöillä on tietoturvasta Finavialla?” Kaksi muuta yläteemaa Tietoturvan johtamisviestintä ja Työyhteisön vuorovaikutuksen prosessit sisältävät kuusi ja kaksi alateemaa. Nämä kokonaisuudet vastaavat toiseen tutkimuskysymykseen ” Millaista tietoturvaviestintä on Finavialla työntekijöiden käsitysten ja kokemusten mukaan?” Ylä- ja alateemat ovat kokonaisuudessaan nähtävissä taulukossa 1.

**Taulukko 1 Analyysitaulukko**

| Tutkimuskysymys | Yläteema | Alateema |
|---|---|---|
| Millaisia käsityksiä ja kokemuksia työntekijöillä on tietoturvasta Finavialla? | Näkemyksiä tietoturvasta Finavialla | Tietoturvan monipuolinen määrittely |
| | | Tietoturva vaihtelevasti osana työtehtäviä |
| | | Positiivinen asennoituminen ja suhtautuminen |
| | | Koettu vastuu tietoturvasta |
| | | Motivaatiot toimia tietoturvallisesti |
| | | Toimintaympäristön edellytykset tietoturvalle |
| | | Tietoturvaa voidaan edistää |
| | | Tietoturva voi heikentyä |
| Millaista tietoturvaviestintä on Finavialla työntekijöiden käsitysten ja kokemusten mukaan? | Näkemyksiä tietoturvan johtamisviestinnästä | Monipuoliset viestintäkanavat |
| | | Vaihteleva viestinnän näkyvyys ja tiedon määrä |
| | | Tiedon ja ohjeistuksien saatavuuden haasteet |
| | | Viestinnän ymmärrettävyyden ja kohdentamisen haasteet |
| | | Toimivat tietoturvakoulutukset |
| | | Vähäiset vaikuttamismahdollisuudet |
| | Näkemyksiä työyhteisön vuorovaikutuksen prosesseista | Avoin vuorovaikutus ja sujuva yhteistyö |
| | | Aktiivinen tuen osoittaminen ja hakeminen |

# 6 TULOKSET

## 6.1 Näkemyksiä tietoturvasta Finavialla

Tämän tutkielman tavoitteena on kuvata ja ymmärtää tietoturvaviestinnän yhteyttä organisaation tietoturvakulttuurin rakentumiseen. Tässä luvussa tuloksia esitellään pureutuen Finavian työntekijöiden käsityksiin ja kokemuksiin tietoturvasta. Haastateltavien henkilökohtaiset näkemykset muodostavat suuntaa antavaa yleiskuvaa sen hetkisestä tietoturvakulttuurista Finavialla. Tulokset esitellään taulukossa 1 esiteltyjen teemojen mukaisesti. Tämän luvun tulokset vastaavat ensimmäiseen tutkimuskysymykseen ”Millaisia käsityksiä ja kokemuksia työntekijöillä on tietoturvasta Finavialla?” Yläteeman Näkemyksiä tietoturvasta Finavialla alateemoja ovat:

- Tietoturvan monipuolinen määrittely
- Tietoturva vaihtelevasti osana työtehtäviä
- Positiivinen asennoituminen ja suhtautuminen
- Koettu vastuu tietoturvasta
- Motivaatiot toimia tietoturvallisesti
- Toimintaympäristön edellytykset tietoturvalle
- Tietoturvaa voidaan edistää
- Tietoturva voi heikentyä

**Tietoturvan monipuolinen määrittely.** Tulosten mukaan haastateltavien näkemykset tietoturvasta Finavialla olivat monipuolisia ja osittain toisistaan poikkeavia. Suuri osa haastateltavista määritteli tietoturvaa henkilötietojen suojaamisena eli tietosuojan toteutumisena. Tietosuojan yhteydessä mainittiin usein GDPR eli EU-maissa sovellettava yleinen tietosuoja-asetus. Erityisesti tietoturvan määrittelyssä reflektoitiin matkustajatietoja ja niiden käsittelyä:

> H5: Miten mä lähden ensimmäisenä miettimään sitä niin onko meillä asiakastietoja, tiedetäänkö me henkilöiden, oli ne sitten matkustajia tai meidän käyttäjiä niin mitä tietoa

> henkilöistä meillä on siellä järjestelmässä eli se GDPR näkökulma tulee ensimmäisenä mieleen.

Muita tietoturvaan liitettäviä asioita olivat Finavian laitteiden ja järjestelmien teknologinen turvallisuus, tiedonhallinta ja inhimillinen tekijä. Inhimillinen tekijä määrittyi erään haastateltavan (H9) mukaan seuraavasti: ”osa tietoturvaa on ihmiset itse, että osataan tehdä sellai ettei tulis mitään tietoturvamurtoja ja ei tehä mitään hölmöilyjä, anneta salasanaa jollekkin Windows-soittajalle.” Laitteiden ja järjestelmien teknologisesta turvallisuudesta nostettiin esiin muun muassa virustorjunta, laitteiden turvallinen säilytys ja järjestelmien salasanat sekä Finavian tietotekninen tuki.

> H2: Suoraa sanottuna ensimmäisenä tietoturvasta tulee mieleen meidän atk-tuki ja service deskit. Se on niin kuin yhtä kuin tietoturva meillä. Toisaalta kaikki myös mitä me tehdään kännyköillä, tableteilla ja läppäreillä, niin yritetty (ryhmälle) sanoa ettei niitä (laitteita) jätetä sinne sun tänne ja tietysti kaikki nää salaukset on.

Haasteltavat kertoivat myös tiedonhallinnan, esimerkiksi dokumentoinnin ja tiedon säilyttämisen olevan osana tietoturvaa. Olennaista tiedonhallinnassa ovat tarkat prosessit ja hallinta, että millaisia laitteita ja ohjelmia voidaan käyttää. Tietoturva tunnistettiin myös osaksi kokonaisturvallisuutta ja asiaksi, jota erään haastateltavan (H2) mukaan täytyy ajatella, vaikkei se liittyisi suoraan työntekijän työhön. Myös toimintaympäristöllä todettiin olevan yhteys tietoturvaan, koska lentoasemalla käsitellään paljon sensitiivistä tietoa:

> H4: Mutta siis tottakai ollaan lentoasemalla töissä niin en osaa sanoa missä ne kriittisimmät kohteet on fyysisesti, mutta tosi sensitiivistä tietoa siellä välillä kulkee kun on kyse matkustajatiedoista ja muutenkin salaista tietoa.

**Tietoturva vaihtelevasti osana työtehtäviä.** Tulosten mukaan tietoturva oli vaihtelevasti läsnä arjen työtehtävissä. Työtilanteita, joissa tietoturvaa joudutaan miettimään, olivat haastateltavien mukaan henkilötietojen käsittely, salasananhallinta, fyysiset kulkuoikeudet organisaation tiloissa, huijausviestien ja -puheluiden tunnistaminen ja

niistä ilmoittaminen sekä tiedonhallinta. Eräs haastateltavista (H9) kertoi toimitusjohtajahuijauksesta, jossa ”toimitusjohtajalta tuli viesti, että pitää heti maksaa joku lasku.” Henkilötietojen käsittelyn lisäksi haastateltavien vastauksissa korostuivat myös fyysinen kulkeminen organisaation tiloissa, jota varten työntekijöillä on esimerkiksi henkilökortit työaikana näkyvissä:

> H3: No tottakai henkilökortti, se on hyvä että sellanen on, ja pitää olla näkyvillä aina. Kortti pitää olla että pystyy työskentelemään ja se tarkistetaan joka päivä ja periaatteessa ei pysty tulemaan töihin, jos ei ole henkilökortti mukana.

**Positiivinen asennoituminen ja suhtautuminen**. Tulosten mukaan haastateltavat kokevat tietoturvan todella tärkeäksi turvallisuuden osa-alueeksi Finavialla ja kokevat vastuuta tietoturvan toteutumisesta. Tietoturvan tärkeys tunnistettiin esimerkiksi lentoaseman toiminnan ja sensitiivisen tiedon kannalta. Tietoturvan merkitystä kuvailtiin itsestäänselvyydeksi, tärkeäksi asiaksi ja perusoikeudeksi. Asenteita tietoturvaan liittyvissä haasteissa kuvailtiin myös ratkaisukeskeisiksi. Toisaalta eräs haastateltavista (H2) kuvaili lähityöyhteisön asenteita yhdellä sanalla ”huolettomaksi, et varmaa jengi ei tietämättään, ei nyt tee hallaa, mut vois niiku ajatella sitä.” Kokonaiskuva asenteista tietoturvaa kohtaan on positiivinen ja sen merkitys tunnistetaan Finavian toiminnassa.

> H4: Kyllähän se on, koska väärät henkilöt pääsee käsiksi tietoihin niin aika paljon voi kyllä aiheuttaa ongelmia varsinkin jos miettii itse lentoasemaa ja matkustusta, lentokoneita. Äärettömän tärkeää että ne asiat on kunnossa.

Haastateltavat tunnistivat asenteista ja suhtautumisesta myös kehittämisen paikkoja. Eräs haastateltava (H5) kuvaili turvallisuutta osana Finavian toiminnan arvoja ja totesi, että tietoturvaa ei ole vielä yhtä vahvasti omaksuttu osaksi tekemistä kuin perinteistä turvallisuutta: ”Mitä se tietoturva sitten tarkottaa tekemisenä, niin se ei oo vielä lähimainkaan sellasta, että sitä ymmärrettäisiin.” Tulosten mukaan tietoturva saatetaan kokea työtehtävissä myös rajoittavana tekijänä, joka koitetaan ohittaa tai tehdä

sieltä mistä aita on matalin. Haasteltavan mukaan yksi keino muuttaa tätä ajattelua, olisi perustella miksi asiat täytyy tehdä tietoturvallisesti. Tietoturva tunnistetaan tärkeänä osana kokonaisturvallisuutta, mutta siitä voitaisiin keskustella aktiivisemmin.

> H5: Asenne on ehkä joissakin kohtaa semmonen, että se koetaan rajottavana, sillä tavalla että se voidaan ohittaa ja mennä siitä mistä aita on matalin, kun se koetaan niin hankalaksi. Auttaisko se, että käytäis läpi, että miksi näitä asioita kysytään, kun se koetaan vähän sellasena pakollisena ja rajottavana asiana?
>
> H4: Ihan tiedostaa, että nää asiat on tosi tärkeitä, mutta ei siitä nyt ole hirveesti ole ollut puhetta meidän osastolla.

**Koettu vastuu tietoturvasta.** Haastateltavien mukaan yksilöillä on vastuu tietoturvan toteutumisesta. Yksilön vastuuseen kuuluvat muun muassa oma käyttäytyminen ja ohjeiden mukaisesti toimiminen, tietoturvauhkien tunnistaminen ja ohjeiden vastaiseen toimintaan puuttuminen. Kaikki haastateltavat eivät kuitenkaan kokeneet vastuutaan yhtä merkittäväksi. Esimerkiksi eräs haastateltavista (H9) totesi, että ei ole ”tärkeä palanen tietoturvaa, mutta palanen kuitenkin” ja eräs toinen (H2) kuvaili vastuun olevan pääasiallisesti Finavian tietoteknisellä tuella: ”Tässä roolissa koen, että hirveesti ei oo tarvinnu ajatuksia siihen tietoturvaan laittaa tai kiinnittää huomiota, kun se se tulee tarjottuna ja hoidettuna talon toisen yksikön toimesta.” Kokonaisuutena vahva konsensus oli kuitenkin siitä, että vastuu kuuluu jokaiselle työntekijälle, vaikka tietoteknisen tuen rooli on merkittävä tietoturvan toteutumisessa:

> H1: Musta jokainen on vastuussa tietoturvasta, että se pysyy sillä tasolla millä sen pitää olla. Toimitaan niin kuin pitää eikä mennä kenenkään toisen tunnuksilla sitten tekemään jotakin… Tietysti vastuu on sillon jos menetellään vääriin niin mä otan asian esille.
>
> H5: …yritän olla matalalla kynnyksellä tietoturva-asioissa asiantuntijoihin yhteydessä heti jos havaitsen, että asia on juteltava niin koen, että se kuuluu mun vastuulle se huomata.

**Motivaatiot toimia tietoturvallisesti.** Tulosten mukaan tietoturvallisen toiminnan motivaatiotekijöistä yleisin on toisten työntekijöiden ja organisaation suojeleminen tietovuodoilta. Eräs haastateltavista (H1) mainitsi myös yleisen motivaation tehdä töitä Finavialla olevan yhteydessä myös motivaatioon toimia tietoturvallisesti. Tulosten mukaan myös lentoasema reguloituna toimintaympäristönä ohjaa tekemään asiat tietyllä tavalla, jolloin erään haastateltavan (H7) mukaan motivaatio ei ole merkittävä tietoturvallista toimintaa määrittävä tekijä. Seuraava esimerkki kuvaa työntekijän motivaatiota tietoturvalliseen toimintaan:

> H8: Jos on tietoa toisesta ihmisestä, niin että se ei pääsisi leviämään. Kun en haluaisi itsestäni mitään tietoja vuotavan, niin haluisin itsekin tehdä saman muille.

**Toimintaympäristön edellytykset tietoturvalle.** Tulosten mukaan lentoaseman reguloitu toimintaympäristö asettaa tiettyjä vaatimuksia toimintaan, joka on yhteydessä työntekijöiden tietoturvalliseen toimintaan. Haastateltavien mukaan tekeminen lentoasemilla on tarkasti ohjeistettua ja sääntöjä on totuttu noudattamaan, koska se on edellytys kaikelle toiminnalle. Tämä näkemys ylettyy myös tietoturvan kanssa toimimiseen. Haastateltavien näkemyksistä voidaan tunnistaa HRO (esitelty luvussa 5) -toimijan piirteitä, kuten ehdottomaan turvallisuuteen pyrkiminen. Erään haastateltavan (H3) mukaan ”jo rekrytilanteessa tehdään selväksi millaista käyttäytymistä työntekijöiltä odotetaan.” Tulosten mukaan ohjeistusten noudattamisen voidaan todeta olevan juurtunut tapa toimia lentoaseman toimintaympäristössä, joka on tietoturvakulttuurin rakentumista edistävä tekijä.

> H1: Lentoasematoimijat on yleensä hyvin reguloituja toimijoita, on paljon sääntöjä ja mennään hyvin kello aikataululla ja tosi tarkkaan ohjeistettua ja on hirveen tarkat speksit miten toimitaan ja miten mennään eteenpäin, niin ihmiset on tottuneet sellaiseen putkinäköön ja toteuttamaan niitä tehtäviä tietyn kaavan mukaan. Et jos olis vähän erityyppinen työnkuva niin voisi olla vaikeampi toteuttaa sitä tietoturvaa.

**Tietoturvaa voidaan edistää.** Haastateltavien mukaan tietoturvan toteutumista edistävät toimintaympäristön lisäksi tietoturvalliset laitteet ja järjestelmät, tietotekninen

tuki, viestintä ja koulutus. Tulokset osoittavat, että tietoturva säilyy parhaiten, kun töitä tehdään Finavian laitteilla ja tukea on saatavilla lähes ympärivuorokautisesti. Yhtenä isona teemana haastateltavien vastauksista ilmeni myös viestintä, johon liitettiin aktiivinen ja jatkuvaluontoisesti tapahtuva tiedottaminen sekä perustelut miksi asioita täytyy tehdä tietyllä tavalla. Erään haastateltavan (H3) mukaan tietoturva paranee, ”kun jokaisella työntekijällä on tieto tietoturvasta ja miten pitää toimia.” Viestinnällä voidaan myös yhteensovittaa merkityksiä tietoturvasta, jotta kaikki kokisivat tietoturvan yhtä tärkeäksi:

> H4: Mä luulen, että kaikkien organisaation henkilöiden tulisi ymmärtää sen tärkeyden ja kun tuli ihan konkreettinen tapaus, mitä voi tapahtua kun nää asiat ei oo kunnossa niin ihmiset sai sellasen hyvän esimerkin, se tuli jotenkin toiselle tasolle kun näki sen Vastaamon keissin. Että ei se oo vaan sitä paperisotaa ja niinku raskaita sopimusliitteitä vaan sillä on ihan oikea vaikutus. Se että pyritään informoimaan että ihmiset ymmärtää.

Koulutuksen ja tietoturvajohtajan aktiivisen toiminnan nähtiin myös edistävän tietoturvaa. Haastateltavan (H2) mukaan koulutus voisi olla esimerkiksi kerran vuodessa, jolloin koulutuksen suorittaja saisi tietoturvan ”ajokortin” aina vuodeksi kerrallaan. Tulosten mukaan verkkokoulutusten ei tarvitse olla pitkiä ja ne voivat olla myös tietoiskun tyylisiä. Koulutusten lisäksi myös tietoturvajohtajan rooli eräänlaisena sponsorina tai keulahahmona oli erään haastateltavan (H6) mukaan merkittävä. Hänen mukaansa tietoturva henkilöityy vahvasti tietoturvajohtajaan ja hänen tekemiseensä. Se, että tietoturvalla on näkyvät kasvot, nähtiin toimivan paremmin kuin ”kasvottomien” tiedotteiden tietoturvaan liittyen.

> H6: Tietoturva henkilöityy vahvasti tietoturvajohtajaan ja hänen tekemiseensä, hän on niin avomielinen ja jaksaa selittää ja vääntää rautalangasta, niin mä uskon että se levittää sellasta positiivista koko ympäristöön.

**Tietoturva voi heikentyä.** Haastateltavien näkemysten mukaan tietoturvaa heikentäviä tekijöitä ovat kiire ja inhimilliset tekijät. Haastateltava kertoivat kiireellä olevan merkittäviä vaikutuksia ja se voi johtaa monesti virheisiin tai muihin haasteisiin.

Kiireen nähdään olevan yhteydessä myös tietoturvaan liittyviin asenteisiin, koska tietoturva koetaan työtehtävän raskaana osuutena. Toiveena olisikin, että tietoturva-asioille annettaisiin enemmän aikaa ja rauhaa, ettei vahingossa tehdä virheitä tai huonoja päätöksiä:

> H4: No ehkä just omassa työroolissa, kaikessa *kuvailee työn tekemistä* on niin hirveä kiire, että ehkä se että hosutaan, ettei käytetä tarpeeks paljon aikaa sille että katotaan että asiat on oikeesti kunnossa, että monet ehkä ajattelee että se on se raskas osuus et pyritään saamaan nämä paperihommat että päästään alottamaan. Että vois antaa enemmän aikaa ja rauhaa sille työn teolle, ettei vahingossa sitten tuu huonoja päätöksiä tai jotain

Inhimilliset tekijät nostettiin esille tietoturvaa heikentävänä tekijänä. Työntekijät voivat haastateltavien mukaan olla välinpitämättömiä tai tietämättömiä, he voivat vahingossa ”jättää papereita väärään paikkaan tai lähettää tietoa väärään sähköpostiin” sekä olla ajattelemattomia. Lisäksi haastateltavat mainitsivat, että työntekijöiden yleinen tietotekninen osaaminen voi olla heikolla tasolla tai tietoturvaosaaminen ei ole omasta mielestä riittävää. Haastateltavan (H5) mukaan tilanteissa, joissa omaa osaamista ei koeta riittäväksi, voidaan ”säikähtää” tietoturvaan liittyviä työtehtäviä:

> H5: Välillä tulee sellaisia tilanteita, että henkilöt jotka ei oo vielä niin selvillä, niin ne säikähtää niitä että, se ohjeistus meidän asiantuntijoilta on liian pitkä tai se saahaan kuulostamaan kauheen pahalta, tai sillä tavalla että niille tulee sitten että ”iik pitäisikö mun tää osata ratkoa, enhän mä tiedä, miks mä kysyin, emmä pysty tätä…” Että ne jotenkin niiku pelästyy sitä asiaa.

**Yhteenvetoa.** Näkemykset tietoturvasta antavat yleiskuvaa Finavian tietoturvakulttuurista. Haastateltavien mukaan tietoturva koetaan tärkeäksi ja asenteet ovat yleisesti positiivisia tietoturvaa kohtaan. Yksilöt kokivat olevansa vastuussa tietoturvan toteutumisesta, vaikka Finavian tietoteknisen tuen rooli koettiin myös merkitykselliseksi. Käsitykset ja kokemukset tietoturvasta vaihtelivat eri henkilöiden välillä, mikä selittyy pitkälti omassa työtehtävässä tarvittavasta tietoturvaosaamisesta. Tietoturvakulttuurin rakentumisen näkökulmasta tietoturvaan liittyviä merkityksiä

kannattaisi yhtenäistää. Tietoturvaa edistäviä tekijöitä tunnistettiin monia, kuten aktiivinen viestintä ja tietoturvajohtajan rooli kulttuurin rakentamisessa. Tietoturvaa heikentäviä tekijöitä olivat kiire ja inhimillinen tekijä, jotka ovat osittain ristiriidassa asenteiden ja suhtautumisen kanssa. HRO:n rooli tietoturvan toteutumisessa ilmeni haastateltavien näkemyksissä, kun he kuvasivat lentoasematoiminnan luomaa toimintakulttuuria ohjeistusten noudattamisessa. Tulokset osoittavat, että lentoasema toimintaympäristönä ja turvallisuus juurtuneena arvona voivat edistää tietoturvakulttuurin rakentumista, mutta kehittämiskohteita löytyy silti.

## 6.2 Näkemyksiä tietoturvaviestinnästä Finavialla

Tämän luvun tulokset vastaavat tutkimuksen toiseen tutkimuskysymykseen ”Millaista tietoturvaviestintä on Finavialla työntekijöiden käsitysten ja kokemusten mukaan?” Tulokset ovat jaettu analyysin mukaisesti kahteen alalukuun 1. Tietoturvan johtamisviestintä ja 2. Työyhteisön vuorovaikutuksen prosessit.

### 6.2.1 Käsityksiä ja kokemuksia tietoturvan johtamisviestinnästä

Tässä alaluvussa tarkastellaan tietoturvaviestinnän kokonaisuudesta yläteemaa Tietoturvan johtamisviestintä ja esitellään tulokset seuraavien alateemojen mukaisesti:

- Monipuoliset viestintäkanavat
- Vaihteleva viestinnän näkyvyys ja tiedon määrä
- Tiedon ja ohjeistuksien saatavuuden haasteet
- Viestinnän ymmärrettävyyden ja kohdentamisen haasteet
- Toimivat tietoturvakoulutukset
- Vähäiset vaikuttamismahdollisuudet

**Monipuoliset viestintäkanavat.** Tietoturva-asioista viestimiseen käytetään haastateltavien mukaan monia viestintäkanavia. Käytettyjä kanavia olivat intranet,

sähköposti, Microsoft Teams, viestit puhelimeen ja kasvokkaisviestintä. Ensisijaisina tiedotuskanavina pidetään sähköpostia ja intranetin uutisia, mutta molemmista kanavista löytyy haastateltavien näkemysten mukaan haasteita. Intranet ei haastateltavien mukaan välttämättä tavoita koko henkilöstöä, koska kaikki eivät seuraa sitä aktiivisesti. Erään haastateltavan (H7) intranet on vain uutiskanava, ja tiedon tulisi löytyä myös muualta kootusti. Intranetissä voi myös kohdata vanhentuneita ohjeistuksia. Sähköpostin kohdalla huolena on, että yksittäinen tietoturvaviesti häviää tai hukkuu muiden sähköpostien sekaan, koska sähköposteja tulee työntekijöille paljon. Tärkeiden tietoturvatiedotteiden toivottiin tulevan joko sähköpostitse, puhelimeen viestinä tai Teamsissa järjestettävänä tiedotustilaisuutena.

> H9: Aina kun avaa selaimen niin tulee intran etusivu ja näkee jos on tullu uusia juttuja, esimerkiksi näistä huijausviesteistä. Varmastikaan kaikki ei avaa nettiä viikoittain, tai kuukausittainkaan.

> H3: Puhelin on hyvä ja olennainen ja jokaisella mukana lähes aina. Että puhelimeen kun tulee, jos kehitystä aattelee nii sillä tavalla vois kehittää. Varmasti tavottaa.

**Vaihteleva viestinnän näkyvyys ja tiedon määrä.** Tulokset osoittavat, että viestintä tietoturvasta ei haastateltavien mukaan ole kovin näkyvää tai aktiivista ja tiedon määrä tietoturvasta on vähäinen. Haastateltavan (H6) mukaan tietoturvasta viestitään lähinnä kerran vuodessa, kun muistutetaan suoritettavasta tietoturvakoulutuksesta. Muutama haastateltava muisteli nähneensä uutisia intrassa ja saaneensa sähköposteja liittyen erilaisiin huijauksiin viimeisen vuoden aikana:

> H9: Viimesen vuoden aikana on paljon muistuteltu erilaisista uhista intran puolella, että tämmösiä huijauksia on liikkellä. ET semmosta niiku tiedottamista on ollut.

> H6: Ei oikeen oo muita muistutuksia kun kerran vuodessa että tehkääs tämä tietoturvakoulutus. Sithän meille intrassa kulkee pikatietopaneeli niin voi olla että joku IT-ihminen siellä huutelee että nyt on tällasta liikkellä että katsokaas vähän.

Tietoturvaviestinnän näkyvyyden parantamiseen löytyi haastateltavilta myös kehitysehdotuksia. Sen sijaan, että tietoturvasta muistutetaan kerran vuodessa, olisi erään haasteltavan (H2) mukaan tiheämmin välein tulevat muistutukset parempi vaihtoehto. Tulosten mukaan tärkeitä tiedotteita voitaisiin korostaa väreillä tai tehdä niistä muulla tavoin erottuvia toisista uutisista esimerkiksi intranetissä. Tietoturvasta voitaisiin tiedottaa henkilöstöinfoissa, joissa haastateltavan (H9) mukaan ”toimitusjohtaja puhuu niitä näitä, ni jos sais vaikka laitettuu 5-10min jutun jossa joku mainitsis tietoturvasta niin se vois saavuttaa suuremman joukon ihmisiä.” Toisaalta tietoa on erään haastateltavan (H1) mukaan ”tarpeeksi” ja intranetissä uutiset ovat toisen haastateltavan (H4) kokemuksen mukaan ”bongattavissa.” Tulokset osoittavat, että tietoturvaviestinnän näkyvyydessä ja tiedon määrässä on kehitettävää.

> H2: Tietoturvaan liittyvää tietoa on ehkä sopivasti, se saattaa vähän hukkua sinne ku se tavallaa se syöte on samanlaista. Jos joku ois tietoturvaan liittyvä tiukempi viesti niin se kannattais jotenkin taustaväriks lyödä punanen et se vähän niinku hyppäis silmille sieltä valtavasta virrasta mitä tulee päivittäin.

> H6: Tässä organisaatiossa tietoa ei oikeen tule mitään kautta, että kaikki on alkanut sillä että mä oon kysynyt että mites tää homma ja mikä ohjeistus.

**Tiedon ja ohjeistuksien saatavuuden haasteet.** Haastateltavien kokemusten mukaan tiedon ja ohjeistuksien saatavuudessa oli vaihtelua. Erityisen haastavaksi tiedon löytäminen koettiin intranetissä. Erään haastateltavan (H4) kokemuksen mukaan tieto on kuitenkin helposti löydettävissä intrasta, jos osaa käyttää hakutoimintoa. Intranetissä haasteeksi koettiin navigointi intranetin sisällä ja ”oikeaan paikkaan” löytäminen. Seuraavat esimerkit havainnollistavat näitä vastakkaisia näkemyksiä:

> H4: Joo mun mielestä on helposti löydettävissä, että mun mielestä meillä on intrassa jopa omat sivut sille että kyl jos niinkun sen verran osaa kirjottaa tietoturva sinne hakukenttään nii löytää kaikki tarvittavat.

> H7: Se intrahan on siis ihan loputon suo, välillähän sieltä ei löydy dokumenttia vaikka tietää että se on olemassa. Jos haluaa tietoturvaan liittyvää tietoa löytää niin pitää osata etsiä se heidän sivunsa ja ymmärtää että heillä on myös oma työtila, ja mennä sinne.

Tulosten mukaan tietoturvaohjeistusten saatavuudesta ja löydettävyydestä oli eriäviä näkemyksiä. Moni haastateltavista ei osannut sanoa, ovatko he saaneet tietoturvaan liittyvää ohjeistusta, kun taas toiset haasteltavat kertoivat saaneensa useampiakin ohjeistuksia. Esimerkiksi etätyöhön liittyvän tietoturvaohjeistuksen oli saanut ainoastaan yksi haastateltava. Hän mainitsi, että ohjeistuksia etätyön tietoturvaan on annettua useampia ja ne ovat selkeitä sekä ymmärrettäviä. Haastateltavien näkemysten mukaan ohjeiden löytäminen tarvittaessa olisi myös haastavaa. Tulosten mukaan tietoturvaohjeistusten tulisi olla helpommin saatavilla. Seuraavat esimerkit havainnollistavat saatavuuden eroja:

> H1: On siitä etätyöstä tarkat ohjeet ihan mustaa valkosella, on nimenomaan sitä, että esimerkiksi että kaikki tiedonkäsittely pitää tapahtua sellasessa tilassa ettei muut käsiksi niihin tietoihin ja keskusteluihin mitä käydään esimerkiksi teamsin välityksellä. Selkeet ja ymmärrettävät ohjeet ja niitä toistetaan siellä meidän intranetissä, nyt on taas uudet etätyöohjeet ja samoja aiheita toistetaan tästä tietoturvasta.

> H: Kyl ne (tietoturvaohjeistukset) varmaan jostain jossain muodossa saattais löytyä, mutta nyt suoraansanottuna en tiedä. Meillä ei varsinaisesti meidän puolelle suunnattuja ohjeita missään ole ja mä väittäisin et ne ei ainakaan mun mielestä oo mitenkään helposti löydettävissä edes. Jos vertaa muihin kuten työterveyteen liittyviin asioihin, ne kyllä tuodaan ilmotustaululle, mutta tietoturvaan liittyen ei kyllä ole että se pistäs silmään. Se on selkee puute mun mielestä oikeestaan.

**Viestinnän ymmärrettävyyden ja kohdentamisen haasteet.** Haastateltavien kokemusten mukaan tietoturvaan liittyvän tiedon prosessoinnissa on vaikeuksia. Tietoturvaan liittyvät aiheet koetaan vaikeiksi ymmärtää. Ymmärryksen tueksi kaivataan käytännönläheisiä esimerkkejä sen sijaan, että käytetään suoria viittauksia lakitekstiin. Tulosten mukaan käytännön esimerkit madaltavat kynnystä asian esille ottamiseen, koska tietoturva-asiat voidaan ”helposti ohittaa, jos se koetaan liian

hankalaksi.” Monet ymmärrettävyyden haasteet haastateltavien kokemuksissa liittyivät GDPR:n soveltamiseen työssä. Haastateltavan (H5) mukaan GDPR koetaan jopa pelottavaksi, koska ”jos siitä kysyy meidän talossa ihan ydinasiantuntijoilta, niin sieltä tulee aikamoista vaikeeta kapulakieltä ja sitten se kysyjä jo halvaantuu siinä.” Tulokset osoittavat, että huono ymmärrettävyys voi pahimmillaan johtaa tietoturvan heikentymiseen.

> H5: Kun sähköpostilla kysyy, nii sit tulee vastauksena ihan kauheen pitkä viesti jossa viitataan jo heti artikloihin ja tämmösiin, nii ne halvaantuu ne kysyjät ihan totaalisesti että mitä tässä nyt pitikään tehdä.

> H2: Että kyllä siellä viestivirrassa on myös paljon sellasta tietoturvaan liittyvää mistä mä en niiku ymmärrä yhtään mitään ja tää ei niiku koske mun työtä, kun puhutaan jostain lähtöselvitystiskien jostakin… Niin mä en siis ymmärrä siitä mitään, muuta ku että se on tärkeä asia, mutta mä vaan pistän sen eteenpäin, koska menee liian yli ja ei varmasti koske mun työnkuvaa.

Haastateltavien mukaan tietoturvaviestintää kohdennetaan jonkin verran, mutta kohdennusta voisi ymmärrettävyyden kannalta tehdä enemmän. Haastateltavan (H5) mukaan ”on hyvin valikoituvaa, että kelle lähetetään ja millaista tietoa.” Intranetissä tietoturvaan liittyvä tieto on yleisluontoista ja kaikille suunnattua. Tulosten mukaan tietoturva-asioista viestiessä sama asia täytyy esittää ja puhua eri tavalla eri kohderyhmille, ottaen huomioon kohderyhmän osaamisen lähtötason. Kohdennuksen tulee tapahtua käytännön esimerkkien kautta, ”vaikka taustalla on artiklat ja säännöt.” Haastateltavien vastauksista käy selkeästi ilmi, että tiedon tarve on hyvin erilainen eri työntekijöillä:

> H6: kyl nimenomaan, että matti meikäläinen joka luo lunta nii ei tarvii oikeestaa muuta tietoa, kun sen miten omaa henkilökorttia käyttää ja muuta, mutta ei tarvitse välttämättä tietää että dokumenteilla on eri luottamuksellisuustasoja.

**Toimivat tietoturvakoulutukset.** Haastateltavat kertoivat osallistuneensa erilaisiin tietoturvakoulutuksiin vaihtelevasti. Suurin osa haastateltavista muisti

suorittaneensa verkossa tietoturvakoulutuksen ja kaksi haastateltavista oli myös suorittanut tietosuojaan liittyvän koulutuksen. Kaikki haastateltavat eivät kuitenkaan muistaneet suorittaneensa koulutuksia. Verkossa suoritettava tietoturvakoulutus sai paljon positiivista palautetta haastateltavilta, esimerkiksi ”vaikeat asiat oli osattu pilkkoa ja siinä oli hyviä käytännönläheisiä kysymyksiä, missä piti soveltaa teoriaosuutta.” Haastateltavat toivovat koulutusten jatkossa olevan myös verkossa tai tallenteena, jotta sen pystyisi tarvittaessa kertaamaan ja suorittamaan omassa tahdissa.

> H6: Toi on tosi toimiva, että ne voi itse käydä tekemässä sillon kun on aikaa. Eikä silleen että pitää mennä joku päivä istumaan johonkin koko päiväks ja työasiat polttaa takaraivossa koko ajan.

Haastateltavien mukaan tietoturvakoulutukset voivat lähtökohtaisesti olla verkossa, mutta myös mahdollisuutta keskustella interaktiivisesti koulutuksen aiheista toivotaan. Koulutusten sisältöihin toivotaan vaihtuvuutta ja kohdennusta, koska erään haastateltavan mukaan ”nää koulutukset on kaikissa organisaatioissa samanlaisia, niin mä klikkailin ite vanhasta muistista.” Lisäksi koulutukset voisivat sisältää esimerkiksi salattavan tiedon määrittelyä, salasananhallintaa ja tietoturvan teknologista puolta. Seuraavat esimerkit havainnollistavat haastateltavien kehitysideoita:

> H8: Mikäli yritys vaatii työntekijältä säännöllisin väliajoin tietoturva koulutuksen, niin koulutus pitäisi olla jotenkin poikkeavaa. Eikä vain että minäpäs klikkailen nämä taas läpi ja tuo dia ja miten tästä pääsee nopeasti läpi. Monipuolisuus antaisi paljon enemmän kuulijalle.

> H4: mua henkilökohtaisesti kiinnostaisi ymmärtää sitä (tietoturvan) teknistä puolta enemmän, et ei pelkästään sitä miten pitää toimia vaan niiku… mun mielestä olisi helpompi omaksua ne tietyt toimintatavat jos ymmärtää mitä se teknisesti tarkoittaa.

**Vähäiset vaikuttamismahdollisuudet.** Tulosten mukaan työntekijöitä ei aktiivisesti osallisteta päätöksentekoon organisaation tasolla, mutta toisaalta työntekijät eivät koe omaavansa valmiuksia tai tarvetta osallistua päätöksentekoon tai tietoturvan

liittyvien prosessien kehittämiseen. Haastateltavat arvioivat vaikuttamismahdollisuuksiaan vähäiseksi tietoturva-asioissa, koska he eivät koe omaavansa riittävää osaamista. Haastateltavat kuvailivat organisaation päätöksentekoa seuraavasti: ”Työntekijöiden roolina on ottaa vastaan uudet päätökset ja katsoa jälkikäteen toimivatko ne käytännön työssä.” Erään lähijohtajan mukaan työntekijöitä kannustetaan kehittämään toimintaa, koska ”kehitystä täytyy tapahtua.” Tulosten mukaan toiminnan kehittäminen lentoasemalla voi olla haastavaa, koska toiminta on vahvasti reguloitua ja asiat täytyy tehdä tietyn kaavan mukaisesti. Kaikki haastateltavat eivät olleet varmoja kenelle palautetta tulisi lähettää liittyen tietoturva-asioihin. Aktiivisesti palautetta pyydetään tietoteknisen tuen toiminnasta.

> H1: ja kannustan, esimerkiksi jos on jokin toimintatapa mikä tuntuu hullulta, niin jos keksitte paremman niin ehdottomasti mietitään sitä ja muutetaan toimintatapoja, ettei mennä aina vanhan mukaan vaan ideoidaan ja innovoidaan ehdottomasti. Ja ollaankin muutettu toimintatapoja parempaan suuntaan.
>
> H2: Aloteboksit on verkossa sun muuta ja jokasesta keikasta minkä tuki ottaa niin tulee palautepyyntö. Jonkun verran sitä (palautteen pyytämistä) on ehkä ollut.

### 6.2.2 Käsityksiä ja kokemuksia työyhteisön vuorovaikutuksen prosesseista

Tässä alaluvussa tarkastellaan tietoturvaviestinnän kokonaisuudesta yläteemaa Työyhteisön vuorovaikutuksen prosessit ja esitellään tulokset seuraavien alateemojen mukaisesti:

- Avoin vuorovaikutus ja sujuva yhteistyö
- Aktiivinen tuen osoittaminen ja hakeminen

**Avoin vuorovaikutus ja sujuva yhteistyö.** Haastateltavat kertoivat vuorovaikutuksen olevan avointa ja sujuvaa niin lähijohtajien ja alaisten välillä kuin kollegoiden välillä. Tulosten mukaan avointa vuorovaikutusta tukee lähijohtajien osallistuminen samoihin työtehtäviin alaisten kanssa. Tietoturva-asioista pystytään keskustelemaan ”matalalla kynnyksellä.” Haastateltavien mukaan työntekijät pystyvät myös

myöntämään virheensä ilman pelkoa rangaistuksesta ja pyytävät tarvittaessa apua. Eräs haastateltavista (H5) pohti, että mahdollisuuksia keskustella tietoturva-asioista ei välttämättä ole tarpeeksi ja lähijohtajat voisivat enemmän ohjata keskustelua myös tietoturva-asioiden tarkasteluun. Seuraavat esimerkit kuvaavat työyhteisön avointa vuorovaikutusta:

> H2: Kyllä, meillä on tota hyvä porukka ja hyvä esimies ja alaiset ja juttu luistaa. Työyhteisön sisällä keskusteluyhteydet molempiin suuntiin on älyttömän hyvät.

> H8: Näkisin että ihmiset aika hyvin pystyvät myöntämään virheensä ja pyytävät apua tarkastukseen.

**Aktiivinen tuen osoittaminen ja hakeminen.** Tulokset osoittavat, että työntekijät saavat tietoturva-asioissa tukea tarvittaessa ja lähijohtajat ovat valmiita olemaan tukena alaisilleen tietoturvaa koskevissa haasteissa oman osaamisen puitteissa. Tukea haetaan lähinnä Finavian tietoteknisestä tuesta soittamalla ja kysymällä apua. Yhdeksi tuen kanavaksi kuvailtiin myös suoraa yhteydenottoa tietoturvajohtajaan. Joitain epävarmuuksia yhteydenottoihin kuitenkin on. Seuraavat esimerkit havainnollistavat saatua tukea ja ilmennyttä epävarmuutta:

> H2: Omasta kokemusta, jos tietoturvan kanssa on tullut haasteita niin oon ottanut kännykän käteen ja soittanut tukeen ja he on sitten sen ratkassut ja homma on mennyt eteenpäin. Kun ei itsellä ole sillä tavalla sitä osaamista.

> H4: En oo ihan varma kuka olis se ja mitä kanavaa pitkin ja kuinka nopeesti et onks se sellanen et tietyissä tapauksissa se on tosi aikakriittistä vai riittääkö jos myöhemmin täyttää jonkin lomakkeen. Ois hyvä tietää että kuka henkilö se olisi kehen yhteyttä ottaa sitten.

**Yhteenvetoa.** Haastateltavat kuvasivat monipuolisesti tietoturvaviestinnän lähtökohtia Finavialla ja tarjosivat monia kehitysajatuksia. Tietoturvaviestintään käytetään eri viestintäkanavia monipuolisesti, mutta viestinnän ymmärrettävyyttä voidaan kehittää muun muassa kohdentamalla viestejä eri kohderyhmille. Haastateltavien mukaan tietoturvaan liittyvän viestinnän näkyvyydessä ja tiedon määrässä on kehitettävää,

samoin kuin tiedon ja ohjeistusten saatavuudessa sekä löydettävyydessä. Tietoturvakoulutuksiin on osallistuttu aktiivisesti ja verkkokoulutuksia kannatetaan myös jatkossa. Tietoturva-asioista voidaan keskustella avoimesti työyhteisössä ja tukea on saatavilla tarvittaessa. Epävarmaa oli kuitenkin joissain tilanteissa avun pyytäminen ja palautteen vastaanottajan valitseminen. Vaikuttamismahdollisuudet tietoturvaan liittyvissä muutoksissa koetaan vähäiseksi, joka selittyy osittain osaamisen ja tiedon puutteella. Seuraavassa luvussa esitellään täydennetty tietoturvaviestinnän kokonaisuus taustassa esitellystä aikaisempien tutkimusten perusteella muodostetusta kokonaisuudesta (kuvio 2) ja pohditaan miten tietoturvaviestintä rakentaa Finavian tietoturvakulttuuria. Pohdinnassa esitellään myös keinoja tietoturvaviestinnän kehittämiseen Finavialla ja jatkotutkimusmahdollisuudet.

# 7 POHDINTA

Tämän tutkielman tavoitteena on kuvata ja ymmärtää tietoturvaviestinnän yhteyttä organisaation tietoturvakulttuurin rakentumiseen. Psykoterapiakeskus Vastaamon tietomurto oli osoitus siitä, mihin huono tietoturva voi pahimmillaan johtaa. Teknologisten suojausjärjestelmien lisäksi ihmisten toiminnalla on merkittävä rooli tietoturvan toteutumisessa. Tässä tutkielmassa ihmiskeskeisen tietoturvan vahvistamiseen etsittiin mahdollisuuksia tietoturvakulttuurin lähtökohdista. Da Veigan ja kumppanien (2020) mukaan tietoturvallisesta toiminnasta tulee muodostua organisaation laajuisesti normaali ja luonnollinen tapa tehdä töitä, joka on yhteydessä työntekijöiden oletuksiin, arvoihin, uskomuksiin, tietoisuuteen ja asenteisiin sekä näkemyksiin tiedon turvaamisesta. Lähdin hakemaan ratkaisua näiden tekijöiden hallintaan viestinnästä, tietoturvaviestinnästä. Viestinnän avulla voidaan hallita työntekijöiden näkemyksiä ja merkityksiä, joita he tietoturvalle antavat. Tietoturvaviestinnällä voidaan myös lisätä työntekijöiden tietoisuutta ja osaamista, ja parhaimmillaan se rakentaa organisaation laajuista tietoturvakulttuuria. Arvioin seuraavissa luvuissa Finavian työntekijöiden näkemyksiä tietoturvasta ja tietoturvaviestinnästä, sekä havainnollistan tietoturvakulttuurin rakentumisen kannalta keskeisiä tekijöitä.

## 7.1 Tietoturvakulttuurin rakentumisen edistäminen

**Toimintaympäristön edellytykset tietoturvalle.** Tietoturvaosaaminen on kiinnostava osaamisalue organisaatioissa, koska jokaisella työntekijällä täytyy olla vähintään samantasoinen perusymmärrys ja osaaminen aiheesta. Tietoturvaosaamista voidaan verrata esimerkiksi perinteiseen työturvallisuuden osaamiseen, jossa kaikilla työntekijöillä olisi hyvä olla sama osaamisen ja ymmärryksen taso. Osaamisalueena tietoturva on organisaatioissa kuitenkin uudempi kokonaisuus ja se ei välttämättä ole juurtunut näkyväksi osaksi organisaation toimintaa. Tulosten mukaan Finavialla tietoturvan kanssa ollaan saman haasteen edessä, mutta suunta on oikea. Finavialla turvallisuus on kaiken toiminnan perusta ja edellytys, jonka yhtenä osa-alueena on

tietoturva (Finavia 2019). Tietoturvajohtaja Laakson ja haastateltavien vastauksissa korostuu lentoaseman toimintaympäristön etu tietoturvakulttuurin rakentumiselle: toiminta lentoasemilla on vahvasti laeilla säänneltyä ja reguloitua, joten työntekijät ovat tottuneet noudattamaan turvallisuuteen liittyviä ohjeita tarkasti, myös tietoturvan kohdalla. Toisaalta toimintaympäristön koettiin myös rajoittavan innovatiivisuutta ja kehitysmahdollisuuksia, koska asiat tehdään aina tietyllä tavalla. Sutcliffen (2011, 142) mukaan korkean luotettavuuden organisaatiot (HRO), kuten lentoasematoimijat, tavoittelevat turvallisuutta prioriteettina esimerkiksi kouluttamisen, oppimisen ja kannustimien keinoin. HRO toimijoilla on paremmat mahdollisuudet luotettavuuden saavuttamiseen vahvan turvallisuuskulttuurin ansiosta kuin muilla organisaatioilla. Voidaan todeta, että tietoturvakulttuurin rakentumisessa tulee ottaa huomioon organisaation toimiala ja toimintaympäristö, koska sillä on merkittävä yhteys turvallisuuteen liittyvien toimintakulttuurien lähtökohtiin.

**Tietoturvalle annetut merkitykset.** Haastateltavat määrittelivät tietoturvaa pääosin omien työtehtäviensä kautta, joten määritelmiä tietoturvalle oli yhtä monta kuin haastateltavia. Tietoturvasta tunnistettiin teknologisia sekä inhimillisiä tekijöitä, mutta monien haastateltavien vastauksissa tietoturva näyttäytyi tietosuojan toteutumisena. Voidaan pohtia, että kyberturvallisuuden, tietoturvan ja tietosuojan käsitteet saattavat helposti myös mennä sekaisin työntekijöillä. Nykyään puhutaan myös digitaalisesta turvallisuudesta. Käsitteiden eron hahmottaminen voi auttaa lisäämään ymmärrystä tietoturvasta Finavialla.

Kun rakennetaan jonkin tietyn organisaation tietoturvakulttuuria, tulisi tietoturvan määritelmä kohdistaa kyseisen organisaation toiminnan mukaisesti. Esimerkiksi tietoturvan standardien kohdalla on huomattu heikkoutena se, että ne ovat luonteeltaan liian geneerisiä eivätkä ota huomioon organisaatioiden monimuotoisuutta (Siponen & Willison 2009, 267). Näin ollen organisaatiossa olisi tarkoituksenmukaista määritellä tietoturvaa ja sen tavoitteita vahvasti omaan toimintaan peilaten ja yhtenäistää työntekijöiden merkityksiä tietoturvasta. Se miten tietoturvaa määritellään, on yhteydessä niihin tavoitteisiin ja arvoihin, joita tietoturvalle organisaatiossa

annetaan: mikäli tietoturvaa määritellään vain tietosuojan kautta, jättää se monia tietoturvan ulottuvuuksia pois päivittäisessä työssä. Toisaalta on myös tiedostettava, että tietoturvan tarpeet ovat eri työtä tekevillä erilaiset, mutta yleistä ymmärrystä tietoturvasta oman organisaation kontekstissa voidaan vahvistaa ja yhtenäistää. Etätyön aikana työn ja arjen tietoturvaosaaminen limittyvät kotioloissa, jolloin työstä saatu osaaminen vahvistaa myös vapaa-ajan tietoturvallista toimintaa.

**Asenteet ja suhtautuminen.** Tietoturvakulttuurin rakentumisen kannalta on olennaista tarkastella tietoturvaan liittyviä asenteita ja suhtautumista. Tietoturvallisen toiminnan tulisi olla vapaaehtoista ja itseohjautuvaa (Vroom & Von Solms 2004), jota positiivinen suhtautuminen tietoturvaan voi edistää. Kuten tulokset osoittavat, tietoturva koetaan tärkeäksi turvallisuuden osa-alueeksi ja yksilöt kokevat vastuuta sen toteutumisesta. Toimintaympäristö koettiin merkittäväksi myös asenteita ja suhtautumista ohjaavana tekijänä. Kun haastateltavia pyydettiin kuvailemaan työyhteisön asenteita ja suhtautumista, löysivät he muutamia kehittämisen kohteita. Osa saattaa kokea tietoturvan rajoittavana ja pakollisena asiana, tai suhtautua siihen huolettomasti. Huolettomuus ei itsessään ole huono asia, mutta se voi mahdollistaa inhimillisiä virheitä. Yhdeksi ratkaisuksi ehdotettiin parempien perustelujen viestimistä, jolloin raskailta tai pakollisilta tuntuvat toiminnot saisivat enemmän ymmärrystä työntekijöiltä. Barlowin ja kumppaneiden (2018) tutkimuksesta käy ilmi, että lyhyetkin perusteluviestit vahvistavat ohjeiden noudattamista, koska ne tukevat työntekijää tietoturvaa koskevassa päätöksenteossa.

Haastateltavat kuvasivat inhimillistä tekijää tietoturvaa heikentävänä ominaisuutena ja kuvasivat tilanteita, joissa tietoturva voi heikentyä johtuen työntekijöiden tietämättömyydestä, välinpitämättömyydestä tai huolimattomuudesta. Voidaan pohtia, mihin asti positiiviset asenteet ja suhtautuminen, ja se että tietoturvaa pidetään tärkeänä, heijastuvat työntekijöiden käytännön toimintaan. Tämän ajatuksen tarkasteluun voitaisiin hyödyntää perustellun toiminnan teoriaa (Theory of reasoned action) ja sen jatkeeksi kehitettyä suunnitellun toiminnan teoriaa (Theory of planned behavior) (ks. Azjen 1991, 181). Perustellun toiminnan teorian (Fishbein & Azjen 1975)

perusajatuksena on yksilön aikomus toteuttaa tiettyä toimintaa. Aikomukset muodostuvat motivaatiotekijöistä, jotka vaikuttavat yksilön toimintaan; motivaatiotekijät ovat indikaattoreita sille, kuinka kovasti yksilöt ovat valmiita yrittämään toteuttaakseen toiminnan. Mitä vahvempia aikomukset ovat, sitä todennäköisempää tietyn toiminnan toteuttaminen on. Toiminnan toteuttaminen riippuu usein myös muista tekijöistä, kuten mahdollisuuksista ja resursseista. Koetusta oman toiminnan kontrollista ja toiminnan aikomuksista voidaan suunnitellun toiminnan teorian mukaan ennustaa käytännön toimintaa. Esimerkiksi: jos kaksi yksilöä aikoo muodostaa vahvan salasanan, ja molemmilla on yhtä vahva aikomus tehdä niin, mutta toinen on itsevarmempi onnistumisestaan, muodostaa hän todennäköisemmin vahvan salasanan, kuin henkilö joka epäilee onnistumistaan tai osaamistaan. Suunnitellun toiminnan teorian (Azjen 1991) mukaan toimintaan ovat yhteydessä subjektiiviset normit (näkemykset siitä, onko toiminta hyväksyttyä työyhteisössä vai ei), koettu kontrolli omasta toiminnasta (kuinka helppoa tai vaikeaa toiminnan toteuttaminen on) ja asenteet toimintaa kohtaan.

Suunnitellun toiminnan teoriaa on sovellettu monissa tietoturvan toteutumista tarkastelevissa tutkimuksissa. Esimerkiksi Rocha Flores ja Ekstedt (2016) havaitsivat, että vahvat asenteet käyttäjän manipuloinnin vastustamiseksi ennustavat myös aikomuksia vastustaa sitä. Bulgurcu ja kumppanit (2010) osoittivat tutkimuksessaan, että työntekijöiden aikomukset noudattaa tietoturvaohjeistuksia vaikuttuvat asenteista, subjektiviisista normeista ja minäpystyvyyden kokemuksesta. Sommestad (2018) tarkasteli suunnitellun toiminnan teoriaa työryhmissä, ja löysi ryhmän yksilöiden omaavan samoja asenteita, subjektiivisia normeja ja koettua oman toiminnan kontrollia sekä aikomuksia tietoturvan toteuttamiseen. Näiden tulosten valossa voidaan todeta, että positiiviset asenteet tietoturvaa kohtaan heijastuvat myös vahvasti aikomuksiin ja käytännön toimintaan. Kuten tietoturvan vaikuttamisviestinnän kohdalla arvioin sanktioiden ja pelkoilmauksien käyttöä potentiaalisesti huonona ratkaisuna tietoturvallisen toiminnan muutoksessa, myös suunnitellun toiminnan teorian lähtökohdat tukevat sitä näkökulmaa, että muutosta tulisi tavoitella toiminnan lisäksi myös niissä asenteissa, arvoissa ja näkemyksissä, joita tietoturvalle asetetaan

yksilöiden, ryhmien ja yhteisöjen toimesta. Toisaalta erilaisia tuloksia on saatu kestävän kehityksen kontekstissa, jossa on huomattu, että aikomukset ja arvot eivät aina ennusta käytännön toimintaa: vaikka yksilöt ajattelevat toimivansa ympäristön hyväksi, todellisuudessa he eivät tee niin (Barr 2008). Selittäviä tekijöitä olivat esimerkiksi haluttomuus maksaa enemmän vihreistä tuotteista. Barr toteaakin, että fokus tulisi suunnata tunnistettuihin selittäviin tekijöihin, sen sijaan, että kehitetään yleistä tietoisuutta ja tarjotaan tietoa aiheesta, koska se ei välttämättä johda käytännön toiminnan muutokseen - myöskään tietoturvan kontekstissa (Chen, Ramamurthy & Wen 2015).

**Kiireen yhteys tietoturvan toteutumiseen.** Yhtenä tietoturvaa heikentävänä tekijänä mainittiin kiire tietoturvaa koskevien työtehtävien kohdalla. Kiireellä todettiin olevan merkittäviä vaikutuksia, jotka voivat johtaa virheisiin tai muihin haasteisiin. Kiire on ajankohtainen aihe tietoturvan kontekstissa. Vuosittain lokakuussa järjestettävän Euroopan kyberturvallisuuskuukauden teemana oli viime vuonna *Think Before U Click* (European Commission 2020), joka on vapaasti suomennettuna *ajattele ennen kuin klikkaat*. Kampanjan tavoitteena on lisätä tietoisuutta (awareness), ”promota” kyberturvallisuutta ja tarjota yksilöille sekä organisaatioille resursseja tiedon turvaamiseen.

Chowdhuryn, Adamin ja Skinnerin (2019) mukaan nykyajan työelämässä kiire on jatkuvasti läsnä, myös tietoteknisten laitteiden käytössä. Kiire voi aiheuttaa kognitiivista rasitusta ja stressiä, joka voi lopulta vaikuttaa yksilöiden toimintaan: yksilöiden tekemät päätökset aikapaineessa perustuvat todennäköisemmin totuttuihin tapoihin ja rutiineihin sekä automaattisesti käynnistyviin toimintamalleihin. Kuten tietojenkalastelun yhteydessä tiedetään, käyttäjälle pyritään luomaan kiireen tunne (Moinescu ym. 2019), jotta käyttäjä ei ehtisi ajatella *ennen kuin klikkaa*. Finavian tietoturvakulttuurin kannalta kiirettä tulisi tarkastella tietoturvaan liittyvien tehtävien ympärillä, ja yrittää löytää keinoja helpottaa ajallista painetta. Voidaan pohtia, että mitä tärkeämmäksi tietoturva koetaan työyhteisössä, sitä valmiimpia sille ollaan antamaan työaikaa. Tähän työkaluna voisi toimia aiemmin mainittu perusteluista viestiminen,

jolloin myös kiireessä tietoturvalle osattaisiin antaa resursseja sen toteuttamiseen. Kiire voi asettaa myös toiminnan arvoja ristiriitaan: työtehtävällä on kiire ja se tulee suorittaa nopeasti tiettyyn aikamääreeseen mennessä, mutta tietoturvan huolellinen toteuttaminen vie aikaa ja mahdollisesti viivästyttää palautusta. Kumpi tavoite on tärkeämpi, työtehtävän suorittaminen aikamääreeseen mennessä vai tietoturvan optimointi?

Tietoturvan toteutumisessa merkittävänä koetaan tietoturvalliset laitteet ja järjestelmät, tietotekninen tuki ja viestintä. Laitteiden ja tietojärjestelmien teknologinen turvallisuus voidaan nähdä itsestäänselvyytenä organisaatioille nykypäivänä, varsinkin yhteiskunnalle kriittisillä toimijoilla. Katseet tuleekin suunnata ihmiskeskeiseen tietoturvaan, jota tietoturvaviestinnällä voidaan edistää. Haastateltavat kuvasivat viestinnän mahdollisuuksia muun muassa perusteluiden viestimisessä ja merkitysten yhteensovittamisessa. Aktiivisen ja jatkuvaluontoisen viestinnän, kuten säännöllisten koulutusten, nähtiin myös edistävän tietoturvalle muodostettavia arvoja ja tavoitteita. Tietoturvan johtaminen on perinteisesti rakennettu kontrolliin pohjautuvaan malliin, jonka oletuksena on ihmisten toiminnan kontrollointi ja regulointi (Hedström, Kolkowska, Karlsson & Allen 2011, 383). Tietoturvaviestinnällä pystytään edistämään organisaation tietoturvakulttuuria, joka mahdollistaa kontrollin vähentämistä ja suuremman luottamuksen osoittamista työntekijöille. Kun työntekijöiden osaaminen ja tietoisuus kasvaa, ja heidän näkemyksensä ja asenteensa tiedon turvaamisesta vastaavat organisaation tavoitetilaa, keventyy myös organisaation johdon ja tietoteknisen/tai vastaavan tuen rooli tietoturvan toteutumisessa.

## 7.2 Tietoturvaviestinnän osa-alueiden vahvistaminen

Tässä luvussa täydennetään ja syvennetään tietoturvaviestinnän kokonaisuutta (ks. kuviota 2). Kokonaisuus täydentyy tuloksista tunnistettujen havaintojen perusteella, joita arvioidaan ja tarkastellaan tietoturvakulttuurin lähtökohtiin peilaten. Pohdinta käytännön sovellutuksista tarjoaa myös työkaluja Finavialle tietoturvakulttuurin

rakentamiseen tietoturvaviestinnän osa-alueita vahvistamalla. Ensin käydään läpi Tietoturvan johtamisviestinnän teemoja, jonka jälkeen tarkastellaan kokonaisuutena Työyhteisön vuorovaikutuksen prosessien kehittämistä.

### 7.2.1 Tietoturvan johtamisviestinnän kehittäminen

- **Tietoturvan muutosviestintä**
  - Tietoturvan muutosprosessien johtaminen
  - Työntekijöiden vaikuttamismahdollisuuksien kehittäminen

**Tietoturvan muutosprosessien johtaminen.** Tietoturvaviestinnän kokonaisuus hyötyy vahvasti muutosviestinnän lähtökohdista. Tietoturvaosaamisen ja -tietoisuuden kehittäminen on monissa organisaatioissa suhteellisen uusi osa-alue, jolla muutosta haetaan työntekijöiden käytännön toimintaan ja näkemyksiin tietoturvasta. Tulosten mukaan tietoturvajohtajan rooli muutoksen johtamisessa on merkittävä, koska tietoturvajohtajan aktiivinen toiminta voi edistää positiivisia asenteita tietoturvaa kohtaan. Tietoturvaa koskevat viestit voidaan myös kokea henkilökohtaisemmaksi, mikäli niille annetaan ”kasvot.”

Muutosta täytyy johtaa suunnitelmallisesti (ks. esim. Pádár, Pataki & Sebestyén 2017) ja monesti muutosprojektille valitaan ”sponsori” tai sponsoreita, joiden roolina on edustaa projektin tavoitteita ja arvoja kokonaisvaltaisesti sekä huolehtia tarvittavista resursseista (Harrison 1999; Schroeder 2015, 2). Sponsori eli muutoksen johtaja toimii linkkinä muutosprojektin ja organisaation välillä. Vastuita ovat esimerkiksi muutoksen hallinnan ja päätöksenteon suunnittelu, muutokselle tärkeiden toimijoiden tunnistaminen sekä toimijoiden osallistaminen. Muutoksen johtaja legitimoi muutosta ja omalla toiminnallaan levittää innostusta muutoksen toteuttamiseen. Muutokselle tarvitaan myös projektipäällikkö, jonka osaamisen vahvuudet ovat ihmisten kanssa toimimisessa, koska muutos vaatii luottamuksen rakentamista, toimijoiden aktivoimista ja motivointia. (Harrison 1999; Schroeder 2015.) Finavian organisaatiorakenteesta

riippuen, voidaan pohtia olisiko tietoturvajohtajan paikka myös tietoturvaan liittyvän muutoksen johtajana?

Harrisonin (1999, 8) mukaan johdon sitoutuminen muutokseen voi olla vastuussa jopa 50 prosenttisesti muutoksen sujuvasta onnistumisesta. Muutosjohtajat voivat viestinnällään osoittaa, että he ovat vastuussa projektista ja sen hallinnoimisesta, mutta myös osoittaa sitoutumista uusien toimintatapojen käyttöönottoon. Työntekijät täytyy vakuuttaa siitä, että uusi tapa on parempi tapa toimia. Harrison mainitsee työntekijöiden palkitsemisen olevan tärkeä elementti uusien toimintatapojen ja positiivisten asenteiden edistäjänä. ”Sponsorin” ja projektijohtajan lisäksi muutoksessa toimijoita voivat olla muutosagentit, jotka toteuttavat muutoksen käytännön tasolla, havaitsevat ongelmakohtia ja kehittävät uusia toimintatapoja (Pádár, Pataki & Sebestyén 2017, 802). Finavian tulisi tietoturvakulttuurin rakentamisessa ottaa huomioon muutoksen johtamisen ja muutosviestinnän lähtökohtia, eli suunnitelmallisesti johtaa tietoturvaan liittyviä muutosprojekteja.

**Työntekijöiden vaikuttamismahdollisuuksien kehittäminen.** Finavian työntekijät kokivat vaikuttamismahdollisuutensa vähäiseksi tietoturvaan liittyvässä päätöksenteossa. Hedströmin ja kumppaneiden (2011, 381) mukaan tietoturvan toteutumista edistää jatkuvaluontoinen palautteen hakeminen ja vastaanottaminen tietoturvan johdon ja työntekijöiden välillä. Työntekijät tulisi nähdä yhtenä parhaimmista lähteistä tietoturvaan liittyvien kehitysideoiden ja innovaatioiden löytämiseen. Työntekijöiden osallistaminen tietoturvan suunnitteluun ja toimintatapojen käyttöönottoon edistää tietoturvakulttuurin rakentumista. Hedströmin ja kumppaneiden (2011) tutkimuksessa työntekijöiden vaikuttamismahdollisuuksia perusteltiin mahdollisesti ristiriidassa olevien arvojen (esim. aikamääreet vs. huolellinen tietoturvan toteuttaminen) esiin tuomisen tärkeydellä. Osallistaminen mahdollistaa paremman tietoisuuden niistä arvoista, joita työntekijät ovat tietoturvalle asettaneet. Tietoturva koskettaa jokaista työntekijää, ylimmästä johdosta aina ruohonjuuritasolle asti.

Työntekijät kokivat, että osallistuminen tietoturvan kehittämiseen vaatisi enemmän osaamista ja ymmärrystä. Tästä voidaan päätellä, että kun työntekijöiden tietoturva-osaamista ja -tietoisuutta vahvistetaan, kokevat he olevansa valmiimpia osallistumaan tietoturvan kehittämiseen. Mutta kuten aiemmin osoitin, myös tietoturvaan liittyvät arvot ja asenteet ennustavat työntekijöiden tietoturvallista toimintaa. Työntekijöiltä voidaan hakea palautetta ja innovaatioita liittyen arvojen ja asenteiden kehittämiseen. Osallistaminen tukee muutoksen onnistumista (ks. Lewis 2006). Kun työntekijät kokevat mahdollisuuksia vaikuttaa ja tulla kuulluksi, sitoutuvat he muutokseen paremmin. Laakso kuvailee Finaviaa todella laajaksi ja kompleksiksi organisaatioksi, joten voidaan pohtia, että tietoturvakulttuurin rakentuminen tarvitsee niitä ajatuksia ja innovaatioita ruohonjuuritasolta, jossa käytännön työtä tehdään. Tietoturvan johdon vastuuna on tarjota työntekijöille mahdollisuus vaikuttaa. Lähijohtajat kuvailivat kannustavansa työntekijöitään toiminnan kehittämiseen aktiivisesti, ja kuuntelevat työntekijöiden kehitysideoita avoimesti.

- **Tietoturvakoulutukset**
  - Monipuolisuuden kehittäminen
  - Verkkokoulutusten suosiminen

Tietoturvakoulutukset saivat positiivista palautetta, ja niiden toivottiin jatkossakin olevan pääasiassa e-koulutuksina. Lisäksi toivottiin mahdollisuutta keskustella interaktiivisesti koulutuksen aiheista tarvittaessa. Koulutusten sisältöjen monipuolisuutta tai vaihtuvuutta voidaan edistää. Vaikka perusasiat tietoturvasta täytyy joka vuosi kerrata, kannattaa materiaalia päivittää, jotta se haastaa myös edellisenä vuonna koulutuksen tehneitä. Riippuen työtehtävästä, tietoturvan tarpeet ovat erilaiset. Koulutuksia voisi haastateltavien mukaan olla enemmänkin, ja esimerkiksi tietoturvan teknologista puolta halutaan ymmärtää inhimillisen puolen lisäksi.

- **Kampanjat, tiedotteet ja uutiset**
  - Näkyvyyden kehittäminen

Haastateltavien mukaan tietoturvaan liittyvän viestinnän näkyvyyttä ja tiedon määrää voidaan kehittää. Viestinnän toivotaan olevaan jatkuvaluontoista ja ”muistuttavaa.” Tärkeät tietoturvaan liittyvät viestit voidaan korostaa esimerkiksi värien käytöllä intranetissä tai muissa kanavissa. Lisäksi toivottiin, että tietoturvasta voitaisiin tiedottaa esimerkiksi henkilöstöinfoissa. Henkilöstöinfot voivat toimia yhtenä kanavana ehdotukseni mukaisen muutoksen sponsorin toiminnalle. Tietoturvajohtaja Laakson tavoitteena oli järjestää ”roadshow”, jossa tietoturvasta olisi käyty kertomassa eri yksiköissä. Tuloksiin peilaten myös tämä idea kannattaa toteuttaa, kun se on mahdollista.

- **Viestintäkanavat**
  - Kanavien roolien selkeyttäminen

Viestintäkanavien käyttö tietoturvaviestinnässä on monipuolista, mutta eri kanavien rooleja voisi selkeyttää työntekijöille. Laakson mukaan tietoturvasta viestimiseen hyödynnetään Intranettiä, jonka sisältöjä ovat ohjeet, dokumentit, tiedotteet, uutiset ja blogitekstit. Microsoft Teamsissa löytyy avoin kanava kyberturvallisuudelle, jonka tavoitteena on kehittää vuorovaikutteisuutta. Monipuolinen viestintäkanavien käyttö mahdollistaa sen, että henkilöstöä voidaan tavoittaa laajemmin. Haastateltavista harva oli tietoinen Microsoft Teamsin kyberkanavasta. Sähköpostissa ja intranetissä molemmissa haasteena on se, että tietoturvaan liittyvät viestit voivat hukkua muiden tiedotteiden sekaan. Teamsin kyberkanavaa voisi promota henkilöstölle, jotta tietoturvaan liittyvä tieto on saatavilla kokonaisuudessaan myös yhdestä kanavasta. Tärkeiden tiedotteiden toivottiin tulevan myös puhelimeen viestinä.

- **Ohjeistukset**
  - Tiedon löytämisen kehittäminen
  - Ohjeistuksien saatavuuden kehittäminen
  - Ymmärryksen ja kohdentamisen kehittäminen

Tietoturvaan liittyvien ohjeistusten ja tiedon saatavuudessa on haastateltavien kokemusten mukaan kehittämisen tarpeita. Haastateltavilla oli vastakkaisia näkemyksiä siitä, että kuinka hyvin tietoturvaan liittyvä tieto on löydettävissä ja hyödynnettävissä. Erityisen haastavaksi tiedon löytäminen koettiin intranetissä, josta saattoi löytyä myös vanhentuneita ohjeistuksia. Laakson mukaan tietoturvaohjeet pyritään rakentamaan työnkuvaan tai työtehtäviin, jotta erillisiä tietoturvaohjeita olisi mahdollisimman vähän. Viestinnällistä rakenteistumista kuvaavan CCO-näkökulman mukaan tekstit, kuten ohjeistukset, ilmentävät organisaation tavoitteita ja arvoja (ks. esim. Brummans, Cooren, Robinchaud & Taylor 2014). Tietoturvaohjeistusten saatavuus ja löydettävyys ovat yksi keino tietoturvaviestinnän kokonaisuudessa, jotka edistävät tietoturvakulttuurin rakentumista. Etätyön aikana on tärkeää, että etätyöläiset osaavat toimia ohjeistuksia noudattamalla tietoturvallisesti myös kotioloissa. Tiedon saatavuus, oikea-aikaisuus ja hyödyllisyys edistää työtyytyväisyyttä (Lewis 2006, 31).

Kuten tuloksista huomataan, tietoturvaviestinnän ymmärrettävyyttä voidaan parantaa esimerkiksi kohdentamalla viestejä eri kohderyhmille. Haastateltavat painottivat käytännön esimerkkien helpottavan ymmärtämistä, ja viittauksia lakipykäliin tulisi välttää. Tulosten mukaan kynnys ottaa yhteyttä asiantuntijoihin voi nousta, koska vastaukset saattavat olla vaikeasti ymmärrettäviä ja ”säikäyttää” tai ”halvaannuttaa” työntekijän. Voidaan pohtia, että työntekijät voivat kokea tietoturvallisen toiminnan vaikeammaksi kuin mitä se todellisuudessa on, mikäli tietoturvasta viestitään käyttäen vaikeita käsitteitä ja abstraktilla tasolla. Erityisesti tietosuojan kohdalla ymmärrettävyydessä koettiin parantamisen varaa. On kuitenkin tasapainoiltava sen kanssa, ettei asioita yliyksinkertaisteta, vaan sitten voidaan esimerkiksi kouluttaa työntekijää tarpeen mukaan. Tiedon tarve on erilainen eri kohderyhmillä, joka täytyisi ottaa huomioon tietoturvasta viestittäessä. Jotta kohdennusta voidaan tehdä, täytyy tuntea organisaation työntekijöiden tiedon ja osaamisen tarpeet. Tämä on taas yksi asia, joka puoltaa työntekijöiden vahvaa osallistamista tietoturvan kehittämiseen.

### 7.2.2 Työyhteisön vuorovaikutuksen prosessien kehittäminen

Haastateltavien kokemusten mukaan työyhteisön vuorovaikutus on avointa ja yhteistyö sujuvaa. Tietoturvaan liittyvistä asioista voidaan keskustella matalalla kynnyksellä. Haastateltavat olivat myös sitä mieltä, että työntekijät pystyvät myöntämään mahdollisesti tehtyjä virheitä tietoturvaan liittyen ja hakemaan tukea tarvittaessa. Useamman haastateltavan vastauksista oli huomattavissa se, että tietoturvaan liittyvistä asioista ei keskustella kovinkaan usein. Tämä voi johtua siitä, että haastateltavien työtehtävissä tietoturvaan liittyvät asiat eivät ole läsnä päivittäisessä työssä. Erään haastateltavan mukaan mahdollisuuksia keskustella tietoturvasta voitaisiin kuitenkin lisätä ja lähijohtajat voisivat ohjata keskustelua tietoturvan teemoihin. Laakso kertoo asiantuntijahaastattelussaan, että pienetkin infot tiimipalavereissa ovat osa tietoturvan kouluttamista. Tällaiset lyhyet muistutukset tai keskustelunavaukset tietoturvasta voivat edesauttaa haastateltavien toivetta siitä, että tietoturvaviestintä olisi jatkuvaluontoista.

Työntekijät eivät olleet täysin varmoja siitä, kehen tulee olla yhteydessä, mikäli halutaan antaa palautetta liittyen tietoturvaan. Kuten Hsu ja kumppanit (2015) toteavat, suositusten, palautteen ja huolien jakaminen auttaa johtoa kehittämään organisaation tietoturvakulttuuria. Työntekijöille tulisi olla selvää, että mitä kanavaa pitkin palautetta tai kehitysideoita voidaan välittää eteenpäin, ja kehen yhteyttä tulee ottaa erilaisissa tilanteissa. Laakso kertoi haluavansa jalkauttaa sellaista viestinnän mallia, että henkilöstö voisi ottaa yhteyden suoraan tietoturvatiimiin, ettei asiaa tarvitsisi käyttää monen eri henkilön kautta. Yhdeksi tietoturvaviestinnän tavoitteeksi Laakso mainitsee, että ihmiset kokisivat yhteydenoton tietoturva-asioissa ketteräksi, helpoksi ja avoimeksi. Tämän tutkielman tulokset tukevat Laakson tavoitetta, koska se edistää vastavuoroisuutta ja edistää työntekijöiden osallistamista. Työntekijöille täytyy vain selkeyttää yhteydenoton mahdollisuudet ja kanavat.

Lähijohtajat kertoivat olevansa valmiita tukemaan alaisiaan tietoturvaan liittyvissä asioissa ja tarvittaessa viemään asioita eteenpäin. Mikkolan (2020, 149) mukaan

sosiaalisella tuella on merkittäviä lopputuloksia työyhteisön vuorovaikutussuhteissa. Sosiaalinen tuki voi edistää päätöksentekoa ja ongelmanratkaisua, oppimista, työhyvinvointia ja palautteen antamista. Sosiaalisen tuen roolia lähijohtajien toiminnassa tietoturvan kontekstissa voidaan pitää olennaisena tekijänä kulttuurin rakentumisen kannalta. Sosiaalisella tuella voidaan vähentää työntekijöiden kokemaa epävarmuutta ja lisätä yleistä työhyvinvointia työpaikalla (Mikkola 2020), jonka tiedetään tukevan tietoturvallista toimintaa (ks. Kath ym. 2010). Lähijohtajien lisäksi tukea haetaan Finavian tietoteknisestä tuesta, joka sai paljon positiivista palautetta, muun muassa yhteydenoton vaivattomuudesta ja tehokkaasta avusta.

Monet tietoturvan vahvistamiseen liittyvät toiminnot eivät vaadi työntekijöiltä teknologisen ymmärryksen tai tuen tarvetta, ja monesti työntekijöiden toiminta on kiinni viestinnästä (Moody, Siponen & Pahnila 2018). Pohdin tietoturvakulttuurin rakentumiseen yhteydessä olevia tekijöitä, ja löysin tietoturvaviestinnästä monia keinoja työntekijöiden tietoturvaosaamisen, tietoisuuden, asenteiden ja arvojen vahvistamiseen. Tutkielman tavoitteena oli kuvata ja ymmärtää tietoturvaviestinnän yhteyttä organisaation tietoturvakulttuurin rakentumiseen. Tämä tavoite saavutettiin, mutta samalla tunnistan monia mahdollisuuksia jatkotutkimukselle. Koska tietoturvaviestinnän kokonaisuus on hyvin laaja, tulisi kokonaisuuden yksittäisten osa-alueiden merkitystä tietoturvakulttuurin rakentumiseen tarkastella yksityiskohtaisemmin. Yksityiskohtaisemman tarkastelun vaihtoehtoja kuvailen seuraavassa alaluvussa, jossa esittelen jatkotutkimusmahdollisuuksia.

## 7.3 Jatkotutkimusmahdollisuudet

Viestinnän tutkimus tarjoaa monipuolisia mahdollisuuksia tietoturvan vahvistamiseen organisaatioissa. Tässä tutkielmassa osoitettiin viestinnän vahva rooli tietoturvakulttuurin rakentumisessa, kuten työntekijöiden osaamisen ja tietoisuuden vahvistamisessa. Tietoturvaviestinnän käsitteen jäsentämisessä hyödynsin organisaatioiden viestinnällisen rakenteistumisen näkökulmaa, joka tarkastelee organisaatioiden

rakentumista viestinnässä ja vuorovaikutuksessa (ks. esim. Brummans ym. 2014; Valo & Mikkola 2020). CCO-näkökulmaa ja muita rakenteistumisen teoreettisia lähtökohtia voidaan tarkastella tietoturvan yhteydessä monipuolisemmin. Tämä tutkielma osoittaa, että ymmärrys niistä tekijöistä, jotka rakentavat ja muodostavat organisaatiota ja organisaation kulttuureja ovat olennaisia tietoturvan kontekstissa. Tiedon turvaamisessa onnistuminen on kiinni monista tekijöistä, joihin vaikuttamiseen organisaation tietoturvajohtaja tarvitsee muiden yksiköiden tukea. Esimerkiksi työntekijöiden kokonaisvaltainen hyvinvointi ei edistä ainoastaan tietoturvan toteutumista, vaan tehostaa myös muun työn tekoa vice versa. Vahvaa tietoturvakulttuuria voidaan ehkä jopa pitää yhtenä hyvinvoivan organisaation merkkinä.

Turvallisuuskulttuurin ja oppimiskulttuurin väliltä on löydetty vahvoja yhteyksiä (Littlejohn ym. 2015). Tietoturvan voidaan nähdä olevan organisaatioissa vielä asia, joka täytyy oppia. Toisaalta digitaalisen kehityksen myötä tietoturvaan liittyvä oppiminen tulee olemaan jatkuvasti läsnä. Työntekijöiden oppimista täytyy siis tukea ja vahvistaa. Haastateltavat kehuivat Finavialla suoritettavan e-learning tietoturvakoulutuksen pedagogisia ominaisuuksia ja kokivat sen olevan hyvä keino tietoturvakulttuurin rakentamiseen. Mutta jopa 70 prosenttia oppimisesta voi tapahtua näiden virallisten koulutusten ulkopuolella (Pfeffer & Sutton 1999). Tietoturvakoulutuksella on tärkeä rooli kulttuurin rakentumisessa, mutta olennaista on tarkastella myös muita oppimisen mahdollisuuksia ja sitä tukevia tekijöitä tietoturvan kontekstissa. Avoin viestintä ja vuorovaikutus mahdollistavat lähtökohtia oppimiselle (Littlejohn ym. 2015, 289). Oppimiseen ja oppivan organisaation käsitteeseen voidaan syventyä tietoturvan kontekstissa, ja täydentää oppimisen ulottuvuutta tietoturvaviestinnän kokonaisuudessa.

Tässä tutkielmassa esitelty tietoturvaviestinnän käsite kaipaa systemaattisempaa teoreettista pohjustusta ja arviointia. Jotta viestinnän roolia tietoturvan vahvistamisessa ja tietoturvakulttuurin rakentumisessa voidaan ymmärtää vielä paremmin, täytyy aiheesta tehdä systemaattisempaa kirjallisuuskatsausta. Kuten tiedämme, viestintää on tietoturvan kontekstissa tarkasteltu ainakin vaikuttamaan pyrkivän viestinnän

(Barlow ym. 2018; Siponen ym. 2020), opetus-, harjoitus- ja tietoisuusohjelmien (Chen, Ramamurthy & Wen 2015; Wilson & Hash 2003) ja tietoturvakulttuurin (Da Veiga ym. 2020; Vroom & Von Solms 2004) yhteydessä. Tämän tutkielman tiedonhaun aikana huomattiin, ettei viestinnän aikakauslehdistä löytynyt tietoturvaan keskittyvää tutkimusta, vaan pääosin viestintää oli käsitelty osana tietoturvan johtamisen tutkimusta. Näen näiden tieteenalojen limittyvän ja tarjoavan synergiaetua tietoturvan inhimillisten haasteiden ratkaisuun. Kaipaamme kuitenkin vielä lisää ymmärrystä jo tehdystä tutkimuksesta viestinnän osalta tietoturvan kontekstissa.

Tutkielmassa tietoturvaviestintä keskittyy pääosin tietoturvauhkien ennaltaehkäisyyn. Mainitsin tietoturvaviestinnän tavoitteista ennaltaehkäisyn lisäksi tietoisuuden siitä, miten tietoturvauhkan toteutuessa toimitaan. Tietoturvauhkien toteutuessa painotetaan resilienssiä (Tracey ym. 2017), joka tarkoittaa organisaation kykyä palautua ja sopeutua uhkan toteutuessa (ks. Kahan, Allen, George & Thompson 2009). Tietoturvaviestinnän olisi olennaista sisältää myös kriisiviestinnän osa-alue, jossa määriteltäisiin viestintää tietoturvauhkan toteutuessa, niin henkilöstölle kuin muille osallisille. Vastaamon tietomurron jälkeinen kriisiviestintä sai paljon kritiikkiä mediassa. Esimerkiksi Yle (Leinonen 2020) uutisoi Vastaamon tiedotusvirheistä ja huonosta kriisiviestinnästä. Vastaamon kaltaisissa tapauksissa kriisiviestintä ulkopuolisille on tärkeää, mutta myös omalle henkilöstölle viestiminen korostuu kriisitilanteissa.

Finaviallakin on siirrytty osittain etätyöhön koronapandemian aikana. Voidaankin pohtia, miltä osin tietoturvaviestinnän teknologiavälitteisyys vaikuttaa sen toteuttamiseen. Finavialla osa työntekijöistä tekee etätyötä, ja osa on paikan päällä. Organisaation hajautettu toiminta voi olla yhtenä tekijänä, jota tietoturvakulttuurin rakentumisen näkökulmasta tulisi arvioida tarkemmin. Esimerkiksi voidaan tarkastella lähijohtaja-alaissuhteita: onko tietoturvan teknologiavälitteinen johtaminen, kuten tuen osoittaminen, erilaista teknologiavälitteisesti kuin kasvokkaisviestinnässä? Tuoreessa viestinnän Pro gradussa (Eerola 2020) tarkastelee teknologiavälitteisen vuorovaikutuksen merkitystä hajautetun tiimin hyvinvoinnille. Tutkielman tulosten mukaan teknologiavälitteisyys asettaa tiettyjä haasteita hyvinvoinnin tukemiseen. Nämä

tulokset tukevat myös näkemystä siitä, että teknologiavälitteinen tietoturvaviestintä kaipaa arviointia ja täsmentämistä.

Johnston ja kumppanit (2015) löysivät epävirallisten sanktioiden, kuten kasvojen menettämisen kollegoiden edessä vahvaksi motivaatiotekijäksi tietoturvalliseen toimintaan. Tämän tutkielman tulokset osoittivat, että työntekijöiden motivaationa tietoturvalliseen toimintaan on muiden työntekijöiden tietojen turvaaminen, ja pelko tietovuodon aiheuttamisesta, joka vaikuttaisi myös muihin työntekijöihin. Työntekijät kuitenkin kokivat, että tietoturvaan liittyvistä virheistä uskalletaan ilmoittaa, näistä pelkoon perustuvista motivaatioista huolimatta. Olisi kuitenkin mielenkiintoista tarkastella, ilmoittavatko työntekijät kaikista virheistä avoimesti, vai punnitaanko ilmoittamisen hyötyjä tai haittoja, riippuen siitä kuinka vakava virhe on. Voidaan pohtia, että työyhteisön vuorovaikutuksen prosesseista löytyy monia tekijöitä, jotka edistävät tietoturvaan liittyvien virheiden ilmoittamista, mutta myös tietoturvan johtamisviestintä voi tukea työntekijöiden ilmoittamishalukkuutta. Kuten tutkielmassa aiemmin pohdittiin, sanktiot eivät välttämättä ole paras ratkaisu tietoturvan kehittämiseen.

Tietoturvaa on tarkastelu paljon keskittyen organisaatiotasolle. Tietoturva on kuitenkin yhä vahvemmin osana valtioiden kansallista turvallisuutta ja olemme koko ajan enemmissä määrin riippuvaisia teknologiasta. Kyberturvallisuutta ei voida eikä välttämättä kannata enää erottaa kokonaisturvallisuudesta täysin erilliseksi kokonaisuudeksi. Olisi merkittävää tarkastella, miten tietoturvaviestintää voidaan toteuttaa kansallisella tasolla. Suomen kyberturvallisuusstrategian (2019) mukaan yksi keino lisätä kansallista kyberturvallisuutta on viranomaisten, elinkeinoelämän ja kansalaisten tietoisuuden lisääminen. Tutkielman tulosten mukaan viestinnällä on merkittävä rooli tietoturvan toteutumisen kannalta. Viestinnän roolia tulee tarkastella ja täsmentää kansallisen digitaalisen turvallisuuden kontekstissa. Viestinnän tutkimuksen mahdollisuudet Suomen kansalaisten tietoisuuden, osaamisen ja asenteiden sekä arvojen kehittämiseen ovat monipuoliset, ja ehkä jopa tehokkain valinta.

# 8 ARVIOINTI

Tämän tutkielman arvioinnissa hyödynnän ja yhdistän Tracyn (2013) luokittelemaa kahdeksaa arviointikriteeriä sekä Straussin & Corbinin (2008) kymmentä arviointikriteeriä, joista osa on päällekkäisiä. Strauss ja Corbin (2008) huomauttavat, että arviointikriteerien valinta riippuu laadullisessa tutkimuksessa pitkälti siitä, millainen tutkimus on toteutettu. Näiden arviointikriteerien pohjalta jäsensin yhteensä kuusi kriteeriä, jotka soveltuvat tämän tutkimuksen arviointiin:

- Huomionarvoisuus ja merkityksellisyys
- Hyödyllisyys
- Luovuus
- Perusteellisuus
- Vilpittömyys
- Eettisyys

**Huomionarvoisuus ja merkityksellisyys.** Tracyn (2013, 231) mukaan tutkimuksen huomionarvoisuuteen yhdistyviä tekijöitä voivat olla merkityksellisyys, ajankohtaisuus ja kiinnostavuus. Huomionarvoisuutta vahvistaa uusien näkökulmien ja ajatusten esiin tuominen, jotka täydentävät tai haastavat olemassa olevia näkemyksiä.

Nostin tutkielmassa esille aiheen ajankohtaisuutta monessa yhteydessä. Hyödynsin uutisartikkeleita esimerkiksi Vastaamon tietomurrosta sekä Verizonin ja muiden toimijoiden vuosiraportteja tietoturvasta. Uutisten ja raporttien tavoitteena oli tehdä aiheesta henkilökohtaisempaa ja konkreettisempaa hyödyntämällä tosielämän esimerkkejä. Tuomalla muutosviestinnän osaksi tietoturvaviestinnän kokonaisuutta halusin osoittaa tietoturvan vahvistamisen olevan jatkuva muutosprosessi, joka on sidoksissa yhteiskunnan digitalisaatioon. Tietoturvaan liittyvä tutkimus on tällä hetkellä ehkä ajankohtaisempaa kuin koskaan aiemmin, mutta sama trendi jatkuu varmasti vielä vuosia, joten ajankohtaisuus aiheen ympärillä tulee myös säilymään. Aiheen merkityksellisyyttä pyrin perustelemaan tutkielman johdannosta alkaen,

vahvistamalla näkemystä viestinnän merkittävästä roolista tietoturvan toteutumisessa. Aikaisempaa viestinnän tutkimusta tietoturvan kontekstissa ei myöskään ole toteutettu, joten tämä tutkielma on avaus näiden tieteenalojen yhdistämiselle. Digitaalinen maailma ja fyysinen maailma jatkavat yhä syvempää yhdistymistä, jolloin tarve ymmärtää ihmiskeskeistä tietoturvaa digitaalisessa toimintaympäristössä korostuu. Tämä tutkielma tuo uuden näkökulman tämän ymmärryksen lisäämiseen.

**Hyödyllisyys.** Hyödyllisyyttä arvioitaessa tarkastellaan tutkimuksen tulosten sovellettavuutta käytännön toimintaan, eli voidaanko tulosten pohjalta esimerkiksi kehittää toimintatapoja tai lisätä asiantuntemusta (Strauss & Corbin 2008).

Tutkielma toteutettiin yhteistyössä Finavian kanssa ja tavoitteena oli, että tutkielman tuloksia voidaan hyödyntää Finavian tietoturvan vahvistamiseen. Tutkielma tarjoaa Finavialle monia mahdollisuuksia kehittää tietoturvaviestintää tukemaan tietoturvakulttuurin rakentumista. Tutkielman tuloksia voidaan hyödyntää myös laajemmin eri organisaatiossa, muuallakin kuin Finavialla. Tutkielma tuo esiin uusia lähtökohtia tietoturvan tarkasteluun, joita tietoturva-asiantuntijat voivat tarkastella ja jatkokehittää tietoturvan asiantuntemuksen vahvistamiseksi. Tutkielman sisältö ja tulokset ovat sekä teoreettisesti että käytännöllisesti hyödyllisiä.

**Luovuus.** Arviointikriteerinä luovuus tarkastelee tutkimuksen innovatiivisuutta ja luovuutta aiheen valinnassa (Strauss & Corbin 2008). Tutkimuksen tulee lähtökohtaisesti tuottaa uutta tietoa.

Viestintää on tarkastelu osana tietoturvan johtamista ja tietoturvakulttuurin rakentumista, mutta viestintää ja vuorovaikutusta ei ole kokonaisvaltaisesti tarkasteltu tietoturvan toteutumisen edellytyksenä. Tämä tutkielma osoittaa innovatiivisuutta ja luovuutta uuden käsitteen, tietoturvaviestinnän, jäsentämisessä ja soveltamisessa käytännön toiminnan kehittämistä varten. Tieteenaloja yhdistävä tutkimus osoittaa ymmärrystä eri ilmiöiden yhteisestä rajapinnasta ja luovuutta niiden yhdistämisessä

uuden tiedon tuottamiseksi. Pidän tätä tutkielmaa ennen kaikkea luovan työn prosessina.

**Perusteellisuus.** Tracyn (2013, 231–232) mukaan perusteellisuutta arvioitaessa tarkastellaan tutkimuksen tieteellistä ja huolellista toteutusta. Toteutukseen liittyvässä arvioinnissa kuvaillaan esimerkiksi aineiston riittävyyttä ja soveltuvuutta, haastattelujen toteuttamista ja aineiston analyysin perusteellisuutta.

Organisaation kulttuurin tarkastelu vaatii monipuolisia näkemyksiä organisaation eri tasoilta ja eri työtehtävistä. Tutkielman laajuuteen nähden yhdeksän haastattelua oli sopiva määrä ja lisäksi haastateltavien vastaukset eivät tuottaneet viimeisissä haastatteluissa merkittävästi uutta tietoa, eli saturaatio saavutettiin aineiston osalta. Kaikkien haastateltavien löytämiseen meni kuitenkin paljon aikaa, johon saattoi vaikuttaa Finavialla käynnissä olleet laajat lomautukset ja YT-neuvottelut. Toisaalta tietoturva voi myös aiheena olla sellainen, ettei se innostanut osallistumaan. Kuten tutkielman tuloksista käy ilmi, ei tietoturva ole aktiivisesti läsnä kaikkien työssä ja tietoturvaan liittyen koetaan epävarmuuksia. Haastatteluun osallistuneet vapaaehtoiset saattoivat edustaa sellaisia työntekijöitä, joilla tietoturva oli aktiivisemmin osana työtehtäviä tai kiinnostus aiheesta oli suurempaa. Täytyykin pohtia, edustivatko haastateltavat tarpeeksi laajasti organisaation työntekijöitä, jotta tietoturvakulttuuria voidaan arvioida yleistävästi. Tavoitteena ei tosin ollutkaan yleistää tuloksia, vaan tuoda esiin työntekijöiden käsityksiä ja kokemuksia. Haastateltavien joukko oli monipuolinen ja aineisto oli rikasta, mutta Finavian kokoisessa organisaatiossa he ovat edustaneet hyvin pientä osaa työntekijöistä.

Kaikki haastattelut toteutettiin teknologiavälitteisesti Microsoft Teamsissa. Haastattelut sujuivat hyvin ja teknologisilta haasteilta vältyttiin. Tracyn (2013, 165) mukaan teknologiavälitteiset haastattelut vähentävät nonverbaalisten vihjeiden havainnointia, joka voi heikentää merkitysten tulkintaa. Kaikki haastateltavat eivät pitäneet päällä web-kameraa haastattelujen aikana, joten monesti haastattelin pelkän äänen

varassa. Tutkimuksen tavoitteen kannalta nonverbaaliset vihjeet eivät kuitenkaan olleet merkittävässä asemassa, joten en koe sen vaikuttaneen kerättyyn dataan.

Toteutin analyysin hyödyntäen laadullisen sisällönanalyysin monipuolisia lähtökohtia, sen sijaan että olisin toiminut vain yhden lähteen varassa. Kuvasin analyysin vaiheet selkeästi ja tiiviisti. Toteutin aineiston koodauksen ja teemoittelun huolellisesti, kirjallisuudessa kuvattuja malleja noudattaen. Annoin tilaa aineiston induktiiviselle tulkinnalle ja tunnistin oman positioni aineiston tulkitsijana.

**Vilpittömyys.** Vilpittömyydellä tarkoitetaan laadullisen tutkimuksen avointa ja rehellistä arviointia tutkimuksen aitoudesta, tutkijan tavoitteista, mahdollisista virheistä ja toiveista. Vilpittömyydessä yhdistyy tutkijan itsereflektio ja läpinäkyvyys. (Tracy 2013, 233.)

Tutkielman tekeminen on ollut yli vuoden kestävä oppimisprosessi, jonka aikana olen oppinut tietoturvasta ja sen tutkimuksesta paljon. Ennen tutkielmaa käsitykseni tietoturvasta olivat vielä suppeita. Pohdinkin tutkielman aikana, että olisinko valinnut aiheen toisin, jos olisin tiennyt alkuvaiheessa saman verran kuin nyt. Jossain määrin tietämättömyys aiheesta on mahdollistanut sen, ettei minulla tutkijana ollut monia ennakko-oletuksia tai vahvoja näkemyksiä, jotka olisivat ohjanneet tutkimuksen tekemistä. Toisaalta alun suppea käsitys tietoturvasta on voinut vaikuttaa siihen, että kokonaisuudesta on voinut jäädä jotain merkityksellistä ulkopuolelle. Yhteistyö Finavian kanssa ei vaikuttanut tutkimuksen tavoitteisiin tai toteuttamiseen, koska yhteistyö liittyi vain aineiston keruuseen. Aloite yhteistyölle ja aiheelle tuli puhtaasti tutkielman tekijältä. Tietoturvan ihmiskeskeinen tarkastelu oli luontainen valinta, koska viestintä tutkimusalana tarkastelee ihmisten sosiaalista toimintaa. Miten tutkimusta tehdään ja mikä viestinnän ja vuorovaikutuksen rooli on organisaatioiden toiminnassa, on vahvasti vaikuttunut viestinnän alan opinnoista omaksutuista arvoista. Pidän tätä kuitenkin tämän tutkielman kohdalla vahvuutena, koska se on mahdollistanut tietoturvan tarkastelun viestinnän linssin läpi.

**Eettisyys.** Tutkimuseettinen neuvottelukunta (TENK) (2012) on määritellyt tutkimuseetiikan näkökulmasta keskeisiä lähtökohtia eettisyyden arviointiin. Näitä ovat muun muassa tiedeyhteisön tunnistamien toimintatapojen mukainen toiminta, johon kuuluu esimerkiksi viittausten hallinta, tutkimuslupien hankinta ja tietoaineistojen vaatimusten mukainen hallinta. Tracyn (2013, 243–245) mukaan eettisyyttä voidaan arvioida seuraavia seikkoja tarkastellen: tutkimus ei aiheuta osallistujalle haittoja, tutkimuksesta on informoitu haastateltavia riittävästi, haastateltavien oikeudet tietosuojaan taataan ja haastateltavien kohdalla noudatetaan avoimuutta, rehellisyyttä ja kunnioitusta.

Tutkielman toteuttamisen osalta olen noudattanut yleisiä viestinnän Pro gradun ohjeita, hakenut aktiivisesti palautetta tutkielman ohjaajalta ja hyödyntänyt palautetta aktiivisesti. Erityisen tarkkana olen ollut haastatteluaineistojen säilytyksessä ja haastateltavien tietosuojan takaamisessa. Osallistuminen haastatteluun oli vapaaehtoista ja jokainen haastateltava antoi suostumuksensa suullisesti tallenteelle. Informoin tutkimuksesta haastateltavia ennen haastatteluun osallistumista ja jokaisen haastattelun alussa. Jokaisella haastateltavalla on ollut mahdollisuus ottaa yhteyttä tutkijaan tarvittaessa. Tutkimukseen osallistuminen ei aiheuttanut haittaa osallistujille ja haastattelut pidettiin haastateltaville sopivina ajankohtina. Haastateltavat olivat edellytys tutkielman toteuttamiselle, joten toimin heidän kanssaan rehellisesti ja kunnioittavasti, heidän lähtökohtansa etusijalla. Haastatteluissa olin kannustava ja ymmärtäväinen, koska aihe ja osa kysymyksistä saattoivat olla haastavia reaaliaikaisessa haastattelutilanteessa. Painotin, etten ole etsimässä oikeita vastauksia, vaan haluan kuulla heidän henkilökohtaisia käsityksiä ja kokemuksia aiheesta.

## KIRJALLISUUS

Abawajy, J. 2014. User preference of cyber security awareness delivery methods. Behaviour & Information Technology 33 (3), 237-248.

Ajzen, I. 1991. The Theory of Planned Behavior. Organizational behavior and human decision processes 50 (2), 179.

Albrechtsen, E. 2007. A qualitative study of users' view on information security. Computers & Security 26 (4), 276-289.

Ansari 2020. How Microsoft is transforming its approach to security training. Microsoft 19.2.2020. Saatavana: https://www.microsoft.com/itshowcase/blog/how-microsoft-is-transforming-its-approach-to-security-training/ [viitattu 19.4.2020]

Barlow, J., Warkentin, M., Ormond, D. & Dennis, A. 2018. Don't Even Think About It! The Effects of Antineutralization, Informational, and Normative Communication on Information Security Compliance. Journal of the Association for Information Systems 19 (8), 689-715.

Barr, S. 2008. Environment and society : sustainability, policy and the citizen. Aldershot, England ; Burlington, VT: Ashgate. Ashgate studies in environmental policy and practice.

Baxter, L. A. 2004. Relationships as dialogues. Personal Relationships 11 (1), 1-22.

BBC. 2014. Edward Snowden: Leaks that exposed US spy programme. BBC 17.1.2014. Saatavana: https://www.bbc.com/news/world-us-canada-23123964 [viitattu 6.4.2021]

Berger, P. L. & Luckmannn, T. 1967. The social construction of reality: A treatise in the sociology of knowledge. Open Road Media.

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.

Brummans, B., Cooren, F., Robichaud, D. & Taylor J. R. 2014. Approaches to the communicative constitution of organizations. Teoksessa Putnam, L. L. & Dennis, K. M. The Sage hanbook of organizational communication, 173-194. Thousand Oaks, California: SAGE Publications, Inc.

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.

Bureau, S. 2017. Human-centered cybersecurity, a new approach to securing networks. States News Service.

Cain, A. A., Edwards, M. E. & Still, J. D. 2018. An exploratory study of cyber hygiene behaviors and knowledge. Journal of information security and applications 42, 36-45.

Calvin, N. 2018. Botching Human Factors in Cybersecurity in Business Organizations. Holistica : Journal of business and public administration, 9(3), 71-88

Chen, Y., Ramamurthy, K. & Wen, K. 2015. Impacts of Comprehensive Information Security Programs on Information Security Culture. The Journal of computer information systems 55 (3), 11-19.

Chmura, J. 2016. The impact of positive organisational culture values on information security management in the company. Journal of Positive Management 7 (1), 87-98.

Chowdhury, N. H., Adam, M. T. P. & Skinner, G. 2019. The impact of time pressure on cybersecurity behaviour: A systematic literature review. Behaviour & information technology, 38(12), 1290-1308.

Clarke, V. & Braun, V. 2017. Thematic analysis. The journal of positive psychology 12 (3), 297-298.

Cooper, M. D. 2000. Towards a model of safety culture. Safety Science 36 (2), 111-136.
Corbin, J. M. & Strauss, A. L. 2008. Basics of qualitative research : techniques and procedures for developing grounded theory. (3e [ed.] edition) Los Angeles, Calif. ; London: SAGE.

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

Da Veiga, A., Astakhova, L. V., Botha, A. & Herselman, M. 2020. Defining organisational information security culture—Perspectives from academia and industry. Computers & Security 92.

D'Arcy, J. 2014. Security culture and the employment relationship as drivers of employees' security compliance. Information Management & Computer Security 22 (5), 474-489.

Eerola, S. 2020. Työvointia edistävä ja heikentävä vuorovaikutus hajautetussa tiimissä. Jyväskylän yliopisto, viestintätieteiden laitos. Maisterintutkielma.

Egutkina, A. 2020. Asiantuntija kertoo: näin helposti Vastaamon tietomurto olisi ollut estettävissä. MTV uutiset 22.10.2020. Saatavana: https://www.mtvuutiset.fi/artikkeli/asiantuntija-kertoo-nain-helposti-vastaamon-tietomurto-olisi-ollut-estettavissa/7962838 [viitattu 6.4.2021]

European Commission 2020. EU data protection rules. Saatavana: https://ec.europa.eu/info/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules/eu-data-protection-rules_en [viitattu 19.4.2020]

Europol. 2020. Internet organized crime threat assessment. Saatavana: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020 [viitattu 6.4.2021]

Finavia, 2020. Helsinki-Vantaa on yksi maailman kyberturvallisimmista lentoasemista. Saatavana: https://www.finavia.fi/fi/uutishuone/2020/helsinki-vantaa-yksi-maailman-kyberturvallisimmista-lentoasemista [viitattu 3.5.2020]

Finavia. 2019. Vastuullisuusraportti. Saatavana: https://www.finavia.fi/sites/default/files/2020-03/Vastuullisuusraportti_0.pdf [viitattu 6.4.2021]

Finavia. 2020. Turvallisuus Finaviassa. Saatavana: https://www.finavia.fi/fi/tietoa-finaviasta/vastuullisuus/turvallisuus [viitattu 6.4.2021]

Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention, and behavior: An introduction to theory and research. Reading, MA: Addison-Wesley

Forcepoint 2018. Security predictions. Saatavana: https://www.forcepoint.com/sites/default/files/resources/files/report_2018_security_predictions_en.pdf [viitattu 19.4.2020]

Ford, J. D. & Ford, L. W. 1995. The Role of Conversations in Producing Intentional Change in Organizations. The Academy of Management Review, 20(3), 541-570.

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S. & Jabbar, S. 2018. Security threats to critical infrastructure: The human factor. (Raportti). The Journal of Supercomputing, 74(10), 49-86.

Giddens, A. 1984. The constitution of society: Outline of the theory of structuration. Berkeley, CA. University of California Press.

Grobler, M., Gaire, R. & Nepal, S. 2021. User, Usage and Usability: Redefining Human Centric Cyber Security. Frontiers in Big Data, 4.

Gyunka, B. A. & Christiana, A. O. 2017. Analysis of Human Factors in Cyber Security: A Case Study of Anonymous Attack on Hbgary. Computing and information systems, 21(2), 10.

Halonen, A. 2020. Kalliiksi käyvä ”toimitusjohtajahuijaus” leviää aina kesällä – kohteena erityisesti kesätyöntekijät ja tuuraajat. Iltalehti 02.07.2020. Saatavana: https://www.iltalehti.fi/digiuutiset/a/27a057a0-69fb-490b-8a97-80c57ff70014 [viitattu 6.4.2021]

Hämäläinen, V.P. 2021. Ehkä jopa 32 000 Vastaamon potilaan tiedot ilmestyivät viime yönä Tor-verkkoon – poliisi: "Emme tiedä, monenko käsissä tietokanta on". Yle 27.1.2021. Saatavana: https://yle.fi/uutiset/3-11757676 [viitattu 6.4.2021]

Harrison, D. 1999. Are you ready to be a change sponsor? Industrial Management 41 (4), 6-9.

Harrison, S. & Jurjens, J. 2017. Information security management and the human aspect in organizations. Information & Computer Security 25 (5), 494-534.

Hedström, K., Kolkowska, E., Karlsson, F. & Allen, J. (2011). Value conflicts for information security management. The journal of strategic information systems, 20(4), 373-384.

Heikkilä, M. 2020. Nainen kuoli ambulanssiin, kun kyberhyökkäys jumitti saksalaisen sairaalan tietojärjestelmän – syyttäjä avasi harvinaisen henkirikostutkimuksen. Yle 19.9.2020. Saatavana: https://yle.fi/uutiset/3-11553530 [viitattu 6.4.2021]

Hofmann, D. & Stetzer, A. 1998. The role of safety climate and communication in accident interpretation: Implications for learning from negative events. Academy of Management Journal 41 (6), 644-657.

Hofmann, D. A. & Morgeson, F. P. 1999. Safety-Related Behavior as a Social Exchange: The Role of Perceived Organizational Support and Leader–Member Exchange. Journal of Applied Psychology 84 (2), 286-296.

Hsu, J. S., Shih, S. P., Hung, Y. W. & Lowry, P. B. 2015. The role of extra-role behaviors and social controls in information security policy effectiveness. (Raportti).
Immuniweb. 2020. State of Cybersecurity at Top 100 Global Airports. Saatavana: https://www.immuniweb.com/blog/state-of-cybersecurity-top-100-airports.html © 2021 ImmuniWeb [viitattu 17.4.2021]

Johnston, A. C., Warkentin, M. & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric.

Johnston, A. C., Warkentin, M., Dennis, A. R. & Siponen, M. 2019. Speak their Language: Designing Effective Messages to Improve Employees' Information Security Decision Making. Decision Sciences 50 (2), 245.

Kahan, J., Allen, A., George, J., & Thompson, W. (2009). Concept development: An operational framework for resilience. VA: Homeland Security Studies and Analysis Institute. Saatavana: http://www.homelandsecurity.org/ [viitattu 6.4.2021]

Karyda, M,. Kiontouzis, E., & Kokolakis, S. (2005). Information systems security policies: a contextual perspective. Computers & Security 24, 246-260.

Kath, L. M., Marks, K. M. & Ranney, J. 2010. Safety climate dimensions, leader–member exchange, and organizational support as predictors of upward safety communication in a sample of rail industry workers. Safety Science 48 (5), 643-650.

Kvale, S. 1996. Interviews: an introduction to qualitative research interviewing: Steinar Kvale. Thousand Oaks, CA: Sage.

Lehto M., Limnell, J., Innola, E., Pöyhönen, J., Rusi, T. & Salminen, M. 2017. Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Valtioneuvoston kanslia, 30.

Lehto, M. 2019. Kybermaailman ilmiöitä ja määrittelyjä. Jyväskylä: Jyväskylän yliopisto.

Lehto, M., Limnell, J., Kokkomäki, T., Pöyhönen, J. & Salminen M. 2018. Kyberturvallisuuden strateginen johtaminen Suomessa. Valtioneuvoston kanslia 28/2018.

Lewis, L. K. 2006. Employee Perspectives on Implementation Communication as Predictors of Perceptions of Success and Resistance. Western journal of communication 70 (1), 23-46.

Limba, T., Pleta, T., Agafonov, K. & Damkus, M. 2017. Cyber security management model for critical infrastructure. The inter journal entrepreneurship and sustainability issues, 4(4), 559-573.

Limnéll, J. & Lehto, M. 2019. The importance of strategic leadership in cyber security: Case of Finland.

Littlejohn, A., Dane, L. & Anoush, M. 2014. Comparing safety culture and learning culture. Risk Management 16 (4), 272-293.

Luo, W., Song, L. J., Gebert, D. R., Zhang, K. & Feng, Y. 2016. How does leader communication style promote employees' commitment at times of change? Journal of Organizational Change Management, 29(2), 242-262.

Matta, W. & Cantelli-Forti, A. 2019. An Innovative Airport Physical-cyber Security System (APSS). Information & Security, 43(3), 285-293.

Mattila, J., Mäkäräinen, K., Pajarinen, M., Seppälä, T., Ali-Yrkkö, J. & Tervo, E. 2020. Digibarometri 2020: Kyberturvan tilannekuva Suomessa. Taloustieto Oy: Helsinki.

Mcevoy, T. R. & Kowalski, S. J. 2019. Deriving Cyber Security Risks from Human and Organizational Factors – A Socio-technical Approach. Complex Systems Informatics and Modeling Quarterly (18), 47-64.

Mikkola, L. 2020. Supportive communication in the workplace. Teoksessa Mikkola, L. & M. Valo. Workplace communication (149–162). New York: Routledge.

Mikkola, L., & Valo, M. (toim.). 2020. Workplace communication. New York: Routledge.

Mitnick, K. D. & Simon, W. M. 2003. The Art of Deception: Controlling the Human Element of Security. John Wiley & Sons, Inc., USA.

Moinescu, R., Racuciu, C., Glavan, D., Antonie, N. & Eftimie, S. 2019. Aspects of human weaknesses in cyber security. Scientific bulletin "Mircea cel Batran" Naval Academy; Constanta, 22(1), 1-9.

Moody, G., Siponen, M. & Pahnila, S. 2018. Toward a Unified Model of Information Security Policy Compliance. MIS Quarterly 42 (1), 285.

Pádár, K., Pataki, B. & Sebestyén, Z. 2017. Bringing project and change management roles into sync. Journal of Organizational Change Management 30 (5), 797-822.

Patton, M. Q. 2015. Qualitative research & evaluation methods : integrating theory and practice. (Fourth edition edition) Thousand Oaks, California: SAGE Publications, Inc.

Pfeffer, J. & Sutton, R. (1999). Knowing "what" to do is not enough: Turning knowledge into action. California Management Review, 42(1), 83-108.

Posey, C., Roberts, T. L., Lowry, P. B. & Hightower, R. T. 2014. Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. Information & management 51 (5), 551-567.

Pöllänen, M., Kaartinen, K., Mäkelä, T., Rauhamäki, H. & Mäntynen J. 2014. Ilmakuljetusten huoltovarmuuden tilannekuvan muodostaminen. Huoltovarmuusorganisaatio: Helsinki.

Raggad, B. G. 2010. Information security management : concepts and practice. Boca Raton, Florida ; London, England ; New York: CRC Press.

Reiman, T. & Oedewald, P. 2008. Turvallisuuskriittiset organisaatiot – onnettomuudet, kulttuuri ja johtaminen. Saatavana: https://mycourses.aalto.fi/pluginfile.php/655890/mod_resource/content/1/Turvallisuuskriittiset_organisaatiot_versio%202018.pdf [viitattu 6.4.2021]

Reiman, T., Pietikäinen, E. & Oedewald, P. 2008. Turvallisuuskulttuuri – teoria ja arviointi. VTT Publications 700: Espoo.

Rocha Flores, W. & Ekstedt, M. 2016. Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. Computers &Amp; Security (Print) 59 (C), 26-44.

Schein, E. 1990. Organizational Culture. American Psychologist 45, 109.

Schein, E. H. & Schein, P. 2017. Organizational culture and leadership. (Fifth edition edition) Hoboken: Wiley.

Schoeneborn, D., Blaschke, S., Cooren, F., Mcphee, R. D., Seidl, D. & Taylor, J. R. 2014. The Three Schools of CCO Thinking: Interactive Dialogue and Systematic Comparison. Management Communication Quarterly 28 (2), 285-316.

Schroeder, H. 2015. The role of the executive sponsor in organizational transformation. Strategic Direction 31 (3), 1-3.

Schultz, E. 2005. The human factor in security. Computers & security, 24(6), 424-426.

Siponen, M. & Vance. A. 2010. Neutralization: New insights into the problem of employee information systems security policy violations. MIS Quarterly, 34(3), 487.

Siponen, M. & Willison, R. (2009). Information security management standards: Problems and solutions. Information & management, 46(5), 267-270.

Siponen, M. 2009. Technical opinion - Are employees putting your company at risk by not following information security policies? Communications of the ACM 52 (12), 145-147.

Siponen, M. Puhakainen, P. & Vance, A. 2020. Can individuals' neutralization techniques be overcome? A field experiment on password policy. Computers & Security, 88.

Siponen, M. T. 2000. A conceptual foundation for organizational information security awareness. Information Management & Computer Security 8 (1), 31-41.

Smith, Z. M., Lostri, E. & Lewis, J. A. 2020. The hidden costs of cybercrime. McAfee report. Saatavana: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf [viitattu 6.4.2021]

Sommestad, T. 2018. Work-related groups and information security policy compliance. Information and Computer Security 26 (5), 533-550.

Suomen kyberturvallisuusstrategia. 2019. Saatavana: https://turvallisuus-komitea.fi/wp-content/uploads/2018/05/Suomen-kyberturvallisuusstrategia-ja-taustamuistio.pdf [viitattu 19.4.2020]

Sutcliffe, K. M. 2011. High reliability organizations (HROs). Best practice & research.Clinical anaesthesiology 25 (2), 133-144.

Sykes, G. M. & Matza, D. 1957. Techniques of Neutralization: A theory of delinquency. American sociological association 22(6), 664-670.

Taylor, J. R., Cooren, F., Giroux, N. & Robichaud, D. (1996). The Communicational Basis of Organization: Between the Conversation and the Text. Communication Theory, 6(1), 1-39.

Tiainen, A. 2020. Kun nettisivulla kysytään, hyväksytkö evästeet, moni klikkaa automaattisesti ”kyllä” – Kyse on tietoturvaväsymyksestä, jossa piilee riskejä, sanovat asiantuntijat. Helsingin Sanomat 21.10.2020. Saatavana: https://www.hs.fi/teknologia/art-2000006675896.html [viitattu 6.4.2021]

Tietosuojavaltuutetun toimisto. 2020. Tietosuoja. Saatavana: https://tietosuoja.fi/tietosuoja [viitattu 6.4.2020]

Tracey, S., O'sullivan, T. L., Lane, D. E., Guy, E. & Courtemanche, J. 2017. Promoting Resilience Using an Asset-Based Approach to Business Continuity Planning. SAGE open, 7(2),

Tracy, S. J. 2013. Qualitative research methods : collecting evidence, crafting analysis, communicating impact. Chichester, West Sussex, U.K.: Wiley-Blackwell.

Traficom. 2020. Kybersää. Saatavana: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kybersaa?toggle=Kybers%C3%A4%C3%A4tiedotteet%202020 [viitattu 6.4.2021]

Traficom. 2020. Tietoturvan vuosi 2019: kyberturvallisuuden vuosikatsaus.

Turvallisuuskomitea 2010. Yhteiskunnan turvallisuusstrategia. Valtioneuvoston periaatepäätös.

Turvallisuuskomitea 2018. Sanastokeskus, Kyberturvallisuuden sanasto.

Tutkimuseettinen neuvottelukunta (TENK). 2012. Eettinen ennakkoarviointi ihmistieteissä. Saatavana: https://tenk.fi/sites/default/files/2021-01/Ihmistieteiden_eettisen_ennakkoarvioinnin_ohje_2020.pdf [viitattu 6.4.2021]

Valo, M. & Mikkola, L. 2020. Focusing on workplace communication. Teoksessa L. Mikkola, & M. Valo. Workplace communication (3-14). New York: Routledge.

Vance, A., Siponen, M. & Pahnila, S. 2012. Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. Information & Management, 49(3-4), 190-198.

Verizon 2018. Data breach investigations report. Saatavana: https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf [viitattu 6.4.2021]

Verizon 2019. Data breach investigations report. Saatavana: https://enterprise.verizon.com/resources/reports/dbir/2019/results-and-analysis/ [viitattu 6.4.2021]

Virvilis, N., Serrano, O. S. & Vanautgaerden, B. 2014. Changing the game: The art of deceiving sophisticated attackers.

Von Solms, R. & Van Niekerk, J. 2013. From information security to cyber security. Computers & Security, 38(C), 97-102.

Von Solms, R. 1998. Information security management (3): the Code of Practice for Information Security Management (BS 7799). Information Management & Computer Security 6 (5), 224-225.

Vroom, C. & Von Solms, R. 2004. Towards information security behavioural compliance. Computers & Security, 23(3), 191-198.

Whitman, M. E. & Mattord, H. J. 2012. Principles of information security. Cengage learning, Boston, MA.

Wilhoit Larson, E. 2020. Where is an Organization? How Workspaces Are Appropriated to Become (Partial and Temporary) Organizational Spaces. Management Communication Quarterly 34 (3), 299-327.

Wilhoit, E. D. 2018. Space, Place, and the Communicative Constitution of Organizations: A Constitutive Model of Organizational Space. Communication Theory 28 (3), 311-331.

Wilson-Donnelly, K. A., Priest, H. A., Burke, C. S. & Salas, E. 2004. Tips for Creating a Safety Culture in Organizations. Ergonomics in Design: The Quarterly of Human Factors Applications 12 (4), 25-30.

Wilson, M. and Hash, J. (2003). "Building an Information Technology Security Awareness Training Program." U.S. Department of Commerce, NIST Special Publication 800-50.

Witte, K. 1992. Putting the fear back into fear appeals: The extended parallel process model. Communication monographs 59 (4), 329-349.

YTNK. 2005. Yritysturvallisuuden osa-alueet. Yritysturvallisuus EK. Saatavissa: http://www.ek.fi/ytnk/yritysturvallsuus/index.php. [viitattu 20.7.2020]

# LIITTEET

## Liite 1: Haastattelurunko

1. Työn kuvaaminen

• Asema organisaatiossa (esimies vai alais-asemassa)
• Millaisia työtehtäviä tyypillisesti tekee
• Kuinka monta vuotta olet ollut töissä Finavialla?
• Työskenteleekö yksin/tiimeissä/yhteistyösuhteet/verkostot (kenen kanssa tekee yhteistyötä, kenen kanssa jakaa tietoa)

2. Näkemykset tietoturvasta Finavialla

• Mitä tietoturva on Finavialla? (mistä tekijöistä koostuu)
• Miten tietoturva on osa työnkuvaasi? (työtilanne, jossa tietoturvaa joudutaan miettimään)
• Onko tietoturva tärkeä turvallisuuden osa-alue Finavialla? Miksi on/ei?
• Millainen vastuu sinulla on tietoturvasta? (Koetaanko tietoturvasta vastuuta)
• Mitkä asiat/tekijät edistävät tietoturvan toteutumista (Finavialla)?
• Mitkä tekijät heikentävät tietoturvaa? (voi kuvailla tilanteita)

3. Strateginen ja suunniteltu viestintä tietoturvasta

• Viestintäkanavat (Mitä kanavia pitkin tietoa saadaan, onko kanavat selkeitä ja toimivia)
• Onko palautetta varten selkeä kanava (onko palautteen antaminen mahdollista, helppoa)
• Tiedon saatavuus (Onko tietoturvaan liittyvä tieto löydettävissä ja hyödynnettävissä)
• Tiedon määrä ja ymmärrettävyys (Onko tietoa liikaa/liian vähän, onko se ymmärrettävää?)
• Tiedon kohdentamisen onnistumisen (Onko saatu tieto tietoturvasta relevanttia)

• Koulutukset & harjoitukset (Millaisiin tietoturvakoulutuksiin olet osallistunut? Miten niitä voisi kehittää? Millaisia sisältöjä toivot koulutuksiin? Missä muodossa koulutuksen järjestettäisiin (video, kasvokkais, omatoiminen)
• Tiedotteet & kampanjat (näkyvyys, toistuvuus, kohdennus)
• Ohjeistukset (Ovatko tietoturvaohjeistukset tiedossa ja ymmärrettäviä?)

4. Tietoturvaviestinnän sosiaaliset prosessit

• Johtaja-alaissuhteet (Viestinnän avoimuus, mahdollisuus keskustella tietoturvasta)
• Yhteistyömahdollisuudet? Millaisissa yhteistyötilanteissa mietitään?
• Omat ja kollegoiden asenteet sekä näkemykset tietoturvasta (Asenteet, suhtautuminen, motivaatio eli mikä motivoi esim. noudattamaan ohjeistuksia, asenteiden kuvaamista, suhtautumista)
• Koettu sosiaalinen tuki (Onko sitä tarjolla, oletko saanut tukea, onko tuelle tarvetta)
• Osallistumismahdollisuudet (kuulluksi tuleminen, osallistaminen muutokseen)
• Vapaa sana