TURUN YLIOPISTO
Kauppakorkeakoulu

Tietoturvatietoisuuden kehittäminen finanssialan organisaatiossa

Tietojärjestelmätieteen
pro gradu -tutkielma

Laatija:
Aliisa Mäkinen

Ohjaaja:
Prof. Reima Suomi

31.10.2022
Turku

Pro gradu -tutkielma

Oppiaine: Tietojärjestelmätiede
Tekijä: Aliisa Mäkinen
Otsikko: Tietoturvatietoisuuden kehittäminen finanssialan organisaatiossa
Ohjaaja: prof. Reima Suomi
Sivumäärä: 79 sivua + liitteet 5 sivua
Päivämäärä: 31.10.2022

Verkkorikollisuus kasvaa ja kehittyy jatkuvasti, mikä on lisännyt finanssialan paineita suojautua verkkohyökkäyksiltä entisestään. Tähän eivät kuitenkaan riitä kehittyneet suojausteknologiat tai finanssialan tarkat tietoturvavaatimukset, vaan keskeisessä roolissa ovat ihmiset. Tutkimusten mukaan jopa 88 % tietovuodoista johtuu ihmisten tekemästä virheestä, kuten liian helpoista salasanoista, päivittämättömistä laitteista tai tietoturvaosaamisen puutteesta. On siis tärkeää, että suojausteknologioiden lisäksi organisaatioissa kehitetään työntekijöiden tietoturvatietoisuutta. Tämän tutkielman tavoitteena on selvittää, miten tietoturvatietoisuutta voidaan kehittää finanssialan organisaatiossa.

Tämän tutkielman empiirinen tutkimus suoritettiin hyödyntäen laadullista tutkimusmenetelmää. Tutkimusaineisto kerättiin puolistrukturoitujen teemahaastatteluiden avulla ja haastateltaviksi valittiin kuusi tietoturva-asiantuntijaa neljästi eri suomalaisesta pankista. Haastatteluiden teemat perustuivat teoriassa keskeiseksi määriteltyihin aiheisiin, jotka olivat tietoturvatietoisuus finanssialalla ja tutkittavissa organisaatiossa, tietoturvatietoisuuteen vaikuttavat tekijät, tietoturvatietoisuuden kehittämisen menetelmät sekä tietoturvatietoisuuden mittaaminen ja arviointi. Tutkimusten tulosten analysointi toteutettiin teoriaohjaavalla analyysillä, jossa aikaisempi tutkimus ohjasi aineiston analysointia, mutta tutkimus ei testannut valmiiksi olemassa olevaa teoriaa tai teoreettista viitekehystä.

Tutkielman tulosten pohjalta muodostettiin uusi teoreettinen viitekehys tietoturvatietoisuuden systemaattiseen kehittämiseen, joka perustuu PDCA-mallin mukaiseen jatkuvaan kehittämiseen. Mallin tarkoituksena on toimia apuna finanssialan organisaatioille ja sen takia siinä hyödynnettiin haastatteluissa hyväksi todettuja malleja muodostaen niistä mahdollisimman kattava kokonaisuus. Viitekehys asettaa vaatimukset tietoturvatietoisuuden kehittämiselle, sekä prosessin tietoturvatietoisuuden eri osa-alueiden kehittämiselle. Tutkielmassa on esitetty myös käytännön esimerkki viitekehyksen hyödyntämiseen.

Tutkimuksen tulokset olivat pitkälti linjassa aiemman tutkimuksen kanssa. Tietoturvatietoisuuden kehittämisessä tärkeinä nähtiin jatkuva kehitys ja koko organisaation sitoutuminen kehittämiseen. Organisatoriset tekijät nähtiin hyvin tärkeinä, mutta haastatteluissa todettiin, että isoissa organisaatioissa yksilöllisten tekijöiden huomioiminen ei ole mahdollista vaan ajattelun tulisi olla enemmän roolipohjaista. Tietoturvatietoisuuden kehittämisen menetelmissä keskeisenä pidettiin saavutettavuutta, käytännönläheisyyttä ja positiivista lähestymistapaa. Empiriassa nousi esille myös organisaation koon, rakenteen ja organisaatiokulttuurin vaikutus tietoturvatietoisuuden kehittämiseen.

Tärkeä huomio oli, että työntekijöitä ei nähdä enää tietoturvauhkana vaan tietoturvan vahvimpana lenkkinä tai tietoturvan puolustajina, joiden tekemät virheet johtuvat tietämättömyydestä ja riittämättömästä opastuksesta. Kaikissa organisaatioissa haluttiin luoda positiivista tietoturvakulttuuria, jonka edellä mainittu ajattelutapa mahdollistaa. Empiriassa nousi esille uutena havaintona ADKAR-malli, jota voidaan hyödyntää tietoturvatietoisuuden kehittämiseen niin kulttuurin näkökulmasta kuin tehokkaiden menetelmien kehittämiseen. ADKAR-malli on myös osa tutkielmassa kehitettyä viitekehystä.

Avainsanat: tietoturva, tietoturvatietoisuus, finanssiala

SISÄLLYSLUETTELO

1 Johdanto 7

1.1 Motivointi 7

1.2 Tutkimusaukko, tutkimuskysymykset ja tutkielman tavoitteet 9

1.3 Tutkielman rakenne 10

2 Tietoturvatietoisuuden kehittäminen finanssialan organisaatiossa 12

2.1 Tietoturvallisuus finanssialalla 12

2.1.1 Tietoturvallisuus ja tietoturvallisuuden hallinta 12

2.1.2 Finanssialan tietoturvallisuusvaatimukset 13

2.2 Tietoturvatietoisuuden kehittäminen 15

2.2.1 Tietoturvatietoisuus 15

2.2.2 Tietoturvatietoisuuden systemaattinen kehittäminen 18

2.2.3 Tietoturvatietoisuuden arviointi ja mittaaminen 21

3 Tietoturvatietoisuuteen vaikuttavat tekijät 25

3.1 Parsons ym. (2017) viitekehys 25

3.2 Organisatoriset tekijät 26

3.3 Yksilölliset tekijät 27

3.4 Välilliset tekijät 28

3.4.1 Viestintä 28

3.4.2 Harjoitukset ja koulutus 29

3.4.3 Palkitseminen ja rankaiseminen 30

4 Metodologia 33

4.1 Tieteenfilosofiat 33

4.2 Tutkimusmenetelmä ja -strategia 33

4.3 Aineistonkeruumenetelmä 34

4.4 Aineiston analysointi 35

5 Tutkimuksen tulokset 38

5.1 Tietoturvatietoisuus finanssialalla ja tutkittavissa organisaatioissa 38

5.1.1 Tietoturvatietoisuus finanssialalla 38

5.1.2 Organisaatioiden tietoturvatietoisuus 39

5.2 Tietoturvatietoisuuteen vaikuttavat tekijät 42

5.2.1 Haastatteluiden tulokset 42
5.2.2 Yksilölliset tekijät 43
5.2.3 Organisatoriset tekijät 44
5.2.4 Välilliset tekijät 47
5.3 Tietoturvatietoisuuden arviointi ja mittaaminen 51
6 Tietoturvatietoisuuden systemaattisen kehittämisen viitekehys 54
6.1 Viitekehyksen muodostaminen 54
6.2 Vaatimukset 56
6.3 Kehittäminen 57
6.4 Lopputuotokset 58
6.5 Esimerkki viitekehyksen hyödyntämisestä 59
7 Pohdinta 63
7.1 Johtopäätökset 63
7.2 Yhteenveto 66
7.3 Tutkimuksen luotettavuuden arviointi 67
7.4 Jatkotutkimusehdotukset 69
Lähteet 71
Liitteet 80
Liite 1: Haastattelurunko 80
Liite 2: Aineistonhallintasuunnitelma 82

KUVIOT

Kuvio 1: PDCA-malli (Deming 1952) 19
Kuvio 2: Maturiteettimalli (SANS 2022) 23
Kuvio 3: Tietoturvatietoisuuteen vaikuttavat tekijät (Parsons ym. 2017) 25
Kuvio 4: Tietoturvatietoisuuden systemaattisen kehittämisen viitekehys 54

TAULUKOT

Taulukko 1: Finanssialalla käytettyjä tietoturvan hallintamenetelmiä 13
Taulukko 2: Tietoturvatietoisuuden tutkimuksessa hyödynnetyt teoriat 17
Taulukko 3: Kuvaus haastateltavista 35
Taulukko 4: Organisaatioiden tietoturvatietoisuus 40
Taulukko 5: Haastatteluiden tulokset 42
Taulukko 6: Esimerkki ADKAR-mallin hyödyntämisestä 60

1 Johdanto

1.1 Motivointi

Vahvasti säännellyllä finanssialalla on paljon tietoturvaa koskevia vaatimuksia ja kehittyneitä suojausteknologioita (Finanssiala 2021a), mikä on varmasti osittain syynä finanssialan johtavaan asemaan Huoltovarmuuskeskuksen (2020) tekemässä kyberturvallisuuden nykytilan kartoituksessa eri toimialoilla. Kehittyneet suojausteknologiat eivät kuitenkaan ole yksinään ratkaisu tietoturvaan liittyvien uhkien minimoimiseen, vaan keskeisessä roolissa ovat myös ihmiset. Liian helpot salasanat, päivittämättömät laitteet ja tietoturvaosaamisen puute yhdistettynä koko ajan kehittyvään verkkorikollisuuteen aiheuttavat organisaatiolle uhan, johon tietoturvatietoisuudella pyritään vastaamaan (Finanssiala 2021a).

Tutkimusten mukaan jopa 88 % tietovuodoista johtuu ihmisen tekemästä virheestä (Verdict 2019) ja usein kuullaankin sanottavan, että ihminen on tietoturvan heikoin lenkki. Vastauksena tähän ongelmaan organisaatioissa on alettu kiinnittää entistä enemmän huomiota työntekijöiden tietoturvatietoisuuteen, jonka avulla pyritään hallitsemaan tietoturvaan liittyvää inhimillistä riskiä (SANS 2021). Tietoturvatietoisuuden kehittämisen avulla tavoitteena on päästä tilanteeseen, jossa vastoin perinteistä oletusta, työntekijöistä voidaan tehdä tietoturvan vahvimpia lenkkejä (Caruna 2022).

Siposen (2000) mukaan tietoturvatietoisuudella viitataan tilaan, jossa organisaation työntekijät ovat tietoisia ja sitoutuneita heille asetettuihin tietoturvaan liittyviin tavoitteisiin. Ymmärtääkseen tietoturvaan liittyvät tavoitteet, työntekijät ymmärtävät organisaation tietoturvaan tietoturvakäytännöt (Khan 2011) ja käyttäytyvät niiden mukaisesti (ISF 2002). Tietoturvatietoisuuden kehittäminen on jatkuva prosessi, jossa keskeistä on systemaattisuus ja mukautuminen tietoturvakentän jatkuviin muutoksiin (Wilson & Hash 2003). Tätä varten organisaatiot ovat kehittäneet tietoturvatietoisuusohjelmia, joissa tietoturvatietoisuuden lisäämisellä ja työntekijöiden kouluttamisella tavoitteena on luoda vahva tietoturvakulttuuri, joka on osa organisaatiokulttuuria (Peltier 2005).

Vahva tietoturvakulttuuri ei synny itsestään, vaan se vaatii usein muutosta työntekijöiden tietoisuudessa, asenteissa ja käyttäytymisessä liittyen organisaation

tietoturvakäytäntöihin. Tämän takia on tärkeä tunnistaa näihin vaikuttavat tekijät ja ymmärtää, minkä menetelmien avulla organisaatio pystyy itse vaikuttamaan työntekijöiden tietoturvatietoisuuteen. (Parsons ym. 2017) Mikäli tietoturvatietoisuuden kehittämisen avulla halutaan tuottaa arvoa organisaatiolle, on tärkeää myös kehittämisen jatkuva mittaaminen ja arviointi (Kruger & Kearney, 2006), minkä avulla voidaan vastata ympäristön ja organisaation muutoksiin ja löytää organisaatiolle tehokkaimmat menetelmät tietoturvatietoisuuden kehittämiseen (Khan 2011).

Tämä tutkielma keskittyy tietoturvatietoisuuden kehittämiseen suomalaisissa finanssialan organisaatioissa. Finanssialan esittelymateriaalissa on kuvattu finanssialaa seuraavasti: ”Finanssiala on pankkipalveluja, vakuutustuotteita, sijoituspalveluja – ja julmettu määrä teknologiaa, joka mahdollistaa sen kaiken” (Finanssialalle 2022a). Käytännössä finanssiala koostuu rahoitusmarkkinoilla toimivista instituutioista, jotka muodostuvat pankeista, vakuutusyhtiöistä ja rahoituslaitoksista. Nykyään eri toimijoiden välinen raja on häilyvä, koska osa pankeista tarjoaa myös laajasti varainhoito- ja vakuutuspalveluita. (Finanssialalle 2022b) Tässä tutkimuksessa haastateltavat organisaatiot ovat pankkeja, jotka tarjoavat myös edellä mainittuja varainhoito- ja vakuutuspalveluita.

Pankit ovat kriittisen infrastruktuurin toimijoita, mikä tarkoittaa, että niiden toiminta on välttämätöntä yhteiskunnan toimivuudelle (Huoltovarmuuskeskus 2005). Digitalisaation seurauksena finanssialan toiminnot ovat yhä enenevissä määrin verkossa, ja koronapandemia on vauhdittanut käteisestä luopumista ja sähköisiin maksutapoihin siirtymistä entisestään (Suomen Pankki 2021). Myös siirtyminen etä- ja hybridityöhön on luonut uusia tietoturvauhkia ja kasvattanut työntekijöiden roolia näiden uhkien torjunnassa. Tietoturvauhat eivät rajoitu myöskään Suomen sisälle, vaan digitalisaation seurauksena kiristynyt maailmantilanne näkyy myös verkossa, jossa verkkorikolliset käyttävät hävyttömästi hyväksi poliittisia ja yhteiskunnallisia ongelmia. (SoSafe 2022)

Finanssialalla ei ole Suomessa toistaiseksi koettu merkittäviä tietomurtoja, mutta samaan aikaan pankit käyvät jatkuvaa taistelua koko ajan kasvavaa verkkorikollisuutta vastaan. Vuonna 2021 suomalaiset menettivät verkkorikollisille noin 47 miljoonaa euroa (Kuluttajaliitto 2022) ja yli 90 % suomalaisista altistui vuoden aikana verkko- ja puhelinhuijauksille (Saxholm 2022). Vastaavasti pankkiryöstöjä on Suomessa 2000-luvun aikana tehty vuodessa alle kymmenen, kun 1990-luvulla niitä tehtiin vuosittain yli

sata (Helsingin Sanomat 14.10.2014). Voidaan siis todeta, että varkaat ovat päivittäneet osaamisensa tähän päivään.

Verkkopankin käyttöön liittyvät tunnistustiedot ovat verkkorikollisten keskuudessa haluttua tavaraa ja vuoden 2021 aikana verkkohuijauksia tehtiin pankkien nimissä 10 miljoonan euron edestä (Kuluttajaliitto 2022). Kansainvälisellä tasolla arvioidaan, että verkkorikollisuuden kustannukset olisivat vuonna 2021 nousseet 17,5 miljardiin dollariin ja niiden ennustetaan ylittävän 30 miljardia vuoteen 2025 mennessä (Cybersecurity Venture 2022). Tämä kehityssuunta on kasvattanut finanssialan paineita suojautua verkkohyökkäyksiltä entisestään. Asiakkaiden luottamuksesta riippuvalla toimialalla on finanssialan organisaatioiden yhä keskeisempää kehittää palveluita tietoturvaan liittyvät edellytykset mielessä (Finanssiala 2021b) ja huomioida niin tietoturvan tekninen kuin inhimillinen puoli (Ashenden 2008).

1.2 Tutkimusaukko, tutkimuskysymykset ja tutkielman tavoitteet

Tässä tutkielmassa tutkitaan tietoturvatietoisuuden kehittämistä finanssialan organisaatiossa. Tutkielmassa haastatellaan tietoturva-asiantuntijoita neljästä eri suomalalaisesta pankista, jotka ovat eri kokoisia, erilaisia organisaatiorakenteeltaan ja joissa tietoturvatietoisuuden kehittäminen on eri vaiheissa. Haastateltavat asiantuntijat ovat olleet aktiivisesti mukana kehittämässä organisaatioiden tietoturvatietoisuutta. Tutkimus toteutetaan käyttäen laadullista tutkimusmenetelmää ja aineisto kerätään puolistrukturoitujen haastatteluiden avulla. Haastatteluiden tuloksia verrataan toisiinsa sekä aiempaan kirjallisuuteen, jonka avulla muodostetaan viitekehys tietoturvatietoisuuden systemaattiseen kehittämiseen.

Tietoturvatietoisuudesta on melko paljon aikaisempaa tutkimusta, mutta suurin osa tutkimuksesta on tehty määrällistä tutkimusmenetelmää hyödyntäen, joten laadullinen tutkimus tuo uutta näkemystä aikaisempaan tutkimukseen (Lebek ym. 2014). Lisäksi finanssialaan keskittyvää tutkimusta tietoturvatietoisuudesta ei ole tehty paljoa. Albrechtsen (2007) tutki laadullisella tutkimusmenetelmällä työntekijöiden kokemuksia tietoturvasta pankissa, ja Bauer ja Bernroider (2017) tekivät case-tutkimuksen tietoturvatietoisuuden vaikutuksesta työntekijöiden tietoturvakäytäntöjen noudattamiseen suuressa Eurooppalaisessa pankkiorganisaatiossa. Tietoturvatietoisuutta ei ole kuitenkaan tutkittu juuri kehittämisen näkökulmasta, jossa haastateltavat koostuisivat tietoturvatietoisuutta kehittävistä asiantuntijoista, vaan monet tutkimukset

keskittyvät tutkimukseen työntekijöiden näkökulmasta. Lähimpänä kehittämisen näkökulmaa on Khandon ym. (2021) tekemä kirjallisuuskatsaus yksityisellä ja julkisella sektorilla hyödynnettävistä menetelmistä tietoturvatietoisuuden kehittämiseen. Näiden lisäksi tietoturvatietoisuuden kehittämiseen on laadittu erilaisia, usein kaupallisia, käytännön oppaita. Nämä oppaat ovat hyviä työkaluja, mutta ne eivät keskity finanssialaan ja niihin ei ole vapaata pääsyä kaikilla organisaatioilla.

Tutkielman tavoitteena on vastata alla esitettäviin tutkimuskysymyksiin ja muodostaa viitekehys tietoturvatietoisuuden kehittämiseen finanssialan organisaatiossa. Keskeistä on saada selville, mitkä ovat olleet tehokkaita menetelmiä työntekijöiden tietoturvatietoisuuden parantamiseen ja mitkä ominaisuudet tulevat esille, kun puhutaan tietoturvatietoisuuden kehittämisestä finanssialalla. Lisäksi halutaan selvittää, mitä osa-alueita tulee ottaa huomioon tietoturvatietoisuuden kehittämisessä. Tietoturvatietoisuus ei ole osa-alue, jossa finanssialan organisaatiot kilpailevat, joten tarkoituksena on jakaa eri organisaatiossa hyväksi todettuja käytäntöjä koko finanssialalle ja täten auttaa suomalaisia finanssialan organisaatioita kehittämään inhimillistä tietoturvaa ja suojautumaan paremmin koko ajan kasvavaa verkkorikollisuutta vastaan.

Tutkielman tutkimuskysymykset ovat seuraavat:

1. Miten tietoturvatietoisuutta voidaan kehittää finanssialan organisaatiossa?
    a. Mitkä ovat tietoturvan vaatimukset finanssialalla ja miten ne vaikuttavat tietoturvatietoisuuden kehittämiseen?
    b. Mitkä yksilölliset, organisatoriset ja välilliset tekijät vaikuttavat tietoturvatietoisuuden kehittämiseen?
    c. Minkälaisten menetelmien avulla työntekijöiden tietoturvatietoisuutta voidaan parantaa tehokkaasti finanssialan organisaatiossa?
    d. Miten tietoturvatietoisuutta voidaan mitata ja arvioida?

1.3 Tutkielman rakenne

Tutkielmassa käydään ensin läpi tietoturvan ja tietoturvan hallinnan käsitteet sekä tietoturvan hallinnassa hyödynnettäviä hallintamenetelmiä, jonka jälkeen käsitellään finanssialan tietoturvavaatimukset ja niiden vaikutus organisaatioiden

tietoturvatietoisuuden kehittämiseen. Tämän jälkeen käsitellään tietoturvatietoisuuteen liittyvää aiempaa kirjallisuutta huomioiden tietoturvatietoisuuden systemaattinen kehittäminen sekä mittaaminen ja arviointi. Luvussa kolme käsitellään Parsons ym. (2017) viitekehystä mukaillen tietoturvatietoisuuteen vaikuttavia tekijöitä, jotka on jaettu yksilöllisiin, organisatorisiin ja välillisiin tekijöihin.

Kirjallisuuskatsauksen jälkeen siirrytään metodologiaan, jossa käsitellään tutkimuksessa hyödynnettäviä tutkimusmenetelmiä, tieteenfilosofioita ja aineistonkeruu- ja analysointimenetelmiä. Metodologian jälkeen siirrytään tutkimusten tulosten analysointiin, joka toteutetaan teoriaohjaavana analyysinä. Luvussa kuusi tulosten pohjalta luodaan malli tietoturvatietoisuuden kehittämiseen. Viimeisessä luvussa esitetään johtopäätökset, yhteenveto tutkielman tuloksista, arvioidaan tutkimuksen luotettavuutta ja annetaan jatkotutkimusehdotukset.

2 Tietoturvatietoisuuden kehittäminen finanssialan organisaatiossa

2.1 Tietoturvallisuus finanssialalla

2.1.1 Tietoturvallisuus ja tietoturvallisuuden hallinta

Tietoturvalla (engl. information security) tarkoitetaan hallinnollisia ja teknisiä toimia, joiden tarkoituksena on taata tiedon luottamuksellisuus, eheys ja käytettävyys (Traficom 2020). Luottamuksellisuudella tarkoitetaan, että tieto on vain siihen oikeutettujen henkilöiden saatavilla. Eheydellä tarkoitetaan, että tieto on yhteneväistä alkuperäisen tiedon kanssa ja käytettävyydellä, että se on hyödynnettävissä haluttuna aikana ja vaaditulla tavalla. (Finanssivalvonta 2020) Tietoturvalle läheisiä käsitteitä ovat tietosuoja ja kyberturvallisuus. Tietosuojalla tarkoitetaan yksilön henkilötietojen suojaamista ja tietoturvaa voidaan pitää yhtenä tietosuojan toteuttamisen keinoista (Tietosuojavaltuutetun toimisto 2022). Kyberturvallisuudella tarkoitetaan tietoturvan osa-aluetta, joka keskittyy kybertoimintaympäristöön, mutta sitä käytetään myös tieturvan synonyyminä (TEPA termipankki 2022) ja siksi myös tietoturvatietoisuuden ja kyberturvatietoisuuden kehittämistä voidaan pitää käytännössä samana asiana (F-Secure 2022).

Keskeinen osa tietoturvaa on tietoturvan hallinta (engl. information security management), johon tietoturvatietoisuuden kehittäminen kuuluu. Tietoturvan sitoutuessa yhä vahvemmin organisaation liiketoimintaan ja tavoitteisiin, on tietoturvan hallinnollinen puoli merkittävässä roolissa ja sen tulee olla integroituna organisaation muuhun johtamisjärjestelmään. (Ashenden 2008) Tietoturvan hallintaan käytetään tietoturvan hallintajärjestelmiä (engl. Information Security Management System, ISMS), jotka määrittävät organisaation tietoturvakäytännöt. Hallintajärjestelmät perustuvat yleisiin IT-hallinnon standardeihin, joiden tarkoituksena on varmistaa, että organisaatiossa hyödynnetään resursseja ja tietoturvakäytäntöjä oikein riittävän tietoturvallisuuden tason varmistamiksi.

Yleisimpiä hyödynnettyjä standardeja/viitekehyksiä ovat ISO/IEC 27000 -standardisarja, COBIT, PCIDSS (Susanto ym. 2011) ja NIST:in standardit, kuten Cyber Security Framework (NIST 2022), jotka esitellään tarkemmin taulukossa 1. Susanto ym. (2011) mukaisesta jaottelusta on jätetty pois BS7799 -standardi, koska se on aiempi versio

nykyisestä ISO/IEC 27000 -standardisarjasta sekä ITIL, koska se on enemmän tietohallinnon kuin tietoturvan viitekehys toisin kuin muut esiteltävät hallintamenetelmät. ISO/IEC 27000 -standardisarja on yleisin tietoturvallisuuden hallinnassa hyödynnetty standardi, mutta taulukossa 1 mainittuja viitekehyksiä/standardeja voidaan hyödyntää myös rinnakkain organisaatioissa (ISACA 2015).

Taulukko 1: Finanssialalla käytettyjä tietoturvan hallintamenetelmiä

Standardisarja/viitekehys	**Selitys**
ISO/IEC 27000	Standardisarja, joka määrittää vaatimukset tietoturvan hallintajärjestelmälle (ISO 2022).
National Institute of Standards and Technology (NIST)	Standardeja, ohjeita, parhaita käytäntöjä ja muita resursseja tietoturvallisuuden kehittämiseen, esimerkiksi Cyber Security Framework (NIST 2022).
The Control Objectives for Information and related technology (COBIT)	Koko organisaation prosessit kattava tietotekniikan hallinnan viitekehys (ISACA 2022).
The Payment Card Industry Data Security Standard (PCIDSS)	Standardi, joka määrittää vaatimukset turvalliseen korttimaksamiseen ja siihen liittyvien prosessien ja tietojen hallintaan (PCI Security Standard Council 2022).

Tietoturvan hallintamenetelmien pohjalta organisaatioihin luodaan näiden omat tietoturvakäytännöt (engl. Information Security Policy, ISP), jotka ovat johdon määrittämät tietoturvaan liittyvät ohjeet ja vaatimukset organisaation työntekijöille. Tietoturvakäytännöt luovat pohjan koko organisaation tietoturvan hallinnalle ja täten ne määrittävät tietoturvatietoisuuden kehittämisen eri osa-alueet. (Koohang ym. 2019)

Se mihin osa-alueeseen tietoturvatietoisuus sitoutuu, vaihtelee standardisarjan/viitekehyksen mukaan, mutta usein osa-alueet liittyvät esimerkiksi koulutukseen ja tarvittavien valmiuksien kehittämiseen (Almuhammadi & Alsaleh 2017; Barclay 2014). Standardeissa ei kuitenkaan anneta ehdotuksia siitä, kuinka työntekijöitä tulisi kouluttaa tai motivoida tietoturvakäytäntöjen noudattamiseen, minkä takia standardeja on tarpeellista täydentää viitekehyksillä, jotka keskittyvät enemmän turvallisuusprosessin sisältöön (Siponen 2006).

2.1.2 Finanssialan tietoturvallisuusvaatimukset

Finanssiala on yksi ”yhteiskunnan toimivuudelle ja huoltovarmuudelle kriittisistä toimialoista” (Varmuuden Vuoksi 2020), joka käsittelee kahta verkkorikollisten

haluamaa asiaa: rahaa ja henkilötietoja. Finanssialalla asiakkaiden luottamus on koko toimialan perusta ja toiminta perustuu pankki- ja vakuutussalaisuuden periaatteisiin. Pankki- ja vakuutussalaisuuden edellyttämä asiakkaiden taloudellisten ja yksityisten tietojen salassapitovelvollisuus muodostaa pohjan finanssialan organisaatioiden tietoturvaan ja tietosuojaan liittyville vaatimuksille. (Finanssiala 2021)

Edellä mainittujen tekijöiden vuoksi finanssiala on yksi säännellyimmistä toimialoista ja alalla toimiville organisaatioille on asetettu paljon tietoturvaan liittyviä vaatimuksia. Vaatimukset liittyvät esimerkiksi operatiivisten riskien hallintaan, turvallisiin tietojärjestelmiin ja varautumis- ja jatkuvuussuunnitelmiin (Finanssivalvonta 2020). Tässä luvussa käydään lyhyesti läpi finanssialan tietoturvavaatimukset, jotta tietoturvatietoisuuden rooli finanssialan organisaatiossa on helpompi ymmärtää.

Tietoturva on osa toimivaa riskienhallintaa, jossa järjestelmällisellä riskien johtamisella voidaan mahdollistaa organisaation toiminnan jatkuvuus ja tavoitteiden saavuttaminen (Valtiovarainministeriö 2017). Suomessa Finanssivalvonta määrää finanssialan operatiivisen riskienhallinnan vaatimukset, jotka perustuvat lainsäädäntöön, Euroopan unionin asetuksiin, Euroopan unionin direktiiveihin sekä kansainvälisiin suosituksiin. Tietoturvaan liittyvät vaatimukset on jaoteltu tietoturvariskien hallintaan ja tietoturvatapahtumien käsittelyyn, tietoturvallisuutta koskevaan ohjeistukseen ja koulutukseen, tietoturvallisuuden varmistamiseen tietoverkoissa ja tietoturvallisten palveluiden kehittämiseen. Perusvaatimuksiin kuuluu riittävä tietoturvallisuuden taso suhteutettuna organisaatioon ja sen toimintaympäristöön, tietojen ja järjestelmien omistajien määrittäminen ja tietojen luokittelu, käyttövaltuuksien myöntäminen ja valvominen sekä tietojärjestelmien hallinta. (Finanssivalvonta 2014)

Yksi tärkeimpiä finanssialan tietoturvaa säätelevistä ohjesäännöistä on Euroopan Unionin direktiiveihin pohjautuvat Euroopan pankkiviranomaisten ohjeet tieto- ja viestintätekniikka- (ICT) sekä tietoturvariskien hallinnasta (engl. EBA guidelines on ICT and security risk management, EBA/GL/2019/04), jotka määrittävät finanssilaitoksilta vaadittavat riskinhallintatoimenpiteet. Ohjesäännöissä on eritelty erikseen tietoturvan vaatimukset, joiden yksi osa-alue on tietoturvakoulutus ja -tietoisuus. Sen mukaan finanssilaitoksilla tulisi olla tietoturvatietoisuusohjelman sisältävä tietoturvan koulutusohjelma, jonka avulla voidaan pienentää inhimilliseen virheeseen liittyvää riskiä. (European Banking Authority 2019)

2.2 Tietoturvatietoisuuden kehittäminen

2.2.1 Tietoturvatietoisuus

Tietoturvatietoisuuden (engl. Information Security Awareness, ISA) käsitteen määritelmä perustuu kirjallisuudessa kahteen eri näkökulmaan riippuen käsitteen laajuudesta ja viitekehyksen pohjana käytetystä teoriasta (Parsons ym. 2017). Näkökulmien eroavaisuus on se, nähdäänkö tietoturvatietoisuus vain työntekijöiden kykynä ymmärtää tietoturvan merkitys ja organisaation tietoturvakäytännöt (Wilson & Hash 2003) vai sisältyykö käsitteeseen myös käyttäytyminen tietoturvakäytäntöjen mukaisesti ja sitoutuminen tietoturvaan liittyvien tavoitteiden saavuttamiseen (Kruger & Kearney, 2006; Siponen, 2000). Monissa tutkimuksissa käytetään myös suunnitelmallisen käyttäytymisen teoriasta johdettua käsitettä ”aikomus noudattaa” (engl. intention to comply), jolla tarkoitetaan tietoturvan konseptissa yksilön valmiutta toimia tietoturvakäytäntöjen mukaisesti (Haeussinger & Kranz 2013; Koohang et al. 2020; Bulgurcu ym. 2010). Tässä tutkielmassa käsitellään tietoturvatietoisuutta jälkimmäistä näkökulmaa mukaillen eli käsitteeseen sisällytetään myös työntekijöiden käyttäytyminen.

Siposen (2000) mukaan tietoturvatietoisuudella viitataan tilaan, jossa organisaation työntekijät ovat tietoisia ja sitoutuneita heille asetettuihin tietoturvaan liittyviin tavoitteisiin. Ymmärtääkseen tietoturvaan liittyvät tavoitteet, työntekijät ymmärtävät organisaation tietoturvaan tietoturvakäytännöt (Khan 2011) ja käyttäytyvät niiden mukaisesti (ISF 2002). Tietoturvatietoisuus koostuu kahdesta eri kategoriasta: yleisestä tietoturvatietoisuudesta (engl. general information security awareness) ja tietoisuudesta organisaation tietoturvakäytännöistä (engl. information security policy awareness). Molemmilla on merkittävä vaikutus yksilön ja täten organisaation tietoturvatietoisuuteen. (Bulgurcu ym. 2010)

Tietoturvatietoisuus on tärkeä osa organisaation strategiaa, koska työntekijöiden huolimattomuus, tietoturvaohjeiden noudattamattomuus, huono koulutus ja motivaation puute aiheuttavat organisaatiolle kaikista merkittävimmän tietoturvauhan, jota kutsutaan sisäiseksi uhaksi (engl. insider threat). Sisäinen uhka voi liittyä joko tarkoituksellisen toimintaan tai työntekijän tiedottomuuteen tai välinpitämättömyyteen organisaation tietoturvakäytäntöjä kohtaan. Jälkimmäisessä tapauksessa voidaan puhua päätepisteen tietoturvauhasta. (engl. endpoint security threat) (Warkentin & Willison, 2009) Tietoturvatietoisuuden avulla pyritään vaikuttamaan etenkin tähän ja minimoimaan

ihmisten toimintaan liittyvät tietoturvariskit. Tietoturvatietoisuutta pidetäänkin yhtenä tärkeimmistä menestystekijöistä tietojärjestelmien ja kriittisen tiedon suojaamiseen. (Siponen 2000; Choi ym. 2008) Samaan aikaan on hyvä muistaa, että tietoturvatietoisuuden kehittämien ei ole vain organisaatioille kriittinen menestystekijä tai organisaation sisäinen vaatimus, vaan finanssialan sääntely, kuten EBA/GL/2019/04, vaatii organisaatioita tekemään toimia tietoturvatietoisuuden edistämiseksi (Tsohou ym. 2015).

Niin kuin aiemmin tuli esille, on työntekijöiden käyttäytyminen ja mahdollisesti käyttäytymisen muuttaminen keskeisessä roolissa tietoturvatietoisuudessa. Ei siis ole ihme, että tietoturvatietoisuutta käsittelevä tutkimus perustuu pääasiassa käyttäytymisteorioihin (engl. behavior theories) ja oppimisteorioihin (engl. learning theories). Pääpaino näistä on esimerkiksi psykologiassa ja sosiologiassa paljon hyödynnettävissä käyttäytymisteorioissa, joiden avulla pyritään selittämään työntekijöiden aiottua ja todellista käyttäytymistä (Lebek ym. 2014). Taulukossa 2 on esitetty yleisimmät tietoturvatietoisuuden tutkimuksessa hyödynnetyt teoriat ja selitetty niiden keskeinen sanoma. Monissa tietoturvatietoisuuden tutkimuksissa ei hyödynnetä pelkästään yhtä taulukossa 2 mainituista teorioista, vaan viitekehys muodostetaan integroimalla eri käyttäytymis- ja oppimisteorioita (Khan ym. 2011).

Taulukko 2: Tietoturvatietoisuuden tutkimuksessa hyödynnetyt teoriat

Teoria	Engl.	Selitys
Perustellun toiminnan teoria	Theory of reasoned action (TRA)	Asenteiden ja subjektiivisten normien vaikutus yksilön käyttäytymiseen (Fisbein & Ajzen 1975).
Suunnitelmallisen käyttäytymisen teoria	Theory of planned behavior (TPB)	Laajentaa perustellun toiminnan teoriaa ottaen huomioon havaitut käyttäytymisen kontrollit (Ajzen 1991).
Peloteteoria	General deterrence theory (GDT)	Rangaistus aiheuttaa pelkoa muissa yksilöissä vähentäen samanlaista käytöstä (Gibbs 1975)
Suojelumotivaatioteoria	Protection motivation theory (PMT)	Yksilön käyttäytymiseen vaikuttavat uhkien arviointi ja selviytymisarviointi (Rogers 1975).
TAM-malli	Technology acceptance model (TAM)	Yksilön käyttäytymiseen hyödyntää teknologiaa vaikuttaa teknologiasta koettu hyöty ja helppokäyttöisyys (Davis 1989).
KAB-malli	Knowledge-attitude-behavior -model (KAB)	Yksilön käyttäytymistä voidaan muuttaa lisäämällä yksilön tietoa ja muuttamalla tämän asenteita (Allport 1935).

Niin kuin taulukossa 2 esitetyistä teorioista voidaan havaita, ei käyttäytymisen muutokseen päästä pelkästään lisäämällä tietoisuutta. Se vaatii mahdollisuuden ymmärtää ja soveltaa tietoturvakäytäntöjä sekä motivaatiota tehdä niin – mikä taas vaatii muutosta asenteissa ja aikomuksissa käyttäytyä tietoturvakäytäntöjen mukaisesti. Motivaatio voi olla joko sisäistä tai ulkoista eli käyttäytymisen taustalla voi olla ilo itse tekemisestä tai käyttäytymisen avulla voidaan pyrkiä saavuttamaan jotain. (Bada ym. 2019) Tietoturvakäytäntöjen noudattaminen lähtee usein enemmän ulkoisesta motivaatiosta, mutta oikeiden menetelmien, kuten työntekijöiden osallistamisen avulla, voidaan pyrkiä kasvattamaan myös työntekijöiden sisäistä motivaatiota tietoturvatietoisuutta kohtaan (Siponen 2000).

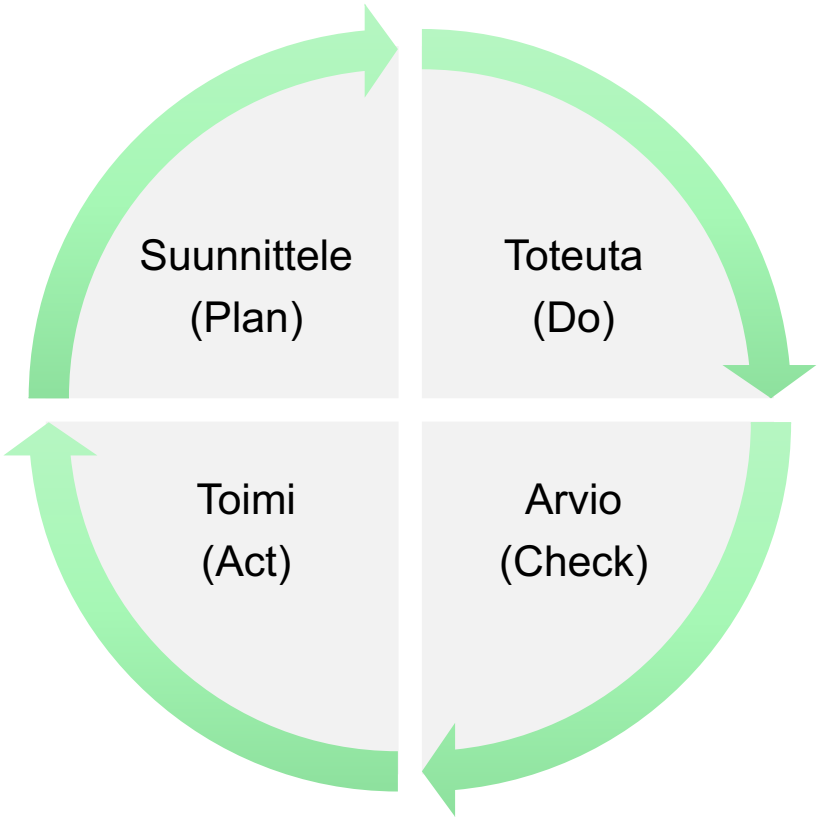
Asenne on keskeinen etenkin perustellun toiminnan ja suunnitelmallisen käyttäytymisen teorioissa, joissa se on ydinkomponentti käyttäytymisen muuttamiseen (Siponen, 2000). Tietoturvatietoisuudessa asenteiden vaikutusta käyttäytymiseen on tutkittu paljon ja esimerkiksi Bulgurcun ym. (2010) sekä Bauerin ja Bernroiderin (2017) tekemien

tutkimuksen mukaan asenne on merkittävä tekijä yksilön aikomuksissa noudattaa organisaation tietoturvakäytäntöjä, kun taas Cox (2012) ei löytänyt merkittävää yhteyttä asenteen vaikutuksesta käyttäytymiseen. Asenteen ja motivaation lisäksi tietoturvatietoisuuteen vaikuttavat luvussa 3 esitettävät yksilölliset, organisatoriset ja välilliset tekijät.

2.2.2 Tietoturvatietoisuuden systemaattinen kehittäminen

National Insitute of Standars and Technologyn (NIST) mukaan ”Jatkuvan kehittämisen tulisi olla aina teema tietoturvatietoisuudessa ja tietoturvaharjoituksissa, sillä se on yksi osa-alue, jossa ei koskaan voi tehdä tarpeeksi” (Wilson & Hash 2003, 35). Muutoksen johtaminen on yksi keskeinen osa-alue tietoturvatietoisuuden kehittämisessä. Teknologiat kehittyvät jatkuvasti tuoden mukanaan uusia tietoturvauhkia ja vaatimuksia tietoturvatietoisuuteen. Lisäksi organisaatiossa tapahtuvat muutokset voivat muuttaa organisaation rakennetta ja organisaatiokulttuuria ja vaikuttaa siihen, mitkä ovat parhaita menetelmiä tietoturvatietoisuuden kehittämiseen. Tämän lisäksi vaikuttavia asioita ovat esimerkiksi muutokset yhteiskunnassa tai ympäröivässä maailmassa, kuten tällä hetkellä vallitseva Venäjän hyökkäyssota Ukrainassa, sekä muutokset tietoturvadirektiiveissä ja muissa vaatimuksissa. (Wilson & Hash 2003).

Kehittämisprosessia voidaan tietoturvatietoisuudessa tulkita esimerkiksi kuviossa 1 näkyvän PDCA-mallin (plan-do-check-act) mukaan, jonka vaiheet ovat suunnittele (engl. plan), toteuta (engl. act), arvioi (engl. check) ja toimi (engl. act) (Bauer ym. 2017). PDCA-malli sopii hyvin tietoturvatietoisuuden kehittämiseen, koska alaluvussa 2.1.1 mainittu, monissa finanssialan organisaatiossa käytössä oleva, ISO/IEC 27000 -standardisarja on suoraan sidonnainen PDCA-mallin mukaiseen jatkuvan kehittämisen malliin (Disterer 2013). PDCA-malli on hyvä työkalu etenkin tietoturvatietoisuusohjelman kehittämiseen, sillä sen avulla voidaan arvioida tietoturvatietoisuusohjelman ja siinä hyödynnettävien menetelmien vaikuttavuutta (Bauer ym. 2017).



Kuvio 1: PDCA-malli (Deming 1952)

PDCA-mallin ensimmäinen vaihe on suunnitteluvaihe, jossa tunnistetaan ja analysoidaan ongelma tai kehityskohde. Toisessa vaiheessa suunnitellaan ja implementoidaan ratkaisut ongelman korjaamiseen. Kolmannessa vaiheessa arvioidaan tulokset ja saavutettiinko asetettu tavoite. Neljännessä vaiheessa tehdään ratkaisuja perustuen arviointivaiheeseen. Jos ratkaisu toimi, integroidaan se osaksi organisaatiokulttuuria, jos taas haluttuihin tavoitteisiin ei päästy, aloitetaan PDCA-mallin mukainen kehitys uudestaan. (Johnson 2002)

Tietoturvatietoisuuden kehittämisessä keskeistä on systemaattisuus, minkä vuoksi organisaatiot ovat kehittäneet viitekehysten ja mallien pohjalta tietoturvatietoisuusohjelmia (engl. Security Awareness Program, Information Security Awareness Program tai Information Security Awareness and Training Program) (Siponen 2000). Information Security Forumin (ISF) mukaan tietoturvatietoisuusohjelma on ”jatkuvaa toimintaa, jonka tarkoituksena on rakentaa ja ylläpitää turvallisuusmyönteistä ympäristöä” (ISF 2007). Tällä viitataan siihen, että tietoturvariskien muuttuessa jatkuvasti, on tietoturvatietoisuusohjelman sanoman ja menetelmien vastattava

ajankohtaisiin tietoturvariskeihin. Tämä on mahdollista, mikäli tietoturvatietoisuus nähdään osana organisaation kulttuuria ja tietoturvatietoisuusohjelmaa johdetaan ja mitataan johdonmukaisesti. (Kruger & Kearney 2006)

Monessa tietoturvatietoisuutta käsittelevässä artikkelissa mainitaan tietoturvatietoisuusohjelmat osana tietoturvatietoisuuden kehittämistä, mutta pelkästään tietoturvatietoisuusohjelmiin keskittyvää tutkimusta ei ole vielä paljon. Tutkimusta on tehty kuitenkin onnistuneen tietoturvatietoisuusohjelman menestystekijöistä (Peltier 2005) ja tietoturvatietoisuusohjelmien ja niissä hyödynnettävien menetelmien tehokkuuden mittaamisesta (Kruger & Kearney 2006; Khan ym. 2011; Bauer ym. 2017). Tämän lisäksi esimerkiksi Kajzer ym. (2014) ovat tutkineet tarkemmin tietoturvatietoisuudessa hyödynnettäviä kampanjoita ja yksilöiden välisiä eroja niiden tehokkuudessa.

Näiden lisäksi esimerkiksi Information Security Forum (ISF), European Union Agency for Cybersecurity (ENISA) ja National Institute of Standards and Technology (NIST) ovat kehittäneet erilaisia oppaita tietoturvatietoisuuden parantamiseen, joita voidaan hyödyntää tietoturvatietoisuusohjelmien kehittämisessä (Tsohou ym. 2015). Tällaisia oppaita ovat esimerkiksi ISF:n (2014) “From Promoting Awareness to Embedding Behaviour”, ENISA:n (2010) ”How to raise security awareness” ja NIST:in ”Building an Information Security Awareness Training Program” (Wilson & Hash 2003). Oppaat tarjoavat käytännön ohjeita tietoturvatietoisuusohjelman rakentamiseen, mutta monet niistä ovat jo melko vanhoja, eivätkä kaikki ole vapaasti käytettävissä. Lisäksi oppaat ovat yleisesti tietoturvatietoisuuden kehittämiseen eivätkä keskity finanssialaan, niin kuin tätä tutkielma. Ne voivat toimia käytännön ohjeina, kun taas tässä työssä tarjotaan laajempi finanssialaan keskittyvä viitekehys.

Tietoturvatietoisuuden kehittäminen ei ole kuitenkaan yksinkertaista, vaan ihmisten asenteiden ja käyttäytymisen muuttamiseen liittyy aina haasteita. Information Security Forumin tekemän tutkimuksen mukaan jopa 85 % tietoturvatietoisuusohjelmista ei saa aikaan toivottua muutosta työntekijöiden käyttäytymisessä (ISF 2014). Tämä haaste liittyy tietoturvallisuustutkimuksessa nykyisin tunnistettuun ongelmaan kuilusta tiedon ja käyttäytymisen välillä, jolla tarkoitetaan tilannetta, jossa työntekijät ovat tietoisia organisaation tietoturvakäytännöistä, mutta he eivät käyttäydy niiden mukaisesti (Cox, 2012).

Albrechtsenin (2007) mukaan syitä ongelman taustalla ovat motivaation puute, ristiriita tietoturvan ja toiminnallisuuden välillä sekä tiedon puute johtuen epätehokkaista menetelmistä ja heikosta tietoturvallisuuden johtamisesta. Näitä tekijöitä voidaan neutralisointiteorian (engl. neutralization theory) mukaan pitää yksilön tapoina oikeuttaa tietoturvakäytäntöjen laiminlyönti (Bauer & Bernroider 2017). Yksi tapa kuvata tätä ongelmaa on niin sanotulla turvallisuuden (engl. security), käytännöllisyyden (engl. functionality) ja käytettävyyden (engl. usability) kolmiolla, joka kuvaa näiden kolmen elementin suhdetta toisiinsa. Olisi tärkeää, että organisaatiossa pystyttäisiin tasapainottamaan kolmio, jotta ristiriitaa turvallisuuden ja toiminnallisuuden välillä voitaisiin helpottaa. (Bada ym. 2019)

Muita syitä tietoturvatietoisuuden kehittämisen epäonnistumiseen voi olla puuttuva tai epäsystemaattinen tietoturvatietoisuuden mittaaminen, vääristyneet odotukset tuloksista, epätehokkaat menetelmät, taidon puute tehokkaaseen tietoturvatietoisuuden kehittämiseen sekä ”one size fits all” -ajattelumalli (ISF 2014). Eri menetelmiin, kuten viestintään ja koulutukseen, liittyviä haasteita tarkastellaan myöhemmin alaluvussa 3.4.

2.2.3 Tietoturvatietoisuuden arviointi ja mittaaminen

Tietoturvatietoisuuden kehittämisessä on tärkeää työn jatkuva arviointi ja mittaaminen (Bauer ym. 2017), mikäli sen avulla halutaan tuottaa arvoa organisaatiolle sekä osoittaa johdolle, mitä organisaatiossa tapahtuu tietoturvan osalta (Kruger & Kearney 2006). Tietoturvatietoisuuden kehittäminen esimerkiksi tietoturvatietoisuusohjelman avulla ei automaattisesti tarkoita, että kaikki työntekijät ymmärtävät ja noudattavat organisaation tietoturvakäytäntöjä, minkä takia on tärkeä jatkuvasti arvioida hyödynnettävien menetelmien tehokkuutta (Khan ym. 2011), onnistumisia ja tulevaisuuden kehityskohteita (SANS 2021). Kehitystä ei ole mahdollista tapahtua, mikäli organisaatiossa ei tiedetä, miten nykyinen tapa kehittää tietoturvatietoisuutta toimii (Wilson & Hash 2003).

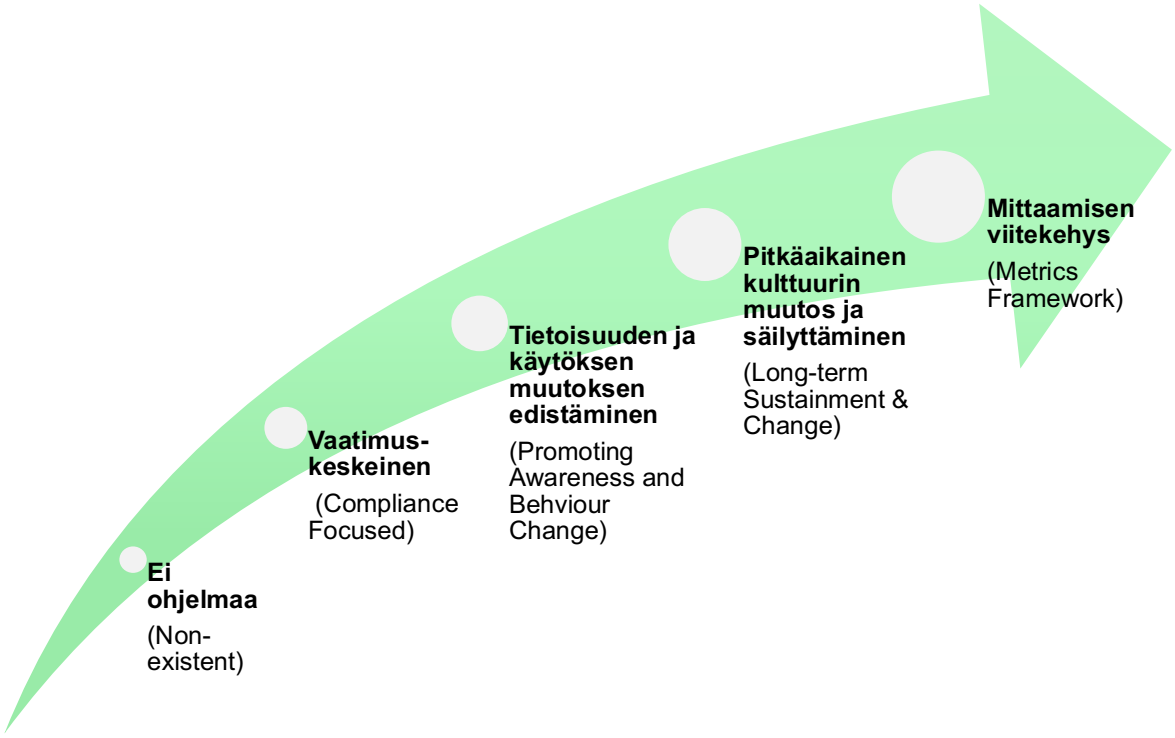
Tietoturvatietoisuuden mittaaminen on tutkimuksessa vielä melko uusi osa-alue ja etenkin tietoturvatietoisuudessa keskeisessä roolissa olevaa ihmisten käyttäytymistä on haastava mitata (SANS 2021). Mittaamiseen voidaan kuitenkin hyödyntää erilaisia keinoja kerätä palautetta. Yleisimpiä keinoja ovat esimerkiksi kyselylomakkeet, fokusryhmähaastattelut, henkilökohtaiset haastattelut, konsultointi ja ulkopuoliset tarkastukset, raportointi sekä esikuva-analyysi (engl. benchmarking). Esikuva-analyysiä

voi ajatella työntekijän näkökulmasta kysymyksellä ”Miten suoriudun verrattuna kollegoihini?” tai vaihtoehtoisesti organisaation näkökulmasta kysymyksellä ”Miten organisaatio suoriutuu tietoturvatietoisuuden kehittämisessä verrattuna muihin saman alan toimijoihin?” (Wilson & Hash 2003)

Tietoturvatietoisuuden systemaattiselle kehittämiselle on tärkeää, että tietoturvatietoisuusohjelmalle asetetaan selkeät mittarit, joiden avulla edistystä voidaan tarkastella. Jotta mittareita voidaan seurata, on myös tärkeää määrittää organisaation lähtötaso ennen tietoturvatietoisuuden systemaattista kehittämistä. Kun lähtötaso on mitattu, voidaan konkreettisesti osoittaa tietoturvatietoisuuden systemaattisen kehittämisen hyödyt. (ENISA 2010) Hyödynnettäviä mittareita tietoturvatietoisuudessa ovat esimerkiksi kerättyjen palautteiden tulokset, tietoturvatapahtumien (engl. information security incident) määrä, tietoturvakoulutusten osallistumisprosentti sekä viestinnän tavoitettavuus ja sitouttavuus (Wilson & Hash 2003).

Tietoturvatietoisuuden arvioinnissa voidaan hyödyntää myös valmiita työkaluja, kuten SANS:in maturiteettimallia (SANS 2022) tai Information Security Forumin ”Standard of Good Practice in Information Security” (ISF 2022). On hyvä huomioida, että osa työkaluista, kuten ”Standard of Good Pratice in Information Security”, ovat maksullisia, joten kaikilla organisaatioilla ei ole välttämättä resursseja näihin. Kuitenkin esimerkiksi seuraavassa kappaleessa esitetty SANS:in maturiteettimalli ja NIST:in työkalut ovat kaikille avoimia, joten ne ovat hyviä keinoja mittaamiseen kehittämisen alussa tai pienissä organisaatioissa.

Kuviossa 3 esiintyvää maturiteettimallia voidaan hyödyntää organisaatioissa, jossa on käytössä tietoturvatietoisuusohjelma tai muu systemaattinen kehitysmalli ja sen avulla organisaatio pystyy tunnistamaan oman tietoturvatietoisuutensa maturiteettitason ja tulevaisuuden kehityskohteet. Tavoitteena on päästä tilaan, jossa tietoturvatietoisuuden mittarit ovat linjassa organisaation mission kanssa, ja niiden avulla voidaan osoittaa tietoturvatietoisuuden arvo organisaation johdolle. (SANS 2022)



Kuvio 2: Maturiteettimalli (SANS 2022)

Maturiteettimallin ensimmäisellä tasolla organisaatiolla ei ole minkäänlaista tietoturvatietoisuusohjelmaa, eivätkä työntekijät ole tietoisia heidän tietoturvavaatimuksistaan tai organisaation tietoturvakäytännöistä. Toisella tasolla organisaation tietoturvatietoisuus keskittyy tiettyjen viranomaisvaatimusten täyttämiseen ja koulutus on vuosittainen pakollinen koulutus. Kolmannella tasolla tietoturvatietoisuutta kehitetään systemaattisesti vuoden ympäri hyödyntäen aktiivisesti viestintää ja erilaisia harjoituksia, joiden seurauksena työntekijät ymmärtävät organisaation tietoturvakäytännöt ja seuraavat niitä sekä osallistuvat aktiivisesti tietoturvatapahtumien raportointiin. Neljännellä tasolla puhutaan pitkän ajan muutoksesta, jossa tietoturvatietoisuus on osa organisaatiokulttuuria. Viimeisellä tasolla tietoturvatietoisuuden mittarit ovat sitoutuneet organisaation missioon, kehitys on jatkuvaa ja tietoturvatietoisuusohjelman avulla voidaan esittää siihen sijoitetun pääoman tuottoaste. (SANS 2022)

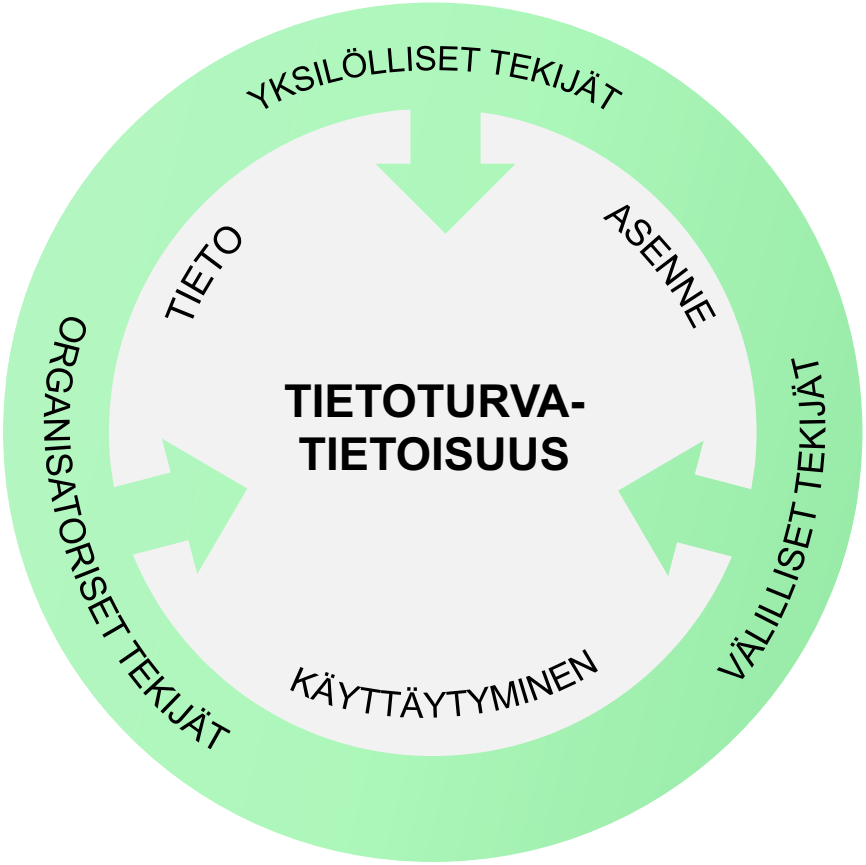
Information Security Forumin (2022) ”Standard of Good Practice in Information Security” on maturiteettimallia laajempi työkalu ja sen avulla voidaan arvioida kokonaisvaltaisesti organisaation tietoturvaa. Osana työkalua ovat SETA-ohjelmat (engl. Security Education, Training and Awareness Program), tietoturvatietoisuuteen liittyvä

viestintä (engl. Security Awarenss Messages) sekä tietoturvakoulutus ja -harjoitukset (engl. Security Education/Training). Työkalu määrittää eri osa-alueiden vaatimukset ja tavoitteet, joihin organisaatio voi peilata omaa toimintaansa. (ISF 2022)

3 Tietoturvatietoisuuteen vaikuttavat tekijät

3.1 Parsons ym. (2017) viitekehys

Kuviossa 4 esiintyvä viitekehys kuvaa tietoturvatietoisuuteen vaikuttavia tekijöitä Parsons ym. (2017) mukaan. Tekijät voidaan jakaa kolmeen eri kategoriaan: yksilöllisiin tekijöihin, organisatorisiin tekijöihin ja välillisiin tekijöihin, mitkä kaikki vaikuttavat yksilöiden tietoon, asenteisiin ja käyttäytymiseen liittyen organisaation tietoturvakäytäntöihin (Parsons ym. 2017). Yksilölliset tekijät sisältävät muun muassa demografiset ja psykologiset tekijät, organisatoriset tekijät organisaatiokulttuurin ja sosiaaliset normit, ja välilliset tekijät viestinnän sekä koulutuksen ja tietoturvaharjoitukset (Parsons ym. 2014). Näitä tekijöitä tarkastellaan tarkemmin alaluvuissa 3.2.–3.4.



Kuvio 3: Tietoturvatietoisuuteen vaikuttavat tekijät (Parsons ym. 2017)

Kirjallisuudessa tietoturvatietoisuuteen vaikuttavia tekijöitä on jaoteltu eri tavalla, vaikka usein samat elementit toistuvat. Khandon ym. (2021) määritelmän mukaan käyttäytymiseen vaikuttavat tekijät tulee huomioida kehitettäessä menetelmiä, joiden avulla työntekijöiden tietoturvatietoisuutta pyritään lisäämään. Tutkielmassa

hyödynnettävässä Parsons ym. (2017) viitekehyksessä välilliset tekijät vastaavat näitä menetelmiä. Haeussinger & Kranz (2013) jakavat tekijät institutionaalisiin tekijöihin, yksilöllisiin tekijöihin ja ympäristötekijöihin. Parsons ym. (2017) mallissa institutionaaliset tekijät vastaavat välillisiä tekijöitä ja ympäristötekijät organisatorisia tekijöitä.

3.2 Organisatoriset tekijät

Tietoturvallisuuden hallinnalla on tutkittu olevan merkittävä vaikutus tietoturvatietoisuuden kehittämiseen. Alaluvussa 2.2.2 yhtenä tietoturvatietoisuuden kehittämisen haasteena nousi esiin heikko tietoturvallisuuden johtaminen, jota tukee myös Albrechtsenin & Hovdenin (2009) tutkimus tietoturvan digitaalisesta kahtiajaosta (engl. digital divide in information security). Tällä tarkoitetaan Albrechtsenin & Hovdenin (2009) mukaan sitä, että tietoturvajohtajat näkevät työntekijät tietoturvauhkana, kun taas työntekijät eivät näe itseään uhkana vaan haluavat olla tietoturvan resurssi. Tämä luottamuksen puute ei edistä tietoturvatietoisuuden kehittämistä, vaan tekee tietoturvajohtajista etäisiä ja johtamisstrategiasta epätehokkaan. Tehdyissä tutkimuksissa tietoturvajohtajien roolissa korostuu vuorovaikutus ja näkyvyys. Ylhäältä alaspäin suuntautuva johtamistapa ei ole tehokas keino tietoturvatietoisuuden kehittämiseen, vaan olisi tärkeää, että tietoturvajohtajat ovat näkyviä työntekijöille ja vuorovaikutus olisi kaksisuuntaista johdon ja työntekijöiden välillä. (Albrechtsen 2007) Toinen tietoturvatietoisuuden kehittämiseen vaikuttava hallinnollinen tekijä on organisaation ylimmän johdon ja hallituksen tuki. Mikäli tietoturva nähdään liiketoimintaa rajoittavana tekijänä tai pelkästään tekniseltä näkökannalta, on tietoturvatietoisuuden kehittäminen ja tietoturvallisen organisaatiokulttuurin luominen haastavaa. (Ashenden 2008)

Yksi tietoturvatietoisuuden kirjallisuudessa esiin nouseva tekijä on organisaatiokulttuurin tai tarkemmin tietoturvakulttuurin vaikutus tietoturvatietoisuuteen. Da Veiga & Eloff (2010) määrittelevät tietoturvakulttuurin yksilöiden asenteiden, uskomusten ja tiedon vuorovaikutukseksi, joka luo organisaatioon käyttäytymismalleja koskien tietoturvakäytäntöjä. Tämä tarkoittaa, että tietoturvakulttuurin tavoitteena on tehdä organisaation tietoturvakäytännöistä automaattisia tapoja toimia. Tietoturvakulttuuri on osa organisaatiokulttuuria ja sillä on osoitettu olevan vaikutus työntekijöiden tietoturvatietoisuuteen (Wiley ym. 2020). Vahvan positiivisen tietoturvakulttuurin

organisaatiossa työntekijöiden näkemys tietoturvasta on organisaation tietoturvakäytäntöjen mukainen (Da Veiga 2018). Osa tietoturvakulttuuria ovat sosiaaliset normit, jotka tarkoittavat työntekijöiden käsitystä hyväksytystä tietoturvakäytäntöjen mukaisesti toiminnasta (Bauer & Bernroider 2017). Sosiaalisten normien muuttaminen on haastavaa, mutta niiden avulla voidaan muuttaa yksilöiden käyttäytymistä ja vaikuttaa etenkin uusien työntekijöiden sitoutumiseen organisaation tietoturvakäytäntöihin (Gjertsen ym. 2017; Lund & Aarø 2004).

3.3 Yksilölliset tekijät

Tietoturvatietoisuuteen vaikuttavat myös monet yksilölliset tekijät, kuten demografiset tekijät ja persoonallisuus (McCormac et al., 2017), yksilöiden aikaisemmat kokemukset, tieto eri tietojärjestelmistä (Haeussinger & Kranz 2013), yleinen tietoturvatietoisuus (Bulgurcu ym. 2010) ja minäpystyvyys (engl. self-efficacy) (Rhee ym. 2009). Nämä taustatekijät luovat eroja yksilöiden välille ja vaikuttavat heidän käyttäytymiseensä epäsuorasti (Bulgurcu ym. 2010).

Tutkimuksissa on osoitettu, että korkea ikä vaikuttaa positiivisesti tietoturvatietoisuuteen, joka johtuu esimerkiksi kokemuksesta ja riskinottoalttiuden vähenemisestä. Sukupuolen ei ole todettu vaikuttavan merkittävästi tietoturvatietoisuuteen. (McCormac ym. 2017; Wiley ym. 2020) Lisäksi yksilöiden persoonallisuudella on tutkittu olevan vaikutusta tietoturvatietoisuuteen. Vaikuttavista persoonallisuuden piirteistä on noussut esiin etenkin tunnollisuus ja sovinnollisuus. (McCormac ym. 2017)

Minäpystyvyydellä tarkoitetaan ihmisen uskomuksia hänen kykyynsä toimia tietyllä tavalla, joka vaikuttaa muun muassa hänen motivaatioonsa ja käyttäytymiseensä (Bandura 1994). Tietoturvatietoisuudessa minäpystyvyydellä viitataan työntekijän käsitykseen hänen taidoistaan, tiedoistaan ja pätevyydestään toimia organisaation tietoturvakäytöntöjen mukaisesti (Bulgurcu ym. 2010). Hyvällä tietoturvan minäpystyvyydellä on osoitettu olevan vahva postitiivinen vaikutus tietoturvakäytäntöjen noudattamiseen (Rhee ym. 2009).

Yksilön aikaisemmat kokemukset voivat vaikuttaa joko negatiivisesti tai positiivisesti yksilön tietoturvatietoisuuteen. Tietoturvatapahtuman uhriksi joutuminen voi heikentää yksilön minäpystyvyyttä ja vaikuttaa negatiivisesti yksilön tietoturvatietoisuuteen (Rhee ym. 2009). Toisaalta altistuminen tietoturvatapahtumalle voi myös lisätä yksilön tietoa

tietoturvauhista ja toimia motivaationa toimia tietoturvallisemmin tulevaisuudessa (Haeussinger & Kranz 2013). On myös osoitettu, että tietojärjestelmien ja yleisesti tietotekniikan hallitseminen parantaa työntekijöiden minäpystyvyyttä ja vähentää tietojärjestelmiin liittyviä tietoturvariskejä (Haeussinger & Kranz 2013; Rhee ym. 2009).

3.4 Välilliset tekijät

3.4.1 Viestintä

Saadakseen työntekijät noudattamaan organisaation tietoturvakäytäntöjä, on ensin pyrittävä lisäämään heidän tietoaan sekä muuttamaan heidän asenteitaan koskien tietoturvaa (Lund & Aarø, 2004). Tähän pyritään tietoturvatietoisuudessa tietoturvatietoisuuskampanjoiden avulla (engl. Information Security Awareness Campaigns). Tietoturvakampanjat ovat tiettyyn teemaan tai kohderyhmään keskittyviä toimia, joiden tarkoituksena on lisätä tietoisuutta tietoturvaan liittyvistä riskeistä ja vastuista (ISF 2008; Kajzer ym. 2014). Niitä ovat esimerkiksi uutiskirjeet, sähköpostiviestintä, näytönsäästäjät, julisteet, koulutusesitykset, videot ja muut viestinnälliset menetelmät (Kajzer ym. 2014; Khan ym. 2011; Albrechtsen 2007).

Viestinnän tarkoituksena on myydä ajatus tietoturvasta työntekijöille ja tehdä siitä niin sanotusti ”in topic” eli herättää työntekijöiden kiinnostus tietoturvaan liittyviä asioita kohtaan (Siponen 2000). Tärkeää onkin, että viestintä tietoturvallisuudesta on paitsi säännöllistä, ajankohtaista ja monipuolista (Kruger & Kearney 2006), niin myös helposti ymmärrettävää ja käyttäjäystävällistä. Esimerkiksi visuaaliset materiaalit ja lyhyet tekstit toimivat paremmin kuin pitkät raportit ja artikkelit. (Eminağaoğlu ym. 2009) Shaw ym. (2009) puhuvat tiedon rikkaudesta (engl. information richness), jota lisäämällä parannetaan median kykyä lisätä käyttäjien tietoa ja ymmärrystä halutusta aiheesta. Tiedon rikkautta voidaan parantaa esimerkiksi monikanavaisuudella, personoinnilla ja kielen moninaisuudella. Viestinnän ei tulisi olla kaikille samanlaista, vaan siinä tulisi ottaa huomioon yksilöiden persoonallisuuksien väliset erot esimerkiksi ajattelumalleissa (Kajzer ym. 2014).

Tietoturvallisuuskampanjoiden avulla voidaan lisätä työntekijöiden tietoisuutta tietoturvaan liittyvistä riskeistä ja niiden ehkäisemisestä sekä muuttaa asenteita tietoturvaan liittyen. On kuitenkin hyvä muistaa, että tehokkaan ja sitouttavan viestinnän luominen ei ole yksinkertainen tehtävä (Tsohou ym. 2008) ja pelkästään yksisuuntainen

viestintä ei tutkimusten mukaan muuta työntekijöiden tietoturvakäyttäytymistä (Albrechtsen 2007; Khan ym. 2011; Lund & Aarø 2004). Toisaalta Khanin (2011) mukaan tieto on ensimmäinen askel tietoturvatietoisuuden kehittämisessä ja ilman sitä ei voida saavuttaa muutosta työntekijöiden tietoturvakäyttäytymisessä. Myös Hwangin ym. (2021) mukaan työntekijöiden motivoiminen tietoturvavaatimusten noudattamiseen lähtee siitä, että ymmärretään, miten työntekijöiden huomio voidaan kiinnittää tietoturva-asioihin. On tärkeä huomioida, että mikään tekniikoista ei ole yksinään riittävä keino tietoturvatietoisuuden lisäämiseen ja tietoturvakäytäntöjen noudattamisen parantamiseen, vaan tehokkain lopputulos saadaan muodostamalla toisiaan tukeva kokonaisuus ja integroimalla se osaksi organisaation toimintaa (Puhakainen & Siponen 2010).

3.4.2 Harjoitukset ja koulutus

Toinen tietoturvatietoisuuden kehittämisen menetelmistä on harjoittelu ja koulutus (Siponen 2000). Ensinnäkin on tärkeä huomioida, että tietoturvatietoisuus, tietoturvaharjoittelu (engl. information security training, IST) ja tietoturvakoulutus (engl. information security education, ISE) ovat erillisiä käsitteitä, vaikka niitä saatetaan käyttää keskenään vaihtokelpoisesti (Amankwa ym. 2014). Lisäksi tietoturvatietoisuuden tutkimuksissa on eroavaisuuksia, lasketaanko harjoittelu ja koulutus osaksi tietoturvatietoisuutta vai ovatko ne oma osa-alueensa (Tsohou ym. 2008). Esimerkiksi Wilsonin ja Hashin (2003) mukaan tietoturvatietoisuus on vain perusta tietoturvaharjoituksille ja -koulutukselle, kun taas Siposen (2000) mukaan harjoitukset ja koulutus ovat osa tietoturvatietoisuutta. Tässä tutkielmassa noudatetaan Siposen (2000) näkökulmaa.

Tietoturvaharjoittelulla pyritään vastaamaan kysymykseen ”miten?” ja sen avulla pyritään kehittämään työntekijöiden osaamista ja pystyvyyttä vastata organisaation tietoturvakäytäntöihin. Tietoturvakoulutuksella pyritään vastaamaan kysymykseen ”miksi?” ja se on keskeisessä roolissa motivoimaan yksilöä tietoturvalliseen käyttäytymiseen. (Siponen, 2000) Sekä harjoitukset, että koulutus on tärkeä osa tietoturvatietoisuusohjelmia, joita voidaan kutsua myös SETA-ohjelmiksi (engl. Security Education, Training and Awareness Program) (D’Arcy ym. 2009; Haeussinger ym. 2015; Khando ym. 2021).

Mahdollisuuksia tietoturvaharjoitusten toteuttamiseen on monia ja niissä on eroja esimerkiksi liittyen interaktiivisuuteen, dynaamisuuteen ja toteutustapaan (HoxHunt

2022a). Eri tietoturvatietoisuusharjoitusten tehokkuutta on tutkittu paljon ja tutkimuksissa on noussut erityisesti esiin käyttäjien osallistamisen merkitys esimerkiksi workshoppien tai ryhmässä jaettujen kokemusten avulla (Albrechtsen 2007; Khan ym. 2011). Tämä mahdollistaa opitun yhdistämisen käytännön työtapoihin ja yhteisöllisen tiedon luomisen (Karjalainen 2011). Tietoturvaharjoituksissa on myös todettu pätevän sama periaate kuin viestinnässä; harjoitusten ei tulisi olla kaikille samanlaisia. Tehokasta on mukauttaa harjoituksia kohderyhmien mukaan ja varmistaa niiden asiaankuuluvuus työntekijöille hyödyntäen esimerkiksi työntekijän omaan työnkuvaan liittyviä esimerkkejä. (Puhakainen & Siponen 2010; Thomson & Von Solms 1998)

Yksi tietoturvaharjoitusten muoto on pelillistäminen, jonka on todistettu olevan yksi tehokkaimmista keinoista tietoturvatietoisuuden kehittämiseen (Khando ym. 2021). Esimerkiksi Ghazvinin ja Shukurin (2018) tekemässä tutkimuksessa pelillistäminen kasvatti työntekijöiden tietoturvatietoisuutta ja paransi heidän asenteitaan tietoturvaan liittyvää koulutusta kohtaan. Pelillistämisellä (engl. gamification) tarkoitetaan, että koulutukseen lisätään pelillisiä elementtejä osallistujien sitouttamiseksi (Marriam-Webster 2022). Työntekijöiden motivaation puute on yksi yleisimpiä haasteita tietoturvakoulutuksessa ja -harjoituksissa ja pelillistämisen keskeinen tavoite on motivoida ihmisiä muuttamaan käyttäytymistä ja saavuttamaan omat tavoitteensa, jotka ovat taas linjassa organisaation tavoitteiden kanssa (Burke 2016).

Gjertsen ym. (2017) on tutkinut tietoturvaturvatietoisuuden näkökulmasta pelillistämistä ja etenkin tekijöitä, jotka vaikuttavat työntekijöiden motivaatioon osallistua pelillistettyihin harjoituksiin ja täten parantaa oppimistuloksia. Tutkimuksen mukaan pelillistämisessä keskeisiä tekijöitä ovat käyttäjän autonomia eli tämän mahdollisuus vaikuttaa harjoituksen kulkuun sekä se, että koulutuksia voi suorittaa joustavammin ja pidemmällä aikavälillä. Tämä pelillistämiselle tyypillinen mikro-oppiminen mahdollistaa muun työn ohella tehtävät lyhyet ja informatiiviset oppimishetket, jotka voivat taas pienentää alaluvussa 2.2.2 esitettyä ristiriitaa tietoturvan ja toiminnallisuuden välillä. (Gjertsen ym. 2017)

3.4.3 Palkitseminen ja rankaiseminen

Palkitseminen ja rankaiseminen ovat välineellisen ehdollistumisen (engl. operant learning) keinoja oppimiseen ja niitä voidaan hyödyntää yhtenä keinon tietoturvatietoisuuden parantamisessa (Thomson & Von Solms 1998). Välineellisellä

ehdollistumisella tarkoitetaan, että käyttäytyminen muuttuu vahvistuksen tai rangaistuksen kautta (Critchfield 2012).

Rankaisemisen lisäksi voidaan hyödyntää negatiivista vahvistamista (engl. negative reinforcement), jonka erona rankaisemiseen on se, että se tapahtuu ennen mahdollista rikettä kun taas rankaiseminen tapahtuu rikkeen jälkeen (Siponen 2000). Tästä esimerkkinä on tietoturvatietoisuuden tutkimuksessa hyödynnetty peloteteoria (engl. deterrence theory) (D'Arcy ym. 2009), joka korostaa negatiivisen vahvistajan merkitystä halutun käyttäytymisen saavuttamisessa. Siinä ajatuksena on saada työntekijät ymmärtämään, että tietoturvakäytäntöjen laiminlyönnillä on seurauksia ja täten niitä kannattaa noudattaa. (Bulgurcu ym. 2010) Yksi peloteteoriasta juurensa juontanut tekniikka on työntekijän tietokoneen valvonta (engl. computer monitoring), jonka avulla pyritään saamaan työntekijät noudattamaan tietoturvakäytäntöjä saamalla heidät ymmärtämään väärinkäytön seuraamukset. Kun he ovat tietoisia valvonnasta, ymmärtävät he myös todennäköisyyden seuraamuksille. (D'Arcy ym. 2009).

Rangaistusten lisäksi ulkoisena motivaationa voidaan käyttää myös palkintoja, joiden avulla pyritään kannustamaan työntekijöitä noudattamaan tietoturvakäytäntöjä (Bulgurcu ym. 2010). Palkitseminen voi olla osa positiivisen tietoturvakulttuurin luomista, jolloin työntekijöitä palkitaan toivotusta tietoturvaan liittyvästä käyttäytymisestä (Da Veiga 2018). Yksi käytännön keino hyödyntää palkitsemista tietoturvatietoisuuden kehittämisessä on edellisessä alaluvussa mainitun pelillistämisen yhteydessä, jossa työntekijöitä voidaan palkita onnistumisista tai vaihtoehtoisesti aktiivisesta osallistumisesta (Gjertsen ym. 2017). Palkitsemista ja rankaisemista voidaan hyödyntää myös sosiaalisen oppimisen näkökulmasta. Kun työntekijät näkevät, että toivotusta käyttäytymisestä palkitaan, käyttäytyvät he todennäköisemmin samalla tavalla. (Thomson & Von Solms 1998)

Palkitsemista tai rankaisemista voidaan hyödyntää tietoturvatietoisuuden kehittämisessä, mutta on hyvä muistaa, että ne toimivat usein yksilölle enemmän ulkoisina motivaatiotekijöinä (Bada ym. 2019), vaikkakin on mahdollista, että positiivinen vahvistaminen voi jossain tapauksissa lisätä yksilöiden sisäistä motivaatiota. Lisäksi, jos palkitsemista hyödynnetään esimerkiksi pelillistämisen yhteydessä, on hyvä huomioida, että siitä ei tuli liian hallitseva elementti. Mikäli käyttäjä ei koskaan saa palkintoa, voi

palkitseminen helposti kääntyä epämotivoivaksi ja heikentää koulutuksen tehokkuutta. (Gjertsen ym. 2017)

4 Metodologia

4.1 Tieteenfilosofiat

Tietoturvatietoisuudessa keskeisessä roolissa on ihmisten käyttäytyminen ja sen muuttaminen, minkä vuoksi tutkimuksen tieteenfilosofiaksi sopii yksilön subjektiivista kokemusta korostavat suuntaukset, joissa hyödynnetään usein laadullista tutkimusta. Näitä tieteenfilosofioita ovat esimerkiksi konstruktivismi ja interpretivismi (Jyväskylän yliopiston Koppa 2015).

Konstruktivismin mukaan tieto rakentuu yksilön omien kokemuksien, havaintojen ja sosiaalisen vuorovaikutuksen seurauksena ja sen keskipisteessä on yksilön subjektiivinen kokemus. Konstruktivismia käytetään paljon psykologisessa tutkimuksessa (Fosnot 2013) ja niin kuin alaluvussa 2.2.1 mainittiin, tietoturvatietoisuutta tutkitaan usein käyttäytymis- ja oppimisteorioiden avulla. Eri teorioissa tietoturvatietoisuuteen liittyvää käyttäytymistä tutkitaan eri näkökulmista, kuten päätöksenteon, asenteiden ja käytettävyyden kautta (Lebek ym. 2014.), jotka sopivat konstruktivismin yksilölliseen käsitykseen.

Interpretivismi korostaa konstruktivismin tavoin yksilön subjektiivisia tulkintoja ja etenkin yksilön roolia sosiaalisena toimijana. Se sopii esimerkiksi organisaatiokäyttäytymisen, markkinoinnin ja johtamisen tutkimiseen (Saunders ym. 2007), jotka ovat keskeisiä myös tietoturvatietoisuuden kehittämisessä. Wallin & Palvin (2021) mukaan interpretivismin näkökulmasta voidaan saavuttaa syvempi ymmärrys niin tietoturvan hallinnasta kuin työntekijöiden käsityksistä, uskomuksista ja asenteista tietoturva-asioita kohtaan. Ymmärtämällä näitä, voidaan organisaatiossa löytää tietoturvatietoisuuteen vaikuttavat keskeiset tekijät ja tehokkaat menetelmät tietoturvakäytäntöjen implementoimiseen. Interpretivismin mukaisesti myös tietoturvatietoisuuden kehittämisessä on tärkeää ottaa huomioon jokaisen organisaation uniikki luonne (Saunders ym. 2007).

4.2 Tutkimusmenetelmä ja -strategia

Alaluvussa 4.1. mainittuja tieteenfilosofioita mukaillen tutkielman tutkimusmenetelmäksi valikoitui laadullinen eli kvalitatiivinen tutkimusmenetelmä. Laadullisen tutkimusmenetelmän avulla tutkittavaa ilmiötä voidaan tulkita ja ymmärtää

kokonaisvaltaisesti sosiaaliset ja kulttuuriset tekijät huomioiden. Lisäksi laadullisen liiketoimintatutkimuksen (engl. qualitative business research) avulla tutkittavaa ilmiötä voidaan tarkastella sen todellisessa liiketoimintaympäristössä. (Eriksson & Kovalainen 2015) Tässä tapauksessa laadullisen tutkimuksen tarjoama mahdollisuus liittää ilmiö organisaation liiketoimintaympäristöön mahdollistaa parhaiden toimintamallien löytämisen tietylle toimialalle.

Tutkielmassa tarkastellaan tietoturvatietoisuutta eri finanssialan organisaatioissa, minkä takia tutkimusstrategiaksi valikoitui vertaileva tapaustutkimus. Tapaustutkimuksessa keskitytään tutkimaan yksittäistä tai useampaa tapausta kokonaisvaltaisesti ja ratkaisemaan tutkimuskysymyksissä esitetty ongelma (Eriksson & Kovalainen 2015). Vertaileva tapaustutkimuksessa on tapaustutkimuksen muoto, jossa tarkastellaan eri tapausten välisiä yhtäläisyyksiä ja eroja (Kaarbo & Beasley 1999).

4.3 Aineistonkeruumenetelmä

Tutkielman aineistonkeruumenetelmäksi valikoitui puolistrukturoidut teemahaastattelut. Tuomen ja Sarajärven (2018) mukaan ”Kun haluamme tietää, mitä ihminen ajattelee tai miksi hän toimii niin kuin toimii, on järkevää kysyä asiaa häneltä”. Puolistrukturoiduissa teemahaastatteluissa tarkkojen kysymysten sijaan rakennetaan teemoihin pohjautuva haastattelurunko. Teemahaastattelu mahdollistaa keskusteluhenkisen haastattelumuodon, jonka avulla pystytään selvittämään laajemmin yksilön ajatuksia, kokemuksia ja tunteita. (Hirsjärvi & Hurme 1995) Tutkittaessa tietoturvatietoisuuden kaltaista moniulotteista ilmiötä, jossa mielipiteitä ja näkökulmia on monia, tarjoaa teemahaastattelu mahdollisuuden ymmärtää haastateltavien näkökulmia monipuolisesti. Haastattelu voi esimerkiksi keskittyä hieman eri asioihin riippuen siitä, kuinka pitkällä tietoturvatietoisuuden kehittäminen on tutkittavassa organisaatiossa sisältäen kuitenkin samaan aikaan tutkielman tutkimuskysymyksille keskeiset teemat.

Tehdyn tutkimuksen tavoitteena oli saada selville mahdollisimman kattavasti, miten tietoturvatietoisuutta voidaan kehittää systemaattisesti. Kehittämisnäkökulman vuoksi haastatteluihin valittiin tietoturvatietoisuuden kehittämisessä mukana olleita tietoturva-asiantuntijoita eri suomalaisista finanssialan organisaatioista. Organisaatioiden valinnassa huomioitiin muun muassa organisaation koko, rakenne ja tietoturvatietoisuuden kehityksen taso. Tutkimuksen moninaisuuden vuoksi haastateltaviin haluttiin valita näiltä ominaisuuksiltaan eroavia organisaatioita.

Yhtiömuotoja tai tarkempia kokoluokkia ei esitetä tutkimuksessa haastateltavien anonymiteetin säilyttämiseksi. Kokoluokittelussa on kuitenkin noudatettu Euroopan Unionin mukaista määritelmää, jonka mukaan suureksi organisaatioksi määritellään yritys, jonka henkilöstö on yli 250 työntekijää (Tilastokeskus 2022). Haastateltavat on esitelty tarkemmin taulukossa 3.

Taulukko 3: Kuvaus haastateltavista

Haastateltava	**Haastattelun kesto**	**Haastateltavan rooli**	**Organisaatio**
Haastattelu 1 (H1)	70 min	Tietoturvajohtaja	Organisaatio A
Haastattelu 2 (H2)	89 min	Tietoturvapäällikkö	Organisaatio A
Haastattelu 3 (H3)	77 min	Tietoturvapäällikkö	Organisaatio B
Haastattelu 4 (H4)	103 min	Tietoturva-asiantuntija	Organisaatio B
Haastattelu 5 (H5)	55 min	Tietoturvajohtaja	Organisaatio C
Haastattelu 6 (H6)	60 min	Alueellinen tietoturvajohtaja	Organisaatio D

Haastattelukysymysten teemat laadittiin perustuen kirjallisuuskatsaukseen. Teemoja oli yhteensä neljä: organisaation tietoturvatietoisuus, tietoturvatietoisuuteen vaikuttavat tekijät, tietoturvatietoisuuden kehittämisen menetelmät ja tietoturvatietoisuuden mittaaminen ja arviointi. Haastattelukysymyksiä oli yhteensä 26, mutta kaikkia kysymyksiä ei kysytty kaikissa haastatteluissa. Kaikissa haastatteluissa hyödynnettiin valmista kysymysrunkoa, mutta puolistrukturoidun teemahaastattelun mukaisesti haastattelut olivat keskustelevia ja yksilöllisiä. Haastattelut toteutettiin joko Microsoft Teamsin välityksellä tai paikan päällä. Kaikki haastattelut nauhoitettiin haastateltavien luvalla tulosten tarkempaa analysointia varten. Haastattelut kestivät tunnista puoleentoista tuntiin.

4.4 Aineiston analysointi

Aineiston sisällönanalyysin tarkoituksena on luoda selkeä kuva tutkittavasta ilmiöstä luoden aineistosta tiivis, mutta keskeiset asiat sisältävä kokonaisuus. Sisällönanalyysiä voi ohjata joko aineisto tai teoria tai näiden välimuoto (Tuomi & Sarajärvi). Tässä

tutkimuksessa hyödynnettiin viimeistä vaihtoehtoa eli aineiston analysointi toteutettiin teoriaohjaavalla analyysillä. Tässä analyysin muodossa teoria toimii analyysin apuna, mutta analyysi ei pohjaudu suoraan teoriaan. Tehty tutkimus ei testaa jo olemassa olevaa teoriaa tai hyödynnä valmista viitekehystä, mutta aikaisempi tutkimus ohjaa aineiston analysointia. Teoriaohjaavassa analyysissä tutkija hyödyntää abduktiivista ajattelua, jossa yhdistetään aineistolähtöisyyttä ja aiemman tutkimuksen valmiita teorioita. (Tuomi & Sarajärvi 2018)

Tässä tutkimuksessa haastatteluiden analysointi eteni teoriasta johdettujen haastattelukysymysten teemojen mukaan eli teoria ohjasi analyysiä, mutta ideana ei ollut testata esimerkiksi valmista viitekehystä. Kun tuloksia analysoidessa empiriasta löydettiin keskeisiä asioita, verrattiin niitä teoriassa esiin tulleisiin ilmentymiin. Analyysissä pyrittiin ottamaan huomioon mahdollisimman laajasti eri näkökulmat, jotta teoria ei ohjaisi liikaa analyysiä vaan tuloksia pystyttäisiin katsomaan uudesta näkökulmasta. Lopulta aineiston analysoinnin jälkeen tuloksista muodostettiin viitekehys tietoturvatietoisuuden systemaattiseen kehittämiseen.

Ennen aineiston analyysin aloittamista, aineisto litteroitiin peruslitteroinnin tarkkuudella. Tämän jälkeen aineiston analyysissä edettiin Tuomen ja Sarajärven (2018) esittämän rungon mukaan. Ensimmäisessä vaiheessa päätettiin, mikä aineistossa kiinnostaa. Tässä tutkimuksessa tutkimuskysymykset toimivat apuna tutkimukselle keskeisten asioiden etsimisessä. Toisessa vaiheessa aineisto käytiin läpi ja merkittiin asiat, jotka tukivat kiinnostuksen kohdetta sekä merkittiin ne ylös. Tässä vaiheessa aineiston analyysiin hyödynnettiin koodaamista. (Tuomi & Sarajärvi 2018)

Koodaamisella tarkoitetaan aineiston jäsentelyä, jonka avulla voidaan löytää tutkimusongelmalle keskeiset osat aineistosta. Koodaamista voi toteuttaa hyvin eri tavoin hyödyntämällä esimerkiksi merkkejä, kirjaimia tai muita jäsentelyä, kuten yliviivausta. (Kauppinen & Puusniekka 2009) Tässä tutkielmassa koodaaminen suoritettiin yliviivaamalla tutkimuskysymyksille keskeisiä löytöjä kaikista haastatteluista ilman tarkempaa luokittelua. Analysoinnin kolmannessa vaiheessa aineisto teemoiteltiin eli ryhmiteltiin eri aihepiirien mukaan ja tyypiteltiin eli tiettyjen teemojen sisältä etsittiin yhteisiä näkemyksiä. Tässä tutkielmassa aineiston teemoittelu suoritettiin teoriaan pohjautuvien haastatteluteemojen mukaisesti. Eri sitaatit kerättiin valittujen teemojen alle taulukkoon, jonka jälkeen aineisto tyypiteltiin eli aineistosta etsittiin toistuvia tai muuten

mielenkiintoisia nostoja. Vaiheessa neljä muodostettiin yhteenveto eli luku 5, jossa kuvaillaan tutkimuksen tulokset analyysin perusteella. (Tuomi & Sarajärvi 2018)

5 Tutkimuksen tulokset

5.1 Tietoturvatietoisuus finanssialalla ja tutkittavissa organisaatioissa

5.1.1 Tietoturvatietoisuus finanssialalla

Haastatteluiden ensimmäinen teema käsitteli organisaatioiden taustoja tietoturvatietoisuuden kehittämisessä sekä tietoturvatietoisuutta finanssialalla. Ensin on hyvä huomioida tutkimuksessa mukana olleiden organisaatioiden erot koossa ja organisaatiorakenteessa, jotka tulivat usein esille haastatteluiden aikana. Niin kuin alaluvussa 4.3. mainittiin, perustuu tutkielman luokittelu Euroopan Unionin määritelmään, jonka mukaan suuryritykseksi lasketaan organisaatio, jonka henkilöstö on yli 250. Haastateltavissa organisaatioissa on kuitenkin merkittäviä eroja tämän luokan sisällä, jotka vaikuttavat tietoturvatietoisuuden kehittämiseen. Esimerkiksi suuremmassa organisaatiossa voi olla enemmän resursseja, kun taas hieman pienemmässä voi työntekijät olla helpompi tavoittaa ja kehitys voi olla joustavampaa.

> (H3) Että kyllä me on välillä naureskeltu sitä, että jaetaan tämä Suomi silleen sektoreihin, että minä lähden turneelle tuonne Itä-Suomeen ja me näemme sitten 3 vuoden kuluttua. -- Jos me tänä vuonna tehdään se koko turneen suomen ympäri niin me päästy edes puoleenväliin vielä ja sitten se pitäisi ottaa uudestaan seuraavana vuonna.

Osa organisaatioista on osuustoiminnallisia, kun taas osa konserneja. Yksi organisaatio on myös kansainvälinen konserni, jota koskevassa haastattelussa keskityttiin Suomen aluekonttoriin. Organisaatiorakenteelliset seikat tulivat esille haastatteluissa jonkin verran, etenkin puhuttaessa tietoturvatietoisuuden kehittämiseen liittyvistä haasteista. Etenkin osuustoiminnallisissa organisaatioissa haasteena nähtiin organisaatioiden suuruus sekä etäisyys osuuspankkeihin. Kokonaiskuvassa tietoturvatietoisuuden kehittämiselle keskeiset asiat koettiin kuitenkin organisaatiorakenteesta huolimatta hyvin samankaltaiseksi. On kuitenkin sopivien menetelmien valitsemisen vuoksi tärkeätä huomioida organisaation taustatekijät, kun tietoturvatietoisuutta lähdetään kehittämään.

> (H5) Organisaatiolle se etäisyys on vaikuttanut myös, kun me mietimme, että me pankkikeskuksessa annetaan ohjeita yksittäisille pankeille, jotka ovat omia yrityksiä, niin he kokevat sen ehkä liian määräilevänä.

Keskusteluissa tietoturvan merkityksestä finanssialalla nousi esiin pitkälti samat teemat kuin teoriaosuudessa: asiakkaiden luottamuksen säilyttäminen, finanssialaa ohjaava

sääntely ja finanssialalla suojattavat tieto ja raha. Toisaalta haastatteluissa tuli esille, kuinka edellä mainitut paitsi korostavat tietoturvatietoisuuden roolia, myös saattavat helpottaa tietoturvakulttuurin luomista ja tietoturvan resursointia verrattuna muihin toimialoihin.

> (H2) Eli se asiakkaan luottamus tässä tapauksessa, kun se on finanssialalla kaikki kaikessa, niin se on aika ilmeinen kytkös, että jos siellä tötöillään niin asiakaslupaus katoaa ja asiakaskato saattaa iskeä vastaan.

> (H3) Meillä on enemmän tuota regulaation kautta tulevaa perustetta siihen, että me pystymme samaan siihen ehkä enemmän resursseja.

Toisaalta, vaikka vaatimuspohjaisuus voi edesauttaa tietoturvan resursointia finanssialalla ja pankkisalaisuuden kautta työntekijät voivat ymmärtää paremmin tiedon huolellisen käsittelyn tarpeen, eivät organisaatiot voi tuudittautua ajatukseen työntekijöiden automaattisesta tietoturvalähtöisyydestä. Tästä kertoo esimerkiksi se, että kahdessa organisaatiossa tietoturvatietoisuuden kehittämisen syynä oli ainakin osittain tietoturvaan liittyvä tapahtuma, joka edesauttoi tietoturvatietoisuuden kehittämistä sekä siihen vaativan resursoinnin saamista, vaikka tapahtumasta ei aiheutunut organisaatiolle sen suurempaa vahinkoa. Lisäksi haastatteluissa ilmeni hyvin tietoturvatietoisuuden olevan edelleen melko tuore aihe, jopa tietoturvan edelläkävijänä pidetyllä finanssialalla ja kehitys on edelleen hyvin sidonnaista tiettyihin henkilöihin. Organisaatiokohtaista tietoturvaa käsitellään tarkemmin seuraavassa alaluvussa.

> (H4) On helppo olettaa, että kun me olemme vahvasti reguloidulla toimialalla, niin ihmiset, jotka hakeutuvat finanssialalle töihin lukisivat kaikki regulaatiot ja ymmärtäisivät ne. Eihän se ole silleen, me olemme kaikki vaan ihmisiä.

> (H1) Kun lähdettiin kehittämään, niin siinä oli ihan selkeä syy ja se oli semmoinen, että meillä oli tietoturvapoikkeama.

5.1.2 Organisaatioiden tietoturvatietoisuus

Taulukossa 4 on kuvattu, miten tietoturvatietoisuutta kehitetään tutkittavissa organisaatioissa. Haastatteluissa käytiin läpi, kuinka pitkään ja miksi tietoturvatietoisuutta on lähdetty kehittämään. Lisäksi keskusteltiin siitä, miten tietoturvatietoisuuden kehitys on käytännössä organisoitu tutkittavissa organisaatioissa sekä siitä, mihin standardeihin, työkaluihin, viitekehyksiin tai muihin mahdollisiin malleihin tietoturvatietoisuuden kehittäminen pohjautuu.

Taulukko 4: Organisaatioiden tietoturvatietoisuus

Organisaatio	Tietoturvatietoisuuden kehitys	Tietoturvatietoisuus-ohjelma	Viitekehys/ standardi
Organisaatio A	3–4 vuotta	Kyllä	ISO/IEC 27000, Standard of Good Practice in Information Security, ulkopuolisen konsultin materiaali
Organisaatio B	2–3 vuotta	Kyllä	ADKAR, ulkopuolisen konsultin materiaali, ”moments that matter”, SANS maturiteettimalli
Organisaatio C	0–1 vuotta	Ei (tulossa)	ISO/IEC 27000
Organisaatio D	Ei tarkkaa määritelmää, useamman vuoden	Ei suoraan, järjestelmällinen ja toistuva koulutus ja viestintä	Standard of Good Practice in Information Security

Niin kuin taulukosta voidaan havaita ja alaluvussa 5.1.1 mainittiin, on tietoturvatietoisuuden systemaattinen kehittäminen vielä finanssialalla melko tuore aihe ja tuloksista ilmeni, että usein ennen varsinaista tietoturvatietoisuusohjelman kehittämistä, tietoturvatietoisuus nojaa usein vahvasti pelkästään tietoturvakoulutukseen ja viestintään, mutta systemaattiset toimenpiteet tai kulttuurin kehittäminen eivät ole vielä osa tietoturvatietoisuuden kehittämistä.

Haastatteluissa kävi hyvin ilmi, kuinka iso ja pitkäjänteinen projekti tietoturvatietoisuuden systemaattinen kehittäminen on ja kuinka se vaatii resursseja ja koko organisaation sitoutumista. Lähdettäessä toteuttamaan systemaattista tietoturvatietoisuuden kehittämistä, olisi myös tärkeä määrittää, miten ohjelma toteutetaan, mitkä ovat sen tavoitteet ja mitä hyötyä siitä on organisaatiolle. Mikäli tietoturvatietoisuudella halutaan saavuttaa hyötyä organisaatiolle, on kehittämisen oltava systemaattista eikä pelkästään hajanaisia yksittäisiä toimia ilman menetelmien arviointia ja kokonaisvaltaista mittaamista (Kruger & Kearney 2006). Projektin pitkäjänteisyys ja resurssivaatimukset voivat selittää, miksi tietoturvatietoisuuden systemaattinen kehitys onkin usein lähtöisin tietoturvapoikkeamasta tai yksittäisestä henkilöstä niin kuin alaluvussa 5.1.1 mainittiin. Tietoturvatietoisuuden kehittämiseen ei haluta pistää resursseja ”ennen kun on pakko” tai ennen kuin joku alkaa ajamaan sitä voimallisesti eteenpäin organisaatiossa.

> (H2) Tässä talossa ei oikein ollut sellaista systemaattista tietoturvatietoisuutta kehittävää ohjelmaa, taikka menettelyä, vaan se oli sellaisia hajanaisia ilmentymiä koulutuksen tai infojen muodossa.

> (H4) Niin me tehtiin tämä silleen, tämä kyberturvallisuuden kulttuurinmuutos, että me tiedettiin, että tämä on niin kun useamman vuoden ja tulee maksamaan paljon rahaa.

> (H4) – Kyllähän me saamme johdon tuen, mutta meillä pitää olla ensin joku viesti, mikä me menemme kertomaan. Sinne on turha mennä sanomaan, että tarvitaan lisää rahaa johonkin tai että ollaan kauhean huolissaan, jos meillä ei ole myöskin kertoa, että mikä se asia on, miten se raha käytetään tai miten se huoli poistetaan --.

Haastateltavat finanssialan organisaatiot olivat hyödyntäneet erilaisia viitekehyksiä tietoturvatietoisuuden kehittämiseen, mutta keskeisinä nousivat esiin ISO/IEC 27000 -standardisarja sekä Information Security Forumin (ISF) ”Standard Of Good Practice in Information Security”, jotka tulivat esiin myös kirjallisuuskatsauksessa. Tietoturvatietoisuuteen ei ole kuitenkaan kehitetty yleisesti käytössä olevaa yhtä viitekehystä, vaan kaikissa organisaatiossa tietoturvatietoisuutta on kehitetty yhdistäen ominaisuuksia eri viitekehyksistä ja konsepteista pohjautuen finanssialan sääntelyvaatimuksiin. Myös kahdessa organisaatiossa hyödynnettiin etenkin tietoturvatietoisuuden kehittämisen alkuvaiheessa ulkopuolista konsulttia/kumppania ja heiltä saatuja materiaaleja ja konsepteja.

> (H2) Sen sijaan, että me olisi tunnistettu jotain yksittäistä tai haluttu ottaa käyttöön, niin ei sellaista välttämättä ole, en minä ainakaan voi sanoa, että sellaista olisi ollut.

Organisaatiossa B tietoturvatietoisuuden kehittämiseen lähdettiin vahvasti kulttuurinmuutoksen näkökulmasta ja se sidottiin muutenkin organisaatiossa käynnissä olevaan kulttuurinmuutokseen. Viitekehyksenä hyödynnettiin muutosjohtamisessa käytettyä ADKAR-mallia, jota voidaan käyttää tietoturvakulttuurin kehittämisen apuna (Da Veiga 2018). ADKAR-malli muodostuu viidestä eli vaiheesta, jotka ovat tietoisuus (engl. awareness), halu (engl. desire), tieto (engl. knowledge), kyvykkyys (engl. ability) ja vahvistaminen (engl. reinforcement). Keskeistä mallissa on, että ymmärretään muutoksen tarve ja halutaan sitoutua siihen, jonka jälkeen varmistetaan tarvittavat tiedot ja taidot muutokseen ja lopuksi muutoksen pysyvyys. (Hiatt 2006) ADKAR-malli tukee tutkielmassa esitettyä tietoturvatietoisuuden määritelmää, sillä siinä keskeistä on käyttäytymisen muuttaminen eikä pelkästään tietoisuuden lisääminen (Hiatt 2006).

Tietoturvatietoisuuden kehittämisessä nousi esiin myös ajatus tietoturvatietoisuuden jatkuvasta kehittämisestä, jota tukee PDCA-mallin lähestymistapaa.

> (H3) Mutta sitten niin kuin yleisesti me katsoimme ADKAR-mallin mukaan sitä, että miten tietoisuus pitäisi tulla käytäntöön.
>
> (H2) Tätä nyt on yritetty tehdä tässä jo jonkun aikaa ja se matka jatkuu, koska eihän se tietoturva ole koskaan valmis. Jatkuva kehittämisen malli tämä PDCA-malli tässä on, mitä pitää pyörittää.

5.2 Tietoturvatietoisuuteen vaikuttavat tekijät

5.2.1 Haastatteluiden tulokset

Luvussa 3 käsiteltiin tietoturvatietoisuuteen vaikuttavia tekijöitä Parsonsin ym. (2017) viitekehyksen mukaisesti, jossa tekijät jaettiin yksilöllisiin, organisatorisiin ja välillisiin tekijöihin. Nämä tekijät vaikuttavat työntekijöiden tietoon, asenteisiin ja käyttäytymiseen liittyen organisaation tietoturvakäytäntöihin. Haastatteluissa käsiteltiin erikseen kaikkia tekijöitä ja keskusteltiin siitä, miten eri tekijät ovat vaikuttaneet organisaatioissa tietoturvatietoisuuden kehittämiseen ja minkä välillisten tekijöiden avulla organisaatiot ovat pystyneet tehokkaimmin kehittämään tietoturvatietoisuutta. Taulukossa 5 on esitetty tiivistettynä haastatteluiden tulokset, joita käsitellään tarkemmin alaluvuissa 5.2.2–5.2.4.

Taulukko 5: Haastatteluiden tulokset

Tietoturvatietoisuuteen vaikuttavat tekijät		
Yksilölliset tekijät	Organisatoriset tekijät	Välilliset tekijät
Erilaiset oppijat Psykologiset tekijät o Riskinottohalukkuus o Palveluhalu o Tekninen osaaminen/kiinnostus IT:tä kohtaan Kaikkia yksilöllisiä tekijöitä ei voi huomioida o Roolipohjaisuus	Organisaatiokulttuuri o Laumakäyttäytyminen o Positiivinen tietoturvakulttuuri Johdon rooli o Johdon rooli esimerkkinä o Tietoturva osana organisaation strategiaa/liiketoimintaa o Tiivis yhteistyö o Resurssit Tietoturvaosaston rooli o Palveluorganisaatio o Lähestyttävyys	Viestintä o Monikanavaisuus o Viestin kohdentaminen o Huumori o Viestin jalkauttaminen o Ajankohtaisuus o Kuvamaailma Koulutus o Pelillistäminen (esim. HoxHunt) o Käytännönläheisyys o Roolipohjaisuus Palkitseminen ja rangaistukset o Seuraamusmenettelyt o Positiivinen näkökulma

5.2.2 Yksilölliset tekijät

Haastateltavissa organisaatioissa tietoturvatietoisuuteen vaikuttavia yksilöllisiä tekijöitä tunnistettiin, mutta niitä ei ollut otettu huomioon erityisesti tietoturvatietoisuuden kehittämisessä. Haastatteluissa tunnistettuja psykologisista tekijöistä nousi esiin riskinottohalukkuus, palveluhalu ja tekninen osaaminen. Kuitenkin esimerkiksi riskinottohalukkuus ja palveluhalu nähtiin enemmän finanssialalla hallitseviksi yksilöllisiksi tekijöiksi, eikä niinkään yksilöitä erottaviksi organisaation sisällä. Lisäksi haastatteluissa nousi esille ajatus siitä, että kaikki yksilöt oppivat eri tavalla.

> (H6) Pankkiin hakeutuu selkeästi ihmisiä, jotka ovat ehkä enemmän riskinkarttajia, joilla on työtapana semmoinen varmaan päälle pelaaminen. -- Sitten on toisaalta se korkea palveluhalu, mikä organisaatiossa D on, että halutaan ajatella asiakkaan etua, että on semmoinen palveluhenkinen asenne.

> (H5) Yksilölliset erot minun mielestäni näkyy meillä enemmän niin, että ketkä on kiinnostuneita tekniikasta ja ketkä ei.

Lähes kaikissa organisaatioissa koettiin, että yksilöllisten tekijöiden huomioiminen suurissa organisaatioissa ei ole mahdollista tai kannattavaa. Tärkeää on tiedostaa yksilöllisten tekijöiden olemassaolo, mutta enemmän ajatusmallina, että yksi tapa ei sovi kaikille. Näkemys yksilöllisistä eroista on siis ristiriidassa kirjallisuuden kanssa, jossa yksilöllisiä tekijöitä korostetaan paljon. Kuitenkin ”yksi tapa ei sovi kaikille” -ajattelu tukee kirjallisuuskatsauksessa todettua väitettä, että niin viestinnässä kuin koulutuksessa tulee huomioida ajatus siitä, ettei sama malli sovi kaikille (Kajzer ym. 2014). Yksilöllisten tekijöiden sijaan haastatteluissa korostettiin kuitenkin roolipohjaista ajattelumallia, jossa tunnistetaan eri käyttäjäryhmiä ja tarpeen mukaan koulutusta ja viestintää voidaan kohdentaa heille. Tästä puhutaan tarkemmin alaluvussa 5.2.4.

> (H1) Me ollaan siinä mielessä erilaisia oppijoita, että emme me pysty niissä awareness-ohjelman mukaisissa koulutuksissa, että ei se ole niin, että one size fits all, että sitäkin pitää miettiä.

> (H4) Siellä on ne yksilölliset roolikohtaiset paikat, jotka ovat tärkeitä, missä se impakti on iso. Jos koodari koodaa vähemmän tietoturvavirheitä heti alkupäästä, niin sillä on loppupäässä iso merkitys siihen palvelun laatuun.

5.2.3 Organisatoriset tekijät

Toisin kuin yksilöllisten tekijöiden rooli, organisatoriset tekijät tunnistettiin organisaatioissa ja niiden huomioimista pidettiin äärimmäisen tärkeänä tietoturvatietoisuuden kehittämiselle. Organisatorisista tekijöistä nousi esiin tietoturva- ja organisaatiokulttuuri ja johdon rooli, joiden nähtiin myös toteutuvan melko hyvin kaikissa organisaatioissa, joissa tietoturvatietoisuutta oli kehitetty systemaattisesti useamman vuoden ajan.

Organisaatiokulttuurin puolella haastatteluissa huomasi selvästi, kuinka paljon koko organisaation yleinen organisaatiokulttuuri vaikuttaa myös tietoturvakulttuurin luomiseen, joka ei ollut tullut esiin aiemmassa tutkimuksessa. Esimerkiksi organisaatioissa, jossa on jo valmiiksi hyvin matala hierarkia, on myös tietoturvatietoisuuden kehittäminen huomattavasti helpompaa. Toisaalta taas erilaiset organisaatiomuutokset aiheuttavat haasteita myös tietoturvatietietoisuuden ja koko organisaation tietoturvakulttuurin luomiseen. Lisäksi tietoturvan tuominen osaksi organisaatiokulttuuria vaatii paljon yhteistyötä koko organisaation kesken ja tukea esimerkiksi HR:ltä. Kulttuurissa keskeisenä nähtiin myös muiden työntekijöiden rooli eli organisaation sosiaaliset normit.

> (H6) Kun aikoinaan organisaatiokulttuuri on kehittynyt yhteistoiminnalliseksi ja sitä yhteistyötä edistäväksi niin sitä kautta kaikkiin uusiin merkittäviin asioihin osataan suhtautua oikealla tavalla avoimesti. Tietoturvapuolella erinomainen onnistuminen on se, että organisaatiokulttuuri tukee tietoturvatyötä.

> (H1) -- miten asiaan suhtautuu niin kun lähimmät työkaverit, joiden kanssa päivittäin teet työtä, niin kyllähän se laumakäyttäytyminen on yksi tämmöinen käytännössäkin toteutuva asia.

Haastatteluissa keskusteltiin myös siitä, mitkä ovat avaintekijöitä alaluvussa 3.2. mainitun positiivisen tietoturvakulttuurin (Da Veiga 2018) luomisessa ja tietoturvan tuomisessa osaksi organisaatiokulttuuria. Keskeisenä teemana keskustelussa nousi henkilöstön tietoisuuden kasvattaminen ja tietoturvan tuominen osaksi työntekijöiden arkea käytännönläheisen näkökulman avulla. Toisena teemana oli saavutettavuus eli tieto on helposti saatavilla ja se on ymmärrettävää valituille kohderyhmille. Tiivistettynä voisi kuvailla, että tietoturvakulttuurin luomisessa on tärkeää siirtyä vaatimuskeskeisestä (engl. compliance-based) ajattelusta siihen, että työntekijät ymmärtävät tietoturvan merkityksen

ja heidän oman roolinsa sen toteuttamisessa, mikä onkin alaluvussa 2.1.1 esitetty tietoturvatietoisuuden määritelmä (Kruger & Kearney, 2006; Siponen, 2000).

> (H3) Me on muutettu meidän omaa ajattelutapaamme enemmän siihen, että me ei anneta mitään leimaa paperiin, vaan me kerrotaan, että tähän liittyy tällaisia riskejä, että miten sinä niitä korjaat tai huomioit, että saat sen parannettua ja näin edelleen.

> (H6) Niin kerrotaan, että mitä sillä on merkitystä, että se raportti tehdään ja saadaan semmoinen psykologinen omistajuus sille, että minun tehtävänäni on osallistua tämän organisaation tietoturvan parantamiseen ja auttaa sitä kautta meidän asiakkaitamme.

Keskeisenä osana tietoturvatietoisuuden kehittämistä nähtiin erityisesti johdon rooli, joka nähtiin avaintekijänä etenkin kehityksen alkuvaiheessa vaadittavien resurssien saamiseksi, mutta myös äsken mainitussa tietoturvan tuomisessa osaksi organisaatiokulttuuria. Lisäksi johdon rooli nähtiin tärkeäksi siinä, että tietoturvatietoisuuden kehittäminen pystytään sitouttamaan organisaation strategiaan, eikä se jää ”päälleliimatuksi”. Tämän toteutumiseksi haastatteluissa painotettiin aktiivista vuorovaikutusta johdon kanssa ja johdon sitouttamista tietoturvatietoisuuden kehittämiseen.

> (H1) Toki se voi olla ja pitääkin olla niin kun rahallista panostusta, että näitä asioita voidaan oikeasti viedä eteenpäin ja saa budjettia ja budjetoinnissa näkyvyyttä, mutta toinen on myös, että kuinka ne johtajat nostavat arjessa tietoturvaan liittyviä asioita esiin.

> (H6) Johdon tuki tulee oikeastaan, miten minä nyt sen sanoisin, se on oikeastaan semmoinen tiivis yhteistyö, jatkuva keskustelu.

Johdon lisäksi tietoturva-asiantuntijoiden rooli koettiin tärkeänä tekijänä tietoturvatietoisuutta kehittäessä. Ensinnäkin haastatteluissa nousi kirjallisuudessakin esille tullut asia, että tietoturva-asiantuntijoiden tulisi olla näkyvillä organisaation työntekijöille. Lisäksi monesti haastatteluissa nousi esille näkökulma siitä, että tietoturvatiimi on ”palveluorganisaatio”, jonka tehtävänä on auttaa liiketoimintaa. Etenkin ajatus matalasta tietoturvaosastosta ja vuorovaikutuksen merkityksestä tukee Albrechtsenin (2007) näkökulmaa tietoturvajohtajien roolista organisaatioissa tietoturvatietoisuuden kehittämiseksi.

> (H2) Siellä niin kun porukat totesivat, että on ihanaa, että joku tulee puhumaan näistä tietoturvallisuuden asioista ja tulette pois sieltä norsunluutornista, että se on valtava muutos aikaisempaan.

> (H1) Minun mielestäni on ihan äärimmäisen tärkeää, että koko henkilöstö tietää ihan nimeltä ja kasvoilta, että keitä me olemme ja meihin halutaan olla yhteydessä matalalla kynnyksellä.
>
> (H3) Me olemme tämmöinen palveluorganisaatio ja me teemme ohjeita muille eikä itsellemme.

Mahdollistaakseen tietoturvaosaston näkyvyyden ja lähestyttävyyden, oli organisaatioissa esimerkiksi pyritty viestimään mahdollisimman paljon henkilökohtaisesti sekä jalkautumaan työntekijöiden joukkoon. Esimerkiksi organisaatiossa A tietoturva-asiantuntijat aloittivat kiertämään organisaation eri toimipisteitä ympäri Suomea. Tässäkin on tärkeä huomioida erot organisaatioiden koossa ja organisaatiorakenteessa. Pienemmissä organisaatioissa työntekijöiden lähestyminen on huomattavasti helpompaa. Suurissa organisaatiossa itse tietoturvajohto voi jäädä helposti etäiseksi työntekijöistä, mutta haastatteluissa tuli esille, että tietoturvaa voidaan pyrkiä jalkauttamaan esimerkiksi turvallisuusvastaavien tai security champion -roolien avulla. Security Champion -roolilla tarkoitetaan henkilöä, joka auttavat tietoturvaosastoa tietoturvatietoisuuden parantamisessa ja auttavat esimerkiksi ohjelmistokehittäjiä tietoturvallisessa ohjelmistokehityksessä (OWASP 2022). Security Champion -ajattelumallia oli laajennettu myös muihin liiketoimintoihin keräämällä yhteen tietoturvasta kiinnostuneita työntekijöitä, jotka auttoivat organisaatioiden tietoturva-asiantuntijoita tietoturvakulttuurin luomisessa.

> (H2) Mulla tuli itsellä sellainen asia mieleen, että meidän pitää osallistaa sitä porukkaa voimallisesti ja minä ehdotin sellaista mallia, että aloitetaan tämmöinen roadshow. Lähdetään käymään jokaisella paikkakunnalla, että ne porukat kentällä näkevät, että ketkä tätä työtä tekevät.
>
> (H3) Ne, joita kiinnostaa enemmän se kyberturvallisuus niin voivat liittyvä siihen ja tulla kuuntelemaan ja viedä eteenpäin viestiä, että mitä on tulossa ja menossa tai että, mitä kannattaisi huomioida.

Teoriassa esille tullutta tietoturvan digitaalista kahtiajakoa (Albrechtsen & Hovden 2009) ei tullut esille haastatteluissa lainkaan. Tietoturva-asiantuntijoiden näkemys oli oikeastaan täysin päinvastainen kaikissa organisaatioissa. Sen sijaan, että työntekijät nähtäisiin tietoturvauhkana, kaikissa haastatteluissa korostettiin sitä, että työntekijät nähdään tietoturvan vahvimpana lenkkinä tai vahvimpana puolustajana. Yhdessä haastatteluista kiteytettiin hyvin kaikkia organisaatioita yhdistävä näkemys:

> (H5) Ihminen on heikoin lenkki, mutta se johtuu siitä, että ihmistä ei ole opastettu oikein, oikeisiin asioihin tai siihen mikä on tärkeää.

Albrechtsenin ja Hovdenin (2009) näkemystä voidaan pitää siis tämän tutkimuksen valossa vanhanaikaisena. Vaikka ihminen saattaa tehdä helposti virheitä, niin kaikissa organisaatiossa lähdettiin ajatuksesta, että tietoturvaa rakennetaan yhdessä ilman syyllistämistä tai osoittelua.

5.2.4 Välilliset tekijät

Tässä tutkielmassa välillisillä tekijöillä tarkoitetaan menetelmiä, jonka avulla organisaatio pyrkii parantamaan työntekijöidensä tietoturvatietoisuutta. Kirjallisuuskatsauksessa välilliset tekijät jaettiin viestintään, koulutukseen ja harjoituksiin sekä palkitsemiseen ja rangaistuksiin. Yleisesti haastatteluissa välillisistä tekijöistä tietoturvatietoisuuden kehittämiseen nousivat esille hyvin samat teemat kuin alaluvussa 5.2.3 koskien positiivisen tietoturvakulttuurin luomista. Kaikissa organisaatioissa pidettiin tärkeänä, että viestinnän ja koulutusten sekä harjoitusten tulisi olla mahdollisimman lähellä työntekijöiden arkipäiväistä työskentelyä ja mahdollisimman kansankielisiä. Lisäksi tärkeässä roolissa pidettiin alaluvussa 5.2.2 mainittua roolipohjaisuutta sekä huumorillista ja positiivista lähestymistapaa.

> (H2) Ja niin, että ei näytetä sitä tietoturvaa pelottavana. Jos tietoturva näkyy ihmiselle pelottavana eli koulutuksessa keskitytään pelkästään niihin uhkiin, mutta ei siihen, miten ihmiset voi omalla toiminnallaan vaikuttaa, niin sittenhän ihmisiä alkaa ahdistamaan, kun ne ajattelevat tietoturvallisuutta.

Haastatteluissa tuotiin esille, kuinka tietoturvatietoisuuden parantamista välillisten tekijöiden avulla voidaan ajatella ADKAR-mallin avulla. ADKAR-mallissa hyvänä pidettiin etenkin sitä, että sen avulla huomio kiinnittyy työntekijän näkökulmaan. Keskeisenä vaiheena ADKAR-mallissa korostettiin halua, joka keskittyy siihen, miten työntekijä saadaan kiinnostumaan aiheesta ja mitä hyötyä hänelle on tietoturvapolitiikan noudattamisesta. Tämän jälkeen varmistetaan tieto tarjoamalla esimerkiksi koulutusta tai viestintää aiheeseen liittyen ja varmistetaan, että yksilöllä on kyvykkyys muuttaa käyttäytymistä eli hän esimerkiksi pääsee tarvittaviin järjestelmiin. Viimeisessä vahvistamisen vaiheessa luodaan alaluvussa 5.2.3. mainittua tietoturvakulttuuria. Haastattelussa haastateltava kuvaili ADKAR-mallin hyödyntämisestä pidempien salalausekkeiden esimerkin avulla.

> (H4) Awareness-kontekstissa kerrotaan kauheasti ihmisille, mutta sitten se, että saadaan jotain irti, niin millä se desire herätetään, että millä ne saadaan vanhasta tottumuksesta pois. Mietitään niitä keinoja. Kerrotaan niille, että

> teette näin, niin voidaan harventaa salasanan vaihtamisen väliä. Teette näin, niin salasana on helpompi muistaa. No ability on sitten käytännössä kyvykkyys sen tekemiseen eli käytetään niitä työkaluja, millä se salasana vaihdetaan. Sitten on se osaaminen tai kyky tehdä se muutos. Viimeinen on se reinforcement eli sitten haetaan se jakelu tai joku kohderyhmälle oikea auktoriteetti vahvistamaan, että tämä on oikeasti hyvä juttu.

Yksi keskeinen nosto haastatteluissa oli, että kun pyritään herättämään työntekijöiden halu noudattaa tietoturvakäytäntöjä ja kehittää tietoturvatietoisuutta tätä kautta, voidaan viestintää ajatella markkinoinnin perusperiaatteiden mukaan. Markkinoinnissa keskeistä on luoda arvoa asiakkaalle (Armstrong 2014) ja myös tietoturvatietoisuuden viestinnässä keskeistä on kysymys, mitä hyötyä tietoturvakäytäntöjen noudattamisesta on työntekijälle. Tätä tukee myös Siposen (2000) ajatus siitä, että tietoturvatietoisuudessa keskeistä on viestinnän avulla tehdä tietoturvasta ”in topic” ja herättää työntekijöiden mielenkiinto tietoturvaa kohtaa.

> (H4) -- Markkinoinnin perusperiaatteet: Mitä myyt? – Herätä mielenkiinto asiaan, pura vaikea asia niin yksinkertaiseksi, kun se on kulloisessakin tilanteessa tarpeen tai järkevää --.

Tässä keskeisessä roolissa haastatteluissa tuli esille huumori, viestin kohdentaminen, ajankohtaisuus ja viestin ymmärrettävyys. Yhtenä tekijänä nousi esiin myös viestinnän monikanavaisuus ja organisaatioille tehokkaimpien viestintäkanavien ja -tapojen löytäminen. Organisaatiolle tehokkaiden viestintäkanavien löytämiseksi organisaatiossa B oli tehty mediakanava-analyysi siitä, mitä kaikkia tapoja organisaatiossa on tavoittaa henkilöstö. Näin organisaatiolle tehokkaat viestintäkanavat ja -keinot oli helpompi löytää. Myös organisaatioiden kulttuurierot tulivat haastatteluissa esiin: Esimerkiksi organisaatiossa A huumorilliset tietoturvavideot herättivät paljon positiivista palautetta, kun taas organisaatiossa B ei ole samanlaista videoiden katselukulttuuria, joten videoita ei koettu tehokkaaksi viestintämenetelmäksi.

> (H6) Oikeastaan ajankohtaisuuden kautta, jos on esim. lehdissä ollut asiaa jostain niin me yritämme tehdä siitä nopeasti intraan semmoinen normaalin ihmisen ymmärrettävissä olevassa muodossa oleva tarina.

> (H2) – jos haluaa vaikuttavuutta aikaiseksi, niin pitää tunnistaa, että mikä kommunikaatiotapa on kulloisellekin porukalle, että kyllähän me on vaihdettu sitä viestintää ihan laidasta laitaan ihan sen kuulijajoukon mukaisesti.

> (H1) Ja sitten ehkä tärkein työkalu on, ja se ei oikeastaan ole tekninen millään tavalla, vaan se on se tyyli ja tapa, millä me viestimme. Pyritään

> hyödyntämään siellä missä on mahdollista aina huumoria viestin läpiviemiseksi.

Organisaatiossa A ja B viestinnässä hyödyttiin myös paljon kuvallista viestintää ja tietoturvallisuusviestinnän alibrändäystä, jossa tietoturvalle oli luotu organisaatioon oma visuaalinen ilme, jonka puitteissa tietoturvaan liittyvistä aiheista viestittiin. Haastateltavat kokivat, että kuvien avulla voitiin tehdä tietoturvaan liittyvästä viestinnästä mahdollisimman ymmärrettävää ja saadaan herätettyä paremmin työntekijöiden mielenkiinto. Tulosten perusteella voitaisiin siis todeta, että on tärkeää huomioida toimivaksi osoitetut ominaisuudet, mutta mukauttaa viestintäkanavat ja -menetelmät sopivaksi omaan organisaatiokulttuuriin. Haastatteluiden tulokset tukevat aiempaa tutkimusta, jossa samat asiat nousivat esille puhuttaessa tehokkaasta viestinnästä tietoturvatietoisuuden kehittämiseksi. Hyvänä tapana pidettiin myös läheistä yhteistyötä organisaation viestinnän ja ulkoisen kumppanin kanssa etenkin, jos omassa tiimissä ei löydy osaamista toivottujen ideoiden luomiseen.

> (H3) Meillä on oma kuvamaailma, mitä me hyödynnetään kyberturvallisuusviestinnässä, jonka hahmot ja piirrosjälki on tehty ihan ulkoisen yhteistyökumppanin kanssa.

> (H1) Me otettiin hyvin aikaisessa vaiheessa mukaan ulkopuolinen kumppani, joka on aiemminkin tehnyt tämän kaltaisia juttuja, ---, niin hänellä oli niin kuin viestintä ja markkinointi taustalla.

Kaikissa organisaatioissa tietoturvaan liittyvät harjoitukset ja koulutukset nähtiin keskeisenä osana tietoturvatietoisuuden parantamista. Koulutuksessa pyrittiin hyödyntämään mahdollisimman paljon käytännön esimerkkejä ja havainnollistamista sekä sitomaan koulutus työntekijöiden omaan toimintaan. Roolikohtaisen koulutuksen merkitys tunnistettiin kaikissa organisaatioissa, mutta sen toteuttaminen koettiin etenkin suuremmissa organisaatioissa haastavaksi. Organisaatioissa oli kuitenkin tunnistettu alaluvussa 5.2.2 sitaatissa mainitut roolit, joissa merkitys tietoturvallisuuden toteutumiselle on iso ja esimerkiksi kehittäjille oli lähes kaikissa organisaatioissa suunnattu roolipohjaista koulutusta. Roolipohjaisen koulutuksen mahdollistamista pidettiin kuitenkin myös haastavana suurissa organisaatioissa, sillä rooleja ja niihin liittyvät eri tietoturvavaatimuksia on paljon.

> (H3) Kyllä minä näen koko ajan vahvemmin sen, että sinne henkilöstöä lähelle niitä asioita pitää saada, että ne menevät mitenkään läpi.

> (H6) No kaikenlainen havainnollistaminen ja sitten se, että yhdistellään niitä asioita ja kerrotaan esimerkkien avulla.
>
> (H5) – Jatkossa olisi tarkoituksena, että tietoturvatietoisuuden vaatimuksetkin yhdistettäisiin työtehtäviin eli rooleihin. – Esimerkiksi vaikka just kehittäjille saattaa olla vaatimuksena, että ne käyvät turvallisen ohjelmoinnin koulutuksen, kun taas sitten peruspankkilaisille ei. Eli jatkossa se mietitään työtehtävien mukaan.

Hyvin keskeisenä tietoturvaan liittyvissä koulutuksissa ja harjoituksissa nähtiin osallistaminen ja vuorovaikutus, minkä vuoksi pelillistämisen mahdollistavat harjoitukset nostettiin usein esiin parhaina menetelminä. Kahdessa organisaatiossa käytössä olevaa HoxHuntia pidettiin yksimielisesti parhaana työntekijöiden tietoturvatietoisuuden kehittämiseen. HoxHunt on sähköpostiin integroitava pelillistetty koulutus, jonka tarkoituksena on opettaa työntekijöitä tunnistamaan kalasteluviestejä leikkimielisessä kilpailussa ja tukea oikeiden kalasteluviestien raportointia (HoxHunt 2022b).

Edellisen lisäksi esille nousivat muut käytännönläheiset ja osallistamisen mahdollistavat harjoitukset. Sääntelyn pakottamat verkkokoulutukset nähtiin puolestaan enemmän pakollisena pahana ja enemmän osana vaatimuslähtöistä ajattelutapaa, josta kaikissa organisaatioissa pyrittiin pois. Organisaatiossa A ja B verkkokoulutuksia oli myös tämän takia pyritty kehittämään enemmän organisaation näköisiksi ja mielenkiintoisemmiksi esimerkiksi videoiden ja kuvien avulla.

> (H1) Meillä on verkkokoulutuksia, jotka ovat vähän sellainen pakollinen paha. En oikein itse ole vakuuttunut siitä, että sitä kautta loppu viimein viesti menee perille, koska niitä verkkokoulutuksia on aika paljon.
>
> (H3) HoxHuntista me on saatu tosi hyvää palautetta, että siis kun sitä kautta me pystymme oikeasti näyttämään se käyttäytymisen muutos. Kun kouluttaudut aktiivisesti, niin raportoit myös todennäköisemmin epäilyttävät viestit ja onnistut merkittävästi paremmin myös noissa harjoituksissa.
>
> (H2) Oppimisen näkökulmasta tommoiset hands on -tekemiset, niin ne on niin kun monesti ollut tällaisia harjoituksia tai JyvSecTecin kanssa tehtäviä ASRIT-harjoituksia niin ne on ollut kaikki sellaisia, että porukat tykkäävät niistä ja just sen takia, että se on jollain tavalla pelillistettyä.

Yhtenä hyvänä ominaisuutena pelillistämisessä nähtiin palkitseminen, jota hyödynnettiin osana tietoturvatietoisuuden parantamista kahdessa organisaatiossa. Puhuttaessa palkitsemisesta ja rankaisemisesta, tuli monesti esille alaluvussa 5.2.3 esille tuotu positiivinen tietoturvakulttuuri, jossa tietoturvatietoisuutta kehitetään aina positiivinen kulma edellä. Rankaisemiseen suhtauduttiin organisaatioissa hyvin varauksella ja

mahdollisia seuraamusmenettelyjä pidettiin viimeisenä keinona. Missään organisaatiossa ei haluttu korostaa seuraamuksia eli negatiivista vahvistamista, vaan ajatuksena oli enemmänkin kannustaa työntekijöitä positiivisen kautta ja välttää luomasta tietoturvasta liian pelottavaa kuvaa korostamalla uhkakuvia.

> (H2) Tämä toinen puoli on äärimmäisen tärkeä eli tämä palkitseminen.

> (H4) Suhtaudun todella varauksella siihen, että rankaisulla saadaan mitään hyvää aikaan. Silloin kun mennään siihen tilanteeseen, että ihmiselle sanotaan, että mokasit tässä kohtaa niin sillä on defenssit heti ylhäällä, mikä estää oppimisen.

Haastatteluissa tuli myös ilmi, että kehittäessä menetelmiä tietoturvatietoisuuden parantamiseen, on hyvä myös huomioida, että aina ei kannata kehittää uutta. Haastatteluissa tuli usein esille, että tietoturvaa kannattaa sitouttaa organisaation muihin toimenpiteisiin, kuten HR:n valmiiksi järjestämiin koulutuksiin tai muihin tilaisuuksiin. Tällainen lähestymistapa tukee ajatusta, että tietoturva on nimenomaan palveluyksikkö, jonka tehtävänä on helpottaa liiketoimintaa. Lisäksi tietoturva on helpompi sitouttaa organisaatiokulttuuriin, mikäli sitä ei nähdä erillisenä yksikkönä, vaan osana organisaation liiketoimintaa ja strategiaa.

> (H2) Sitten oli myös näitä tapahtumia, nyt vaikka täällä HQ:ssa, että jollain porukalla oli joku tilaisuus esim. kehityspäivät, niin me aina huikkasimme sinne, että päästäänkö puhumaan heidän kanssaan tietoturvallisuudesta ja nimenomaan heille suunnatusti siitä asiasta.

5.3 Tietoturvatietoisuuden arviointi ja mittaaminen

Mittaamiseen hyödynnettävät menetelmät olivat kaikissa organisaatiossa melko samanlaiset. Esiin nousivat henkilöstölle sekä sidosryhmille lähetettävät säännölliset kyselytutkimukset, ulkoiset työkalut, kuten ISF:n Health Check ja Kyberturvallisuuskeskuksen kybermittari, koulutusten osallistumisprosentit, tietoturvatapahtumien raportoinnin seuranta sekä keskustelut/lyhyet kyselyt esimerkiksi koulutustilaisuuksien yhteydessä. Lisäksi HoxHuntia pidettiin yhtenä tapana mitata ja seurata tietoturvatietoisuuden kehittymistä organisaatiossa. Kyselytutkimuksissa pyrittiin myös mukauttamaan seuraamaan ihmisten käyttäytymistä, kuten organisaatiossa B oli pyritty tekemään USB tikku -esimerkin avulla.

> (H4) Sitten on tehty kyselytutkimus niin, että siinä oli se käyttäytymispuolen analyysi. Me kysymme kysymyksen: Löydät aulasta kulhollisen USB-

> tikkuja, otatko USB-tikun ja laitatko sen koneeseesi? Eihän se kerro mitään, vaan sitten kysytään, että mitä luulet, että kollegasi tekee?
>
> (H1) Mittaaminen on hyvin paljon tämmöistä kyselyihin sekä tutkimukseen perustuvaa ja jonkin verran saadaan kaivettua mittareita myös järjestelmistä.

Monissa organisaatioissa painotettiin, että mittaaminen on tärkeä keino seurata tietoturvatietoisuuden kehittämistä ja raportoida siitä johdolle, mutta yhdessäkään organisaatiossa ei oltu ennen tietoturvatietoisuuden systemaattista kehittämistä tehty varsinaista lähtötason dokumentoitua mittausta, vaan se perustui enemmän työolettamaan tai hajanaisiin mittauksiin ja keskusteluihin. Tämä tietenkin oli tehnyt vaikeammaksi mittareiden kehittymisen arvioinnin. Kuitenkin etenkin organisaatioissa, jossa tietoturvatietoisuuden systemaattista kehittämistä oli tehty jo useampi vuosi, oli mittareiden huomattu kehittyvän positiiviseen suuntaan. Monissa haastatteluissa korostui etenkin se, että positiivinen kehitys on näkynyt kasvavana kiinnostuksena tietoturvaan liittyviä asioita kohtaa, aktiivisena osallistumisena tieturvan kehittämiseen sekä positiivisena palautteena.

> (H1) Joo niin kuin sanoin niin ei ihan nollatasoa mitattu, mutta sitten kun oli awareness-ohjelmaa pyöritetty noin vuosi, niin mitattiin ensimmäisen kerran ja silloin ne henkilöstökyselyn arvosanat ja sieltä tullut avoin palaute oli tosi hyvää. Ja sitten kun tehtiin toinen mittaus tässä niin mikään osa-alue ei ollut muistaakseni tullut alaspäin ja joissakin oli jonkun verran nousua.
>
> (H5) Nyt kun koulutuksia on alettu tekemään, niin ihmiset on ollut tosi aktiivisia antamaan palautetta ja koetaan, että tietoturva kiinnostaa.

Niin kuin alaluvussa 2.2.3 mainittiin, on tietoturvatietoisuuden mittaamiseen liittyvä tutkimus vielä melko vähäistä ja osa-alue koettiin myös haasteeksi haastateltavissa organisaatioissa. Haasteet liittyivät nimenomaan käyttäytymisen muutoksen mittaamiseen sekä tiettyjen menetelmien tehokkuuden arvioimiseen. Vaikka monissa organisaatioissa oli huomattu positiivinen muutos esimerkiksi tietoturvatapahtumien raportoinnissa tai haavoittuvuuksien havainnoinnissa niin koettiin vaikeaksi tunnistaa, millä konkreettisilla keinoilla tietoturvatietoisuuteen oli parhaiten pystytty vaikuttamaan.

> (H3) Jos haavoittuvuuksien määrä vähenee, niin sehän korreloi siihen, että toimet on tehonnut. Mutta mitkä toimet tehoavat ja mitkä ei tai mikä oli parempi kuin toinen. Mistäs tiedät, et mistään.
>
> (H4) Käyttäytymisen tai viestin substanssin ymmärtämisen mittaaminen on todella vaikeaa.

Haasteet käyttäytymisen mittaamisessa sitoutuu myös alaluvussa 2.2.2 mainittuun kuiluun tiedon ja käyttäytymisen välillä (Cox 2012), joka tunnistettiin suurimmassa osassa organisaatioissa ja jonka korjaaminen koettiin haasteelliseksi. Monissa haastatteluissa todettiin, että käyttäytymisen muuttaminen on pitkäjänteinen prosessi ja siihen täytyy myös suhtautua niin. Kuilua oli pyritty korjaamaan esimerkiksi reagoimalla yksilön toimintaan sekä teroittamalla toiminnan syitä. Kuilu näkyy tietoturvatietoisuuden mittaamisessa esimerkiksi siten, että vastaako yksilö kyselyyn niin kuin hän toimii vai niin kun hän kuvittelee, että hänen halutaan vastaavan.

> (H2) Kun tulee joku tarpeeksi voimakas insentiivi, että lähdetään kahville -tyyppinen tilanne, niin se on ihan inhimillistä toimintaa, että se näyttö jää auki. Ja sitähän se on, että me vaan koko ajan teemme töitä sen eteen, että se paha tapa saadaan kitkettyä pois ja hyvät tavat ajettua sisään.

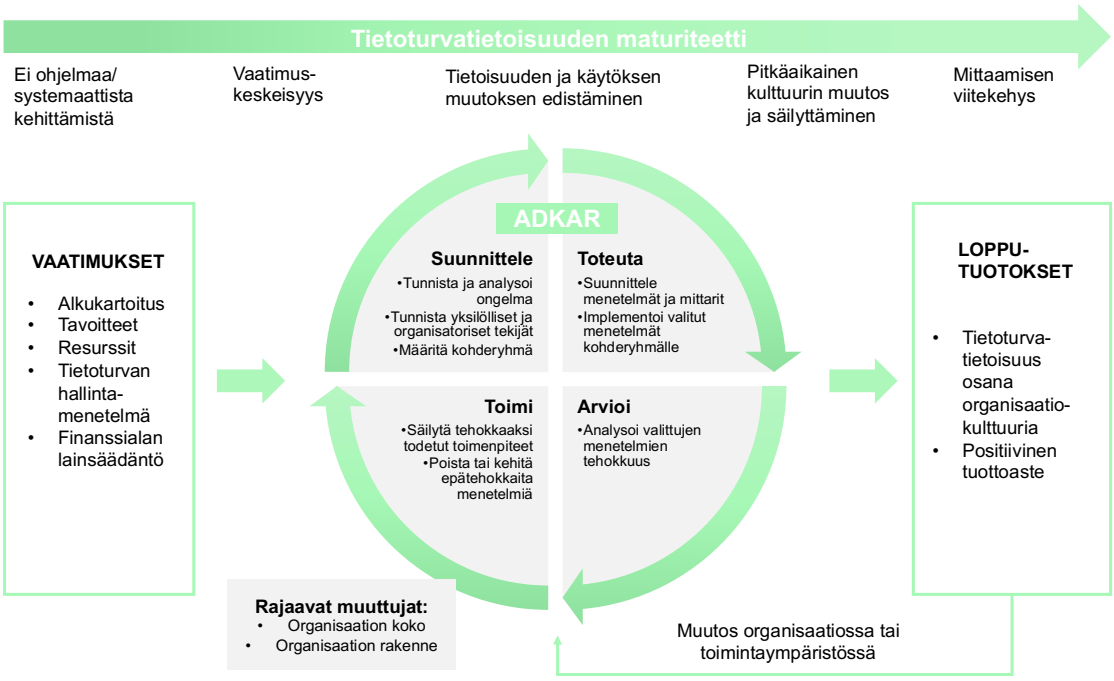
Yhtenä haasteena pidettiin myös sitä, miten mielenkiintoa voidaan pitää yllä pitkällä aika välillä. Tähän kuitenkin nähtiin auttavan jatkuvan kehittämisen malli, joka tuli usein esiin niin kirjallisuudessa kuin haastatteluissa. Arvioimalla hyödynnettyjen menetelmien tehokkuutta, ylläpitämällä laadukkaita ja hyväksi todettuja materiaaleja ja toimenpiteitä sekä kehittämällä uusia, voidaan organisaatiossa vastata haasteeseen säilyttää tietoturvatietoisuuden mittareiden positiivinen kehitys.

> (H1) Haasteena on se, että miten me pidämme sen mielenkiinnon yllä ilman, että se saturaatiopiste tulee ja meihin kyllästytään. Tähän asti on vielä johtoa ja henkilöstöä myöten ollut selkeästi tilausta niin täytyy pitää huoli, että se meidän tuottama sisältö resonoi sen kohderyhmän kanssa.

6 Tietoturvatietoisuuden systemaattisen kehittämisen viitekehys

6.1 Viitekehyksen muodostaminen

Tässä alaluvussa käsitellään kuviossa 5 esiintyvää viitekehystä tietoturvatietoisuuden systemaattiseen kehittämiseen. Mallin tarkoituksena on auttaa organisaatioita kehittämään tietoturvatietoisuutta systemaattisesti valiten tehokkaimmat menetelmät ja kehittäen niitä niin kauan, että lopulta organisaatioissa voidaan osoittaa lopputuotoksena eri menetelmien vaikutus ja liiketoiminnan saama hyöty.



Kuvio 4: Tietoturvatietoisuuden systemaattisen kehittämisen viitekehys

Kuvion 5 viitekehys on kehitetty perustuen alaluvussa 2.2.2 esitettyyn PDCA-malliin, joka kuvaa jatkuvaa kehittämistä. PDCA-mallin lisäksi viitekehyksessä hyödynnetään haastattelussa esille tullutta ADKAR-mallia, joka kuvaa organisatorista muutosta. Mallissa tietoturvatietoisuuden kehitystä mitataan luvussa 2.2.3 esitellyn SANS:in maturiteettimallin avulla. Jotta viitekehys voisi vastata käytännön tarpeeseen finanssialan organisaatioille, on keskeisenä tekijänä sen muodostamisessa huomioitu tutkimuksen tuloksissa esiintyneet keskeisimmät mallit tietoturvatietoisuuden kehittämiseen ja mittaamiseen sekä tietoturvatietoisuuteen vaikuttavat tekijät finanssialalla. Niin kuin luvussa 2.2.3 mainittiin, PDCA-malli sopii hyvin tietoturvatietoisuuden kontekstiin,

koska sitä hyödynnetään myös ISO/IEC 27001-standardisarjassa, jota hyödynnetään monissa finanssialan organisaatioissa.

Viitekehys muodostuu kolmesta eri vaiheesta, jotka ovat vaatimukset, kehittäminen ja lopputuotokset. Lisäksi mallissa on huomioitu rajaavat muuttujat (engl. control variables) eli organisaation koko ja organisaatiorakenne, joiden vaikutus tietoturvatietoisuuden kehittämiseen tuli esille kaikissa haastatteluissa. Nämä muuttujat vaikuttavat olennaisesti siihen, minkälaisia menetelmiä kannattaa hyödyntää ja mitkä menetelmät ovat tehokkaita kussakin organisaatiossa. Esimerkiksi osuuskuntamallisessa tai suuremmassa organisaatiossa voi olla viisaampaa jalkauttaa tietoturvaa ”sanansaattajien” kautta, kun taas konsernissa tai pienemmässä organisaatiossa tietoturvayksikkö pystyy itse olemaan enemmän läsnä työntekijöiden arjessa. Tässä tutkielmassa toimialaa ei ole merkitty rajaavaksi muuttujaksi, koska tutkimus on rajattu finanssialan organisaatioihin. Mikäli kuitenkin viitekehystä hyödynnettäisiin toisella toimialalla, voitaisiin myös toimiala lukea rajaaviin muuttujiin.

Viitekehyksessä tietoturvatietoisuuden tasoa mitataan SANS:in maturiteettimallin avulla. Malli ja sen eri vaiheet on esitelty tarkemmin luvussa 2.2.3. Maturiteettimallia voidaan hyödyntää tietoturvatietoisuusohjelman kehittämisessä arvioiden sen nykytilaa ja tulevaisuuden kehityskohteita (SANS 2022). Tässä viitekehyksessä maturiteettimallia sovelletaan mittaamaan tietoturvatietoisuuden eri osa-alueiden tai tietoturvatietoisuuteen liittyvien kehityskohteiden kehittämistä eikä pelkästään tietoturvatietoisuusohjelmaa kokonaisuutena.

Eri osa-alueita voivat olla esimerkiksi tiedonhallinta, tietoturvatapahtumien raportointi, salasanojen hallinta, sähköpostin käyttö, internetin ja sosiaalisen median käyttö sekä liikkuva tietojenkäsittely (Parsons ym. 2014). Eri osa-alueet riippuvat organisaation omista tarpeista ja tietoturvatietoisuuteen liittyvistä puutteista. Lisäksi niihin vaikuttaa jatkuvasti muuttuva ympäristö ja sen aiheuttamat uudet tietoturvauhat. Esimerkiksi tällä hetkellä uhat liittyvät kasvavaan hybridityöhön, kiristyshaittaohjelmien lisääntymiseen, tekoälyyn ja tietojenkalasteluun (SoSafe 2022), jotka näkyvät myös finassialan toimijoille. Alaluvuissa 6.2–6.5 käsitellään tarkemmin viitekehyksen eri vaiheita ja esitetään esimerkki viitekehyksen hyödyntämisestä.

6.2 Vaatimukset

Tietoturvatietoisuuden kehittämisen alkuvaiheessa puhutaan maturiteettimallin ensimmäisestä ja toisesta tasosta, joissa tietoturvatietoisuutta ei kehitetä organisaatiossa systemaattisesti tai kehittäminen pyrkii täyttämään tietyt lainmukaiset vaatimukset (SANS 2022). Ennen varsinaista PDCA-mallin mukaista kehittämistä on olemassa tiettyjä vaatimuksia, jotta tietoturvatietoisuutta voidaan kehittää mahdollisimman tehokkaasti ja lopulta toimenpiteiden voidaan osoittaa tuottavan arvoa organisaatiolle. Nämä vaatimukset on määritelty perustuen aiempaan kirjallisuuteen ja haastatteluiden tuloksiin.

Ensimmäiseksi organisaatiossa tulisi tehdä alkukartoitus eli mitata tietoturvatietoisuuden lähtötaso. Ilman lähtötason mittausta on eri toimenpiteillä saatava hyöty mahdotonta osoittaa. Mittarit voidaan valita sopivaksi organisaatiolle, mutta keskeistä on, että niitä toistetaan systemaattisesti kehittämisen aikana. (ENISA 2010) Mittaamisen lisäksi alkukartoituksessa pystytään selvittämään, millä osa-alueilla tietoturvaa tulisi pääasiassa kehittää. Tätä voidaan esimerkiksi hyödyntää, kun mietitään seuraavan vaiheen kehittämisen tärkeysjärjestystä.

Mittaamisen lisäksi toinen asia ennen varsinaista kehitysprosessia on tavoitteiden tai vaatimusten asettelu riippuen organisaatiossa hyödynnettävästä tietoturvan hallintamenetelmästä. Mikäli organisaatiossa hyödynnetään esimerkiksi ISO/IEC 27000 -standardisarjaa, on tärkeää, että tietoturvatietoisuuden kehittäminen on linjassa kyseisen standardin mukaisiin vaatimuksiin. Mikäli organisaatiossa ei ole selkeää tietoturvan hallintamenetelmää, on sellainen hyvä määrittää ennen tietoturvatietoisuuden kehittämistä. Tietoturvanhallintamenetelmän avulla tietoturvan ja täten myös tietoturvatietoisuuden kehittäminen voidaan sitoa organisaation muuhun johtamisjärjestelmään ja täten organisaation liiketoimintaan (Ashenden 2008).

Haastatteluissa tuli esille, kuinka pitkäjänteinen prosessi tietoturvatietoisuuden kehittäminen on. Systemaattiselle kehittämiselle tärkeää on johdon tuki (Ashenden, 2008), joka voidaan haastatteluiden mukaan saavuttaa osoittamalla johdolle selkeä viesti siitä, mitä tietoturvatietoisuuden kehittämisellä voidaan saavuttaa ja miten/mihin pyydetyt resurssit käytetään. Lisäksi on tärkeää ottaa huomioon lainsäädännölliset vaatimukset, jotka koskevat finanssialalla tietoturvaa ja tietoturvatietoisuutta (Tsohou ym. 2015). Kun tietoturvatietoisuuden kehittäminen on aloitettu ja tietyt

perusvaatimukset täytetty, voidaan siirtyä miettimään enemmän osa-alueittain tietoturvatietoisuuden kehittämistä eri menetelmien avulla.

6.3 Kehittäminen

Toinen vaihe viitekehyksessä on itse kehittäminen PDCA-mallin mukaisesti. Tämä vaihe vastaa maturiteettimallin mukaista kolmatta ja neljättä tasoa, jotka ovat ”tietoisuuden ja käytöksen muutoksen edistäminen” ja ”pitkäaikainen kulttuurin muutos ja säilyttäminen”. Kehittämisvaihetta voidaan ajatella tietoturvatietoisuuden eri osa-alueiden mukaan eikä niinkään koko tietoturvatietoisuusohjelman mukaan. Esimerkiksi jos organisaatiossa halutaan kehittää kalasteluviestien tunnistamista, kehitetään PDCA-mallin mukaan tätä osa-aluetta eri menetelmien avulla. Tätä havainnollistetaan paremmin luvussa 6.5 esitetyn esimerkin avulla.

PDCA-mallin ensimmäinen vaihde on suunnittelu. Kun kehittämistä lähdetään suunnittelemaan, on ensin keskeistä tunnistaa ja analysoida mahdollinen puute tai ongelma organisaatiossa. Sen jälkeen tunnistetaan organisatoriset ja yksilölliset tekijät ja kohderyhmä tai kohderyhmät. Luvussa 3 tunnistettiin yksilöllisiä, organisatorisia ja välillisiä tekijöitä, jotka vaikuttavat tietoturvatietoisuuden kehittämiseen. Haastatteluissa näistä tekijöistä nousi erityisesti esille yksilöllisistä tekijöistä roolipohjainen ajattelu ja organisatorisista tekijöistä johdon ja tietoturva-asiantuntijoiden rooli sekä organisaatiokulttuuri.

Välillisillä tekijöillä tarkoitetaan työntekijöiden tietoturvatietoisuuden parantamiseen hyödynnettäviä menetelmiä, joista haastatteluissa nousi esiin aiempaa tutkimusta mukaillen erityisesti viestintä sekä harjoitukset ja koulutus. Molemmissa esille nousivat samat ominaisuudet eli käytännönläheisyys, kansankielisyys, roolipohjaisuus/kohdentaminen, huumorillinen ja positiivinen lähestymistapa. Lisäksi pelillistäminen koettiin tehokkaaksi, kun taas viestinnässä tärkeänä pidettiin monikanavaisuutta. Positiivista lähestymistapaa tukeva palkitseminen nähtiin tärkeäksi menetelmäksi, mutta rankaisemiseen suhtauduttiin hyvin varauksella.

Suunnitteluvaiheessa sekä PDCA-mallin toisessa vaiheessa eli toteuttamisvaiheessa voidaan hyödyntää ADKAR-mallia toivotun muutoksen saavuttamiseksi. Toteuttamisvaiheessa suunnitellaan ja implementoidaan menetelmät valitulle kohderyhmälle. Lisäksi valitaan mittarit, joiden avulla kehitystä voidaan seurata tiettyjen

toimenpiteiden tai ongelmien kohdalla. Keskeistä ADKAR-mallin hyödyntämisessä on käydä läpi kaikki kohdat, jotta pystytään varmistamaan, että työntekijöillä on tieto, motivaatio ja kyvykkyys muuttaa toimintaansa. Yleensä mikään menetelmä ei ole yksittäin riittävä keino halutun lopputuloksen saavuttamiseen, vaan eri menetelmiä pitää käyttää yhdessä muodostaen toisiaan tukeva kokonaisuus (Puhakainen & Siponen 2010). ADKAR-mallin mukaan halu (desire) voidaan herättää esimerkiksi viestinnän avulla, kun taas tietoa (knowledge) voidaan lisätä koulutuksen avulla.

Kun menetelmien suunnittelussa huomioidaan vielä tunnistetut yksilölliset ja organisatoriset tekijät, voidaan luoda juuri omalle organisaatiolle tehokas tapa lisätä työntekijöiden tietoturvatietoisuutta ja parantaa sitoutumista organisaation tietoturvakäytäntöihin. Myös keskittymällä työntekijän näkökulmaan ja pyrkimällä löytämään vastaus siihen, mitä hyötyä työntekijä voi kokea toivotusta tietoturvakäyttäytymisestä, voidaan yrittää pienentää kirjallisuudessa tunnistettua kuilua tiedon ja tekemisen välillä (Cox, 2012). Keskittymällä kyvykkyyteen (ability) voidaan taas tasapainottaa turvallisuuden, käytännöllisyyden ja käytettävyyden kolmiota ja pienentää ristiriitaa tietoturvan ja toiminnallisuuden välillä (Bada ym. 2019).

PDCA-mallin kolmannessa vaiheessa analysoidaan toteutettujen menetelmien tehokkuutta. Jotta arviointivaihe voidaan toteuttaa, on tärkeää, että aikaisemmin on määritelty kehitettävälle osa-alueelle mittarit, joita voidaan seurata. PDCA-mallin viimeinen vaihe on toimintavaihe, joka perustuu arviointivaiheen tuloksiin. Tehokkaaksi todetut menetelmät voidaan pitää, kun taas menetelmät, joilla ei ole saatu toivottua muutosta aikaan, voidaan poistaa tai niitä voidaan jatkokehittää tilanteen mukaan. Mikäli osa hyödynnetyistä menetelmistä ei toimi halutulla tavalla tai ne vaativat kehittämistä, niin siirrytään takaisin suunnitteluvaiheeseen ja kehitysprosessi alkaa uudestaan. Kun kehittämisellä aletaan saavuttaa haluttuja tuloksia ja tietyn osa-alueen tietoturvakäytännöt alkavat sitoutua osaksi organisaatiokulttuuria, voidaan siirtyä viimeiseen vaiheeseen eli arviointiin.

6.4 Lopputuotokset

Viitekehyksen viimeisessä vaiheessa ollaan maturiteettimallin viimeisellä tasolla ”mittaamisen viitekehys”, jossa kehitettävän tietoturvatietoisuuden osa-alue on osana organisaatiokulttuuria ja sen avulla voidaan osoittaa positiivinen tuottoaste. Tämä

tarkoittaa, että johdolle voidaan konkreettisesti osoittaa, että annetuilla resursseilla on saatu aikaan organisaatiolle hyödyllistä muutosta.

Tietoturvan kentällä tapahtuu jatkuvasti muutoksia, jotka muuttavat myös organisaatioiden kohtaamia tietoturvauhkia. Muutoksia tapahtuu teknologiassa, toimintaympäristössä sekä mahdollisesti organisaation sisällä. Näillä kaikilla on merkittävä vaikutus tietoturvatietoisuuden kehittämiseen. (Wilson & Hash 2003) Vaikka tietyllä osa-alueella olisi päästy viitekehyksen viimeiseen vaiheeseen, on aina mahdollista, että kehityksessä joudutaan palaamaan takaisin PDCA-mallin mukaiseen kehitykseen. Haastatteluissa tuli esimerkiksi ilmi, kuinka organisaatiomuutos voi vaikuttaa tietoturvakulttuurin luomiseen. Mikäli esimerkiksi yrityskaupan yhteydessä organisaatiokulttuuri muuttuu, voidaan olemassa olevia menetelmiä joutua miettimään uudestaan. Toisaalta haastatteluissa nousi esiin haaste mielenkiinnon ylläpitämisestä ja saturaatiopisteen tulemisesta vastaan. Tämä voi olla myös syy palata takaisin edelliseen vaiheeseen ja arvioida hyödynnettyjä menetelmiä uudestaan.

Kun tietoturvatietoisuutta on kehitetty organisaatiossa pidempään systemaattisesti, voidaan monella osa-alueella päästä viimeiseen vaiheeseen, joka taas helpottaa uusien menetelmien implementoimista, koska organisaation tietoturvakulttuuri muuttuu positiivisemmaksi (Da Veiga 2018) ja sosiaaliset normit vaikuttavat siihen, miten hyvin organisaatiossa otetaan vastaan uusia tietoturvaan liittyviä käytäntöjä (Gjertsen ym. 2017; Lund & Aarø 2004). Lisäksi kun organisaatiossa tunnistetaan tietyille kohderyhmille hyvin toimivia menetelmiä, kuten tehokkaita viestintäkanavia ja koulutusmenetelmiä, on uusien tietoturvakäytäntöjen implementoiminen yhä helpompaa. Tietoturvatietoisuuden osa-alueella ei ehkä koskaan voi tehdä tarpeeksi, mutta jatkuvan kehittämisen avulla voidaan pyrkiä vastaamaan kasvaviin haasteisiin (Wilson & Hash 2003).

6.5 Esimerkki viitekehyksen hyödyntämisestä

Tietojenkalastelu on verkkorikollisten eniten hyödyntämä taktiikka ja tietojenkalastelusähköpostit muuttuvat jatkuvasti uskottavimmiksi (SoSafe 2022). Tässä alaluvussa esitellään viitekehyksen hyödyntämistä kuvitteellisen esimerkin avulla, jossa organisaatiossa on havaittu puute tietojenkalasteluviestien tunnistamisessa ja tällä osa-alueella tietoturvatietoisuutta halutaan parantaa. Tähän tarkoitukseen organisaatiossa on päätetty hyödyntää pelillistettyä kalastelukoulutusta, HoxHuntia, joka mainittiin alaluvussa 5.2.4.

Mikäli ajatellaan, että organisaatiossa tietoturvatietoisuutta on jo kehitetty systemaattisesti, ei mallin ensimmäistä kohtaa tarvitse enää huomioida. Organisaatiossa tietoturvatietoisuuden lähtötaso on mitattu, ohjelmalla on selkeät tavoitteet ja johdon tuki sekä resurssit. Tämän lisäksi tietoturvatietoisuutta kehitetään tietoturvan hallintamenetelmän puitteissa, jolloin se on linjassa organisaation liiketoiminnan kanssa. Mikäli organisaatio on ”nollatasolla”, on tärkeää keskittyä huolellisesti tähän vaiheeseen, sillä se luo pohjan eri osa-alueiden kehittämiselle.

Voidaan siis siirtyä PDCA-mallin mukaiseen kehittämisvaiheeseen. Suunnitteluvaiheessa tunnistetaan ja analysoidaan ongelma, organisatoristen ja yksilöllisten tekijöiden vaikutus ja määritetään kohderyhmä. Kalasteluviestien tunnistaminen on tärkeää koko organisaatiossa, joten kohderyhmäksi valitaan koko organisaatio. Organisaatiossa on todettu, että organisaatiokulttuurillisesti osallistavat menetelmät ovat toimivia, joten HoxHunt on hyvä valinta tietoisuuden lisäämiseen. Lisäksi organisaatiossa on tunnistettu roolipohjainen ajattelumalli, minkä HoxHunt mahdollistaa (HoxHunt 2022b).

Toteutusvaiheessa hyödynnettävät menetelmät havaitun ongelman korjaamiseksi suunnitellaan ja toteutetaan ADKAR-mallin mukaan taulukon 6 mukaisesti.

Taulukko 6: Esimerkki ADKAR-mallin hyödyntämisestä

ADKAR-mallin vaihe:	**Toimenpiteet**
Tietoisuus (Awareness)	Tunnistetaan ongelma, että organisaatiossa ei tunnisteta tietojenkalasteluviestejä. Taustalla käytännön tapahtuma, jossa työntekijä on syöttänyt tunnukset huijaussivustolle.
Halu (Desire)	Mietitään, miten työntekijöille saadaan mielenkiinto aihetta kohtaan. Voidaan käyttää viestinnässä käytännön esimerkkiä. Hyödynnetään markkinoinnin perusperiaatteita.
Tieto (Knowledge)	HoxHunt on uusi työkalu, joten on tärkeää viestiä selkeästi sen käytöstä. Hyödynnetään monipuolisesti eri viestintäkanavia ja erilaisia viestintämenetelmiä, esim. videoita ja sähköpostiviestintää.
Kyvykkyys (Ability)	HoxHunt on käytettävyydeltään hyvä, koska se integroituu organisaatiossa käytettyyn sähköpostijärjestelmään. Varmistetaan, että työntekijät osaavat käyttää työkalua.
Vahvistaminen (Reinforcement)	Vahvistetaan työntekijöiden motivaatiota palkitsemalla säännöllisesti HoxHuntissa menestyneitä työntekijöitä. Tuodaan esiin positiivisia tilastoja.

HoxHuntissa on olemassa tietyt sisäänrakennetut mittarit, kuten osallistumisprosentti ja menestymis- sekä epäonnistumisprosentti kalasteluviestin tunnistamisessa. Näitä voidaan hyödyntää mittareina, mutta tärkeää on myös huomioida, kuinka paljon organisaatiossa raportoidaan oikeita kalasteluyrityksiä. Tavoitteena on kuitenkin oikeiden kalasteluviestien raportoinnin lisääminen ja ”haksahdusten” vähentäminen.

Arviointivaiheessa analysoidaan menetelmien tehokkuutta ja sitä, onko haluttua muutosta käyttäytymisessä saavutettu. Voidaan todeta, että käyttöaste on kohtuullisen hyvä ja kalasteluviestejä osataan jo tunnistaa, mutta oikeiden kalasteluyritysten raportointi ei ole lisääntynyt. Neljännessä, toimintavaiheessa todetaan, että jatketaan HoxHuntin käyttöä, mutta pyritään kehittämään sitä niin, että HoxHuntin viestien raportoinnin lisäksi myös oikeiden kalasteluviestin raportointi lisääntyisi. Tämän jälkeen aloitetaan PDCA-malli uudestaan. Kehitetään työkalua niin, että samasta painikkeesta pystyy raportoimaan HoxHunt -viestejä ja muita kalasteluviestejä. Tällöin käytettävyys paranee työntekijöille entisestään. Lisäksi voidaan kehittää uusia tapoja viestiä, joiden avulla tavoitetaan työntekijöitä, jotka eivät ole vielä mukana koulutuksessa.

Kun päästään pisteeseen, jossa HoxHuntia käytetään aktiivisesti koko organisaatiossa ja sen avulla pystytään konkreettisesti osoittamaan muutosta käyttäytymisessä, voidaan siirtyä viimeiseen vaiheeseen. Tämä näkyy esimerkiksi siinä, että HoxHuntin simulaatioviestien lisäksi myös oikeiden kalasteluviestien raportointi on lisääntynyt ja raportointityökalua hyödyntäen on voitu estää tietoturvatapahtumia. Tällöin työkalusta voidaan osoittaa olevan konkreettinen hyöty. Siihen käytetyt kustannukset ovat pienemmät kuin kustannus, jonka organisaatio kärsisi, mikäli se altistuisi tietojenkalastelusta johtuneelle tietovuodolle.

Tässä riskinä on kuitenkin se, että HoxHunt sitoutuu jopa liian hyvin organisaatiokulttuuriin ja kalasteluviestien lisäksi myös oikeita sähköpostiviestejä aletaan raportoimaan. Tällöin voi olla hyvä palata kehitysvaiheeseen ja miettiä, minkä keinojen avulla voidaan pyrkiä estämään väärät ja turhat raportoinnit. Tässä keskeisessä roolissa on esimerkiksi viestintä, jolloin kalasteluviesteiltä vaikuttavista oikeista viesteistä ilmoitetaan myös toisessa kanavassa. Toinen syy, miksi viitekehyksessä voitaisiin joutua siirtymään takaisin kehitysvaiheeseen, olisi esimerkiksi iso organisaatiomuutos, kuten yrityskauppa, jossa organisaatioon tulisi paljon uusia työntekijöitä ja

organisaatiokulttuuri muuttuisi. Tällöin koulutustapa ei välttämättä sopisi uuteen organisaatioon tai ainakin sen käyttö pitäisi implementoida uusille työntekijöille.

7 Pohdinta

7.1 Johtopäätökset

Koko ajan kasvava ja kehittyvä verkkorikollisuus luo jatkuvasti uusia tietoturvauhkia ja vaikka finanssiala on toistaiseksi säilynyt merkittäviltä tietovuodoilta, on uhka todellinen. Suurin osa tapahtuvista tietovuodoista johtuu ihmisen tekemästä virheestä, jonka vuoksi organisaatioissa on alettu kehittämään tietoturvatietoisuutta. Tietoturvatietoisuuden avulla pyritään sitouttamaan työntekijöitä heille asetettuihin tietoturvaan liittyviin tavoitteisiin ja käyttäytymään organisaation tietoturvakäytäntöjen mukaisesti. Kehittämällä tietoturvatietoisuutta, voidaan suojata organisaation tietojärjestelmiä ja kriittistä tietoa ja täten pyrkiä säilyttämään asiakkaiden luottamus.

Tietoturvatietoisuutta on tutkittu melko paljon, mutta kokonaisvaltaisia viitekehyksiä tietoturvatietoisuuden kehittämiseen ei juurikaan ole, vaan tutkimus painottuu enemmän yksilölliseen kuin organisatoriseen näkökulmaan. Tämä tutkielma painottuu tietoturvatietoisuuden systemaattiseen kehittämiseen nimenomaan organisaation näkökulmasta. Tutkimuksessa tehtiin ensin kirjallisuuskatsaus aiempaan tutkimukseen, joka jaettiin kahteen lukuun ”tietoturvatietoisuuden kehittäminen finanssialan organisaatiossa” ja ”tietoturvatietoisuuteen vaikuttavat tekijät”. Haastattelukysymykset rakennettiin teorian pohjalta, jotta myöhemmin voitiin verrata empiriasta saatuja tuloksia teoriaan.

Teoria oli suurilta osin linjassa empiriassa kerättyjen tuloksien kanssa. Keskeisen uusi näkökulma haastatteluista saatiin ADKAR-mallin yhteydessä, joka ei ollut juuri tullut esiin aiemmassa tutkimuksessa. ADKAR-malli on tunnettu muutosjohtamisen malli, mutta tietoturvatietoisuuden kontekstissa sitä ei ole juuri hyödynnetty lukuun ottamatta Da Veigan (2017) tekemää tutkimusta tietoturvakulttuurin muuttamisesta ADKAR-mallia hyödyntäen. Haastatteluissa tuli esille, kuinka ADKAR-mallia voi hyödyntää apuna kehittäessä tehokkaita menetelmiä tietoturvatietoisuuden kehittämiseen. Tätä näkökulmaa hyödynnettiin myös luvun kuusi viitekehyksessä.

Toinen mielenkiintoinen huomio on ajatusmallien muuttuminen liittyen tietoturvatietoisuuteen. Esimerkiksi Albrechtsenin & Hovdenin (2007) esittämä ajatus digitaalisesta kahtiinjaosta todettiin empiriassa vanhentuneeksi ajatusmalliksi. Sen sijaan, että työntekijöiden ajateltaisiin olevan tietoturvauhkia, niin tietoturva-asiantunijat

kaikissa organisaatioissa näkivät inhimillisen riskin syynä sen, että työntekijöitä ei ole koulutettu tarpeeksi tai heille ei ole opastettu mikä on tärkeää. Työntekijät haluttiin nähdä riskin sijaan tietoturvan vahvimpina lenkkeinä tai puolustajina.

Positiivinen näkökulma nousi kaikissa haastatteluissa esiin tärkeimpänä teemana tietoturvatietoisuuden kehittämisessä. Esimerkiksi tietoturvatietoisuutta kehitettävistä menetelmistä rankaisuun suhtauduttiin hyvin varauksella, kun taas palkitsemista pidettiin monessa organisaatiossa tärkeänä. Myös muissa menetelmissä, kuten koulutuksessa ja viestinnässä, sekä tietoturvakulttuurin luomisessa positiivisuus nousi esiin yhtenä tärkeimmistä tekijöistä. Positiivisen tietotototurvakulttuurin luomiselle pidettiin tärkeänä siirtymistä vaatimuskeskeisestä ajattelusta siihen, että työntekijät aidosti ymmärtävät tietoturvan merkityksen ja heidän roolinsa sen toteuttamisessa. Tässä nähtiin keskeisenä käytännönläheisyys, ymmärrettävyys ja mielenkiinnon herättäminen esimerkiksi huumorin ja kuvallisen viestinnän avulla. Lisäksi empiriassa nousi hyvin esille, kuinka paljon organisaatiorakenne, organisaation koko ja organisaation kulttuuri vaikuttavat tietoturvatietoisuuden kehittämiseen. Mikäli organisaatiossa on valmiiksi matala ja yhteistoiminnallinen kulttuuri, on myös tietoturvan tuominen osaksi organisaatiokulttuuria helppoa.

Vaikka tietoturvatietoisuutta on tutkittu jo pitkään, on hyvä huomioida, että haastateltavista organisaatioista systemaattinen kehitys oli kestänyt vasta enimmillään 3–4 vuotta. Tämä tarkoittaa, että aihe on kuitenkin melko tuore ja tietoturvatietoisuuden merkitys ymmärretään koko ajan paremmin. Lisäksi monissa organisaatioissa tietoturvatietoisuuden systemaattinen kehittäminen alkoi vasta, kun organisaatiossa tapahtui tietoturvatapahtuma tai vaihtoehtoisesti organisaatioon sattui tulemaan tietoturvatietoisuudesta kiinnostunut ihminen. Olisi tärkeää, että tietoturvatietoisuuden rooli organisaatioissa ymmärrettäisiin ennen kuin jotain tapahtuu, sillä tietovuodoilla voi pahimmassa tapauksessa olla merkittävä vaikutus organisaation maineeseen ja asiakkaiden luottamukseen koko toimialalla.

Luvussa kuusi esiteltiin tutkielman teorian ja empirian tulosten pohjalta rakennettu viitekehys, joka kuvaa tietoturvatietoisuuden systemaattista kehittämistä. Viitekehyksen tavoitteena on muodostaa mahdollisimman kattava kuva tietoturvatietoisuuden systemaattisesta kehittämisestä finanssialan organisaatiossa. Viitekehys muodostuu jatkuvan kehittämisen PDCA-mallista sekä muutosjohtamisen ADKAR-mallista. Lisäksi

siinä hyödynnetään SANS:in maturiteettimallia arvioimaan kehitystä sekä Parsonsin ym. (2017) viitekehystä tietoturvatietoisuuteen vaikuttavien tekijöiden jaotteluun.

Käytännössä malli muodostuu kolmesta eri vaiheesta. Ensin muodostetaan pohja tietoturvatietoisuuden kehittämiselle täyttämällä tietyt vaatimukset, tämän jälkeen kehitetään eri osa-alueita erilaisten menetelmien avulla ja lopulta pyritään pääsemään tilaan, jossa voidaan osoittaa tietoturvatietoisuudesta saatava konkreettinen hyöty. Mallissa on otettu huomioon myös ympäristössä ja organisaatiossa tapahtuvien muutosten vaikutus sekä erot organisaatioiden rakenteessa ja koossa.

Käytännön tasolla tutkielma tarjoaa finanssialan organisaatioille viitekehyksen, jonka avulla tietoturvatietoisuutta voidaan kehittää systemaattisesti. Tutkielmasta on etenkin hyötyä organisaatioille, joissa tietoturvatietoisuuden kehittäminen on vielä hyvin alkuvaiheessa. Tämän lisäksi tutkielman tuloksia voidaan käyttää myös vertailukohtana organisaatioissa, joissa tietoturvatietoisuutta on kehitetty pidempään. Näissä organisaatioissa voidaan hyödyntää myös viitekehystä kehittämisvaiheesta eteenpäin niin kuin alaluvun 6.5 esimerkissä. Viitekehyksen muodostamisen lisäksi tutkimuksen yhtenä tavoitteena oli jakaa hyväksi todettuja käytäntöjä tietoturvatietoisuuden kehittämiseen finanssialalla. Luvussa 5 tulee esiin paljon eri organisaatioissa tehtyjä huomioita, joista myös muut finanssialan organisaatiot voivat hyötyä miettiessään mahdollisia uusia ideoita tietoturvatietoisuuden kehittämiseen.

Vaikka tutkielma keskittyykin finanssialan organisaatioihin, on tuloksia ja luvussa 6 esiteltyä viitekehystä mahdollista hyödyntää myös muilla toimialoilla. Tutkielmassa korostui, että finanssiala eroaa muista toimialoista lähinnä siinä, että sitä koskee tarkka sääntely ja se on hyvin riippuvainen asiakkaiden luottamuksesta. Tämän takia finanssiala on melko edistynyt tietoturvatietoisuuden kehityksessä. Verkkorikollisuuden lisääntyessä, todennäköisesti myös muilla toimialoilla tietoturvaan liittyvät huolet lisääntyvät. Tällöin myös tietoturvatietoisuuteen aletaan kiinnittämään enemmän huomiota ja tutkielmasta voi olla hyötyä, kun monessa organisaatiossa tietoturvatietoisuutta aletaan rakentamaan alusta. Kasvattamalla tietoturvatietoisuutta organisaatioiden sisällä, voidaan myös edesauttaa tekemään tietoturvasta uutta kansalaistaitoa, joka hyödyttää koko yhteiskuntaamme.

7.2 Yhteenveto

Tässä tutkielmassa tutkittiin tietoturvatietoisuuden kehittämistä finanssialan organisaatiossa. Tutkimuksen aineisto kerättiin haastattelemalla tietoturva-asiantuntijoita neljästä suomalaisesta pankista, joista monet tarjoavat myös laajasti varainhoito- ja vakuutuspalveluita. Tutkittavat organisaatiot ovat eri kokoisia, eri rakenteisia ja eri vaiheissa tietoturvatietoisuuden kehittämisessä. Tutkimuksen päätutkimuskysymys oli ”Miten tietoturvatietoisuutta voidaan kehittää finanssialan organisaatiossa?” Vastaus päätutkimuskysymykseen muodostettiin alatutkimuskysymysten avulla.

Ensimmäinen alatutkimuskysymys oli ”Mitä ovat tietoturvan vaatimukset finanssialalla ja miten ne vaikuttavat tietoturvatietoisuuden kehittämiseen?” Finanssialaa koskee tarkka sääntely, sillä se on kriittisen infrastruktuurin toimija, jossa asiakkaan luottamus on koko toiminnan perusta. Tietoturvallisuus on osa toimivaa riskienhallintaa, jonka vaatimukset finanssialalla perustuvat lainsäädäntöön ja EU:n direktiiveihin. Näissä vaatimuksissa määritellään myös tietoturvakoulutukseen- ja tietoisuuteen liittyvät vaatimukset, joiden mukaan organisaatioissa tulee olla tietoturvan koulutusohjelma, jonka avulla voidaan pienentää inhimilliseen virheeseen liittyvää riskiä. Helpottaakseen tietoturvavaatimuksiin vastaamista, organisaatioissa hyödynnetään tietoturvan hallintajärjestelmiä, joiden perusteella tietoturvatietoisuutta kehitetään. Finanssialan pankki- ja vakuutussalaisuus sekä vaatimuskeskeisyys voivat helpottaa tietoturvatietoisuuden kehittämistä, mutta samaan aikaan organisaatioissa ei voida tuudittua ajatukseen työntekijöiden automaattisesta tietoturvalähtöisyydestä.

Toinen alatutkimuskysymys oli ”Mitkä yksilölliset, organisatoriset ja välilliset tekijät vaikuttavat tietoturvatietoisuuden kehittämiseen?” Tutkielman teoriassa yksilöllisiksi tekijöiksi tunnistettiin demografiset tekijät, minäpystyvyys, yksilön aikaisemman kokemukset ja IT-osaaminen, mutta empiriassa todettiin, että käytännössä yksilöllisiä tekijöitä ei ole mahdollista huomioida suuren organisaation toiminnassa. Yksilöajattelun sijaan tärkeänä pidettiin roolipohjaista ajattelua. Organisatorisista tekijöistä tunnistettiin johdon merkitys, joka voi näkyä esimerkiksi tiiviinä yhteistyönä ja johdon toimimisena työntekijöiden esimerkkinä. Lisäksi organisatorisista tekijöistä tunnistettiin tietoturvaosaston rooli mahdollisimman helposti lähestyttävänä ja palveluorganisaationa. Organisaatiokulttuuri nähtiin merkittävänä osana tietoturvatietoisuuden kehitystä ja positiivisen tietoturvakulttuurin luomisessa pidettiin tärkeänä siirtymistä

vaatimuslähtöisestä ajattelusta syvempään ymmärrykseen. Välillisistä tekijöistä tunnistettiin teoriassakin esiin tulleet viestintä, koulutus sekä harjoitukset ja palkitseminen.

Kolmas alatutkimuskysymys oli ”Minkälaisten menetelmien avulla työntekijöiden tietoturvatietoisuutta voidaan parantaa tehokkaasti finanssialan organisaatiossa?” Menetelmillä viitataan äsken mainittuihin välillisiin tekijöihin eli viestintään, koulutukseen ja harjoituksiin sekä palkitsemiseen. Menetelmien ominaisuudet olivat myös hyvin linjassa teoriassa esille tulleiden tulosten kanssa. Niiden tulisi olla mahdollisimman kansankielisiä sekä lähellä työntekijöiden arkipäiväistä työskentelyä. Lisäksi tulisi huomioida eri kohderyhmät ja hyödyntää erilaisia kanavia ja tapoja viestiä ja kouluttaa. Empiriassa nousi esille myös, kuinka ADKAR-mallia voidaan hyödyntää menetelmien suunnittelussa mahdollisimman tehokkaiksi ja kuinka suunnittelussa tulee ottaa huomioon organisaatiokulttuuri ja mukauttaa menetelmät siihen sopivaksi.

Neljäs alatutkimuskysymys oli ” Miten tietoturvatietoisuutta voidaan mitata ja arvioida?” Molemmat, sekä empiria että teoria, tukivat ajatusta, että käyttäytymisen muutoksen mittaaminen on haasteellista ja etenkin eri menetelmien syy-seuraussuhteita on vaikea todistaa. Mittaamiseen hyödynnettiin esimerkiksi kyselytutkimuksia, osallistumisprosenttien seuraamista, vuorovaikutusta, tietoturvatapahtumien raportointia ja erilaisia työkaluja. Haastatteluissa ja teoriassa tuli myös vahvasti ilmi jatkuvan kehittämisen merkitys tietoturvatietoisuuden parantamiselle.

Luvussa kuusi pyrittiin vastaamaan päätutkimuskysymykseen luomalla tulosten perusteella viitekehys, jonka puitteissa tietoturvatietoisuutta voidaan kehittää mahdollisimman tehokkaasti. Käytännössä tietoturvatietoisuuden systemaattinen kehitys muodostuu edellä mainituista komponenteista eli huomioimalla finanssialan vaatimukset, tunnistamalla tietoturvatietoisuuteen vaikuttavat tekijät, kehittämällä organisaatiolle parhaiten sopivat menetelmät ja lopulta mittaamalla sekä arvioimalla kehitystä jatkuvasti.

7.3 Tutkimuksen luotettavuuden arviointi

Tutkimuksen eettisyyden varmistamiseksi on tärkeää, että tutkimuksessa on noudatettu hyvää tieteellistä käytäntöä (Tuomi & Sarajärvi 2018). Tässä tutkimuksessa käytäntöä on noudatettu esimerkiksi luomalla ennen aineiston keräämistä aineistonhallintasuunnitelma, joka löytyy liitteenä 2 tutkielman lopusta. Lisäksi

tutkielman teossa on käytetty eettisiä tiedonhankinta ja arviointimenetelmiä ja kunnioitettu muiden tutkijoiden työtä oikeellisella viittaustekniikalla.

Laadullisessa tutkimuksessa luotettavuutta on määrällistä tutkimusta haasteellisempi arvioida, koska tutkimus perustuu aina osittain tutkijan subjektiiviseen käsitykseen. Laadullisessa tutkimuksessa tulee siis aina arvioida tutkijan puolueettomuutta. (Tuomi & Sarajärvi 2018) Tässä tutkimuksessa tutkijan puolueettomuuteen vaikuttaa se, että tutkielma on tehty toimeksiantona yhdelle tutkimuksessa mukana olleista organisaatioista. Kaikkiin haastateltaviin on kuitenkin suhtauduttu samalla tavalla ja tulosten analysoinnissa on pyritty olemaan mahdollisimman objektiivinen. Objektiivisuus näkyy esimerkiksi siten, että toimeksiantajaa käsiteltiin haastatteluissa samalla tavalla kuin muitakin haastateltavia eikä toimeksiantajayrityksellä ole ollut pääsyä aineistoon, josta voisi selvitä esimerkiksi haastateltavien henkilötietoja. Tulosten analysointi on tehty täysin perustuen tutkimuksessa kerättyyn aineistoon ja aikaisempaan tutkimukseen, eikä siinä ole erikseen tarkasteltu toimeksiantajaorganisaation näkökulmaa tai muita kuin haastatteluissa selvinneitä tietoja.

Laadullisen tutkimuksessa luotettavuutta ei usein arvioida validiteetin ja reliabiliteetin avulla, sillä ne sopivat paremmin määrälliseen tutkimukseen. Sen sijaan arvioinnissa voidaan käyttää neljää eri kriteeriä, joiden suomennoksissa ja merkityksissä on melko paljon eroja riippuen eri lähteistä. Nämä tekijät ovat uskottavuus (engl. credibility), siirrettävyys (engl. transferability), luotettavuus (engl. dependability) ja vahvistettavuus (engl. confirmability). (Tuomi & Sarajärvi 2018)

Uskottavuudella tarkoitetaan luottamusta tutkimustulosten totuudenmukaisuuteen. Tässä tutkimuksessa tulokset on otettu suoraan alkuperäisestä aineistosta ja niihin viitataan analyysivaiheissa sitaateilla tiedon vahvistamiseksi. Siirrettävyydellä tarkoitetaan sitä, miten tutkimuksen tuloksia voidaan siirtää muihin ympäristöihin. Tutkielmassa kerrotaan haastateltavien roolit, organisaatioiden koko ja luonnollisesti toimiala. Siirrettävyyden kustannuksella tarkempia tietoja ei kerrota haastateltavien anonymiteetin säilyttämiseksi. Luotettavuudella viitataan löydösten kestävyyteen aikaa vastaan eli ulkoista vaihtelua aiheuttavien tekijöiden ja tieteellisten periaatteiden huomiointiin. Tutkimus on toteutettu noudattaen tieteellisiä periaatteita ja siinä on otettu huomioon mahdolliset muutokset kehityksessä, kuten muutokset ympäristössä tai lainsäädännössä. Vahvistettavuudella tarkoitetaan sitä, että tutkimuksen tulokset ovat peräisin haastateltavilta, eikä niihin

vaikuta tutkijan ennakkoasenteet tai vääristymät. Tässä tutkimuksessa on kaikkiin haastatteluihin sekö tulosten analysointiin pyritty suhtautumaan mahdollisimman objektiivisesti ja tutkielmassa esitetään datan analysoinnin prosessi. (Tuomi & Sarajärvi 2018; Korstjens & Moser 2018)

Tässä tutkimuksessa tutkimuksen luotettavuutta heikentää eniten se, että kaikki haastateltavat ovat tietoturva-asiantuntijoita, joilla on vain oma näkemyksensä koskien oman organisaationsa tietoturvatietoisuutta. Luotettavuuden parantamiseksi olisi ollut mielenkiintoista pystyä haastattelemaan myös tutkittavien organisaatioiden muita työntekijöitä, jolloin tutkimuksessa olisi saatu parempi käsitys siitä, mitkä asian vaikuttavat heidän näkökulmastaan tietoturvatietoisuuden kehittämiseen ja mitkä menetelmät he ovat kokeneet tehokkaiksi. Toisaalta tämä ei ollut mahdollista tämän pro gradu -tutkielman puitteissa ja koska tutkimuksen tarkoituksena oli keskittyä systemaattisen kehittämisen näkökulmaan, oli perustelua valita haastatteluihin tietoturvatietoisuuden kehittämisessä mukana olleita asiantuntijoita.

7.4 Jatkotutkimusehdotukset

Tämän tutkimuksen avulla pystyttiin vastaamaan luvussa 2 esitettyyn tutkimusaukkoon ja kehittämään lisää tutkimusta paitsi tietoturvatietoisuudesta finanssialalla myös tietoturvatietoisuuden kehittämisestä organisaation näkökulmasta. Aiheesta on edelleen melko vähän tutkimusta, joten toistettavuuden vuoksi jatkotutkimus olisi hyödyllistä. Olisi etenkin mielenkiintoista saada tutkimusta, jossa samoista organisaatioista voitaisiin tutkia tietoturva-asiantuntijoiden sekä työntekijöiden näkökulmaa. Tällöin pystyttäisiin luomaan laajempi kuva siitä, mitkä ovat tehokkaita menetelmiä tietoturvatietoisuuden kehittämiseen. Jo pelkkä seurantatutkimus esimerkiksi kolmen vuoden päästä voisi tuoda esiin uusia löydöksiä. Seurantatutkimus olisi myös siksi mielenkiintoinen, että monissa organisaatiossa tehdyillä toimenpiteillä oli saatu aikaan vaikutusta, mutta haasteeksi koettiin tarpeeksi ison kattavuus. Seurantatutkimuksen avulla voitaisiin selvittää, johtuuko tämä yksinkertaisesti ajasta vai tarvitseeko kattavuuden saavuttamiseksi toimintaa kehittää eri tavalla.

Yhtenä uutena löydöksenä empiriassa tuli esille ADKAR-malli, jota ei ole vielä hyödynnetty kovin paljoa tietoturvatietoisuuden tutkimuksessa. Olisi mielenkiintoista saada enemmän tutkimusta kyseisen mallin hyödynnettävyydestä tietoturvatietoisuuden osa-alueella. ADKAR-malli on myös osa luvussa kuusi esitettyä viitekehystä

tietoturvatietoisuuden systemaattiseen kehittämiseen. Olisi tärkeää, että viitekehyksen käytettävyyttä voitaisiin tarkastella jatkotutkimuksessa. Tämän avulla voitaisiin selvittää, onko viitekehys hyödyllinen työkalu tietoturvatietoisuuden kehittämiseen ja miten sitä voisi mahdollisesti kehittää tulevaisuudessa. Samalla pystyttäisiin selvittämään ADKAR-mallin soveltuvuutta käytännön tietoturvatietoisuustyöhön. Lisäksi voisi olla hyödyllistä tehdä tutkimusta luodun viitekehyksen, sekä muiden tietoturvatietoisuuden viitekehysten sitoutumisesta tietoturvan hallintamenetelmiin, kuten ISO27000 -standardisarjaan. Täten tietoturvatietoisuus voitaisiin sitoa yhä paremmin kokonaisvaltaisesti organisaation johtamisjärjestelmään ja muuhun tietoturvatyöhön.

Keskeisenä aiheena teoriassa ja empiriassa tuli esille tietoturvatietoisuuden mittaamiseen liittyvät haasteet. Yksilön käyttäytymisen ja etenkin käyttäytymisen muutoksen mittaaminen on muutenkin vaikeaa, mutta suurin haaste liittyy syy-seuraussuhteiden tunnistamiseen. Olisi tärkeää saada tutkimusta ja uusia menetelmiä siihen, miten organisaatioissa voidaan paremmin tunnistaa millä menetelmillä on saavutettu mitäkin hyötyä. Näin myös pystyttäisiin osoittamaan paremmin tietoturvatietoisuusteen liittyvän työn hyödyt ja samaan lisää resursseja kehitykseen sekä kohdentamaan olemassa olevia resursseja paremmin.

Toinen esiin tullut aihe oli roolipohjaisuus, jota pidettiin äärimmäisen tärkeänä puhuttaessa tietoturvatietoisuuden avulla kehitettävistä menetelmistä. Kuitenkin monessa haastattelussa nousi esiin, että roolipohjainen ajattelu on haastavaa etenkin suuremmissa organisaatioissa ja se vaatii muutenkin paljon resursseja. Olisi hyödyllistä saada tutkimusta siitä, miten roolipohjaisuutta voitaisiin soveltaa organisaatiossa mahdollisimman kustannustehokkaasti. Lisäksi olisi mielenkiintoista tietää lisää, mitkä ovat finanssialan organisaatioissa keskeisiä rooleja ja minkälaiset menetelmät sopivat näille rooleille.

Ylipäänsä tietoturvan kenttä on jatkuvassa muutoksessa teknologioiden kehittyessä, joten jatkuva tutkimus kaikista tietoturvan osa-alueista on äärimmäisen tärkeää. Kun organisaatioissa aletaan tunnistaa paremmin inhimillistä riskiä ja sen aiheuttamaa uhkaa organisaation liiketoiminnalle, tulee myös tarve tiedolle aiheesta lisääntymään. Tämän takia tutkimus tietoturvatietoisuudesta tulee olemaan tulevaisuudessa entistä arvokkaampaa.

Lähteet

Ajzen, I. (1991) The theory of planned behavior. *Organizational behavior and human decision processes*, 50(2), 179–211.

Albrechtsen, E. – Hovden, J. (2009) The information security digital divide between information security managers and users. *Computers and Secur*ity, 28(6), 476–490.

Albrechtsen, E. (2007) A qualitative study of users' view on information security. *Computers and Securit*y, 26(4), 276–289.

Allport, G. (1935) Attitudes. Teoksessa: *A Handbook of Social Psychology*, toim. Charles F Murchison, 798– 844. Clark Univ. Press, Worcester.

Almuhammadi, S. – Alsaleh, M. (2017) Information security maturity model for NIST cyber security framework. *Computer Science & Information Technology (CS & IT)*, 7(3), 51–62.

Amankwa, E. – Loock, M. – Kritzinger, E (2014) A conceptual analysis of information security education, information security training and information security awareness definitions. *2014 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)*, 248–252.

Armstrong, G. – Adam, S. – Denize, S. – Kotler, P. (2014) *Principles of marketing*. Pearson Australia.

Ashenden, D. (2008) Information Security management: A human challenge? *Information Security Technical Report*, 13(4), 195–201.

Bada, M. – Sasse, A. M. – Nurse, J. R. (2019) Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*.

Bandura, A. (1994) Self-efficacy. Teoksessa: *Encyclopedia of human behavior,* toim. Vilayanur S. Ramachandran, 71–81. Academic Press, New York.

Bauer, S. – Bernroider, E. W. N. (2017) From information security awareness to reasoned compliant action: Analyzing information security policy compliance in a large banking organization. *Data Base for Advances in Information Systems*, 48(3), 44–68.

Barclay, C. (2014) Sustainable security advantage in a changing environment: The cybersecurity capability maturity model (CM2). *Proceedings of the 2014 ITU Kaleidoscope Academic Conference: Living in a Converged World - Impossible Without Standards?* 275–282.

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

Bulgurcu, B. – Cavusoglu, H. – Benbasat, I. (2010) Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly,* 34(3), 523–548.

Burke, B. (2016) *Gamify: How gamification motivates people to do extraordinary things.* Routledge, New York.

Caruna (2022) Tietoturvapäällikön blogi: asetelma yrityksen ja kyberrikollisen välillä on epäreilu – siksi henkilöstö on koulutettava. <https://caruna.fi/ajankohtaista/tietoturvapaallikon-blogi-asetelma-yrityksen-ja-kyberrikollisen-valilla-epareilu>, haettu 4.8.2022.

Choi, N. – Kim, D. – Goo, J. – Whitmore, A. (2008) Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action. *Information Management & Computer Security*, 16(5), 484–501.

Cox, J. (2012) Information systems user security: A structured model of the knowing-doing gap. *Computers in Human Behavior*, 28(5), 1849–1858.

Critchfield, T.S. (2012) Operant Learning. Teoksessa: *Encyclopedia of the Sciences of Learning*, toim. Norbert M. Seel, 2527–2529. Springer, Boston.

Cybersecurity Venture (2022) Cryptocrime To Cost The World 30 Billion Annually by 2025, <https://cybersecurityventures.com/cryptocrime-to-cost-the-world-30-billion-annually-by-2025/>, haettu 16.10.2022.

Da Veiga, A. – Eloff, J. H. P. (2010) A framework and assessment instrument for information security culture. *Computers and Security*, 29(2), 196–207.

Da Veiga, A. (2018) An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture. *Information and Computer Security*, 26(5), 584–612.

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

Davis, F.D. (1989) Perceived Usefulness, Perceived Ease Of Use, And User Acceptance. *MIS Quarterly*, 13(3), 319–340.

Deming, W.E. (1952) *Elementary Principles of the Statistical Control of Quality: a series of lecture*. 2. p. Nippon Kagaku Gijutsu Remmei, Tokyo.

Disterer, G. (2013) ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security*, 4(2), 92–100.

European Banking Authority (2019) EBA Guidelines on ICT and security risk management, marraskuu 2019. Final report on guidelines on ICT and security risk management. <https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management>, haettu 26.10.2022.

Eminağaoğlu, M. – Uçar, E. – Eren, Ş. (2009) The positive outcomes of information security awareness training in companies - A case study. *Information Security Technical Report*, 14(4), 223–229.

ENISA (2010) The new users' guide: How to raise information security awareness. European Network and Information Security Agency. <https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide>, haettu 26.10.2022.

Eriksson, P. – Kovalainen, A. (2015) *Qualitative Methods in Business Research: A practical guide to social research*, 2. p. SAGE Publications Ltd.

Finanssiala (2021a) MustRead: Suomalaispankkien varautuminen kyberuhkiin on maailmanlaajuisesti huippuluokkaa, mutta kilpajuoksu rikollisten kanssa kiihtyy. <https://www.finanssiala.fi/uutiset/mustread-suomalaispankkien-varautuminen-kyberuhkiin-huippuluokkaa-kilpajuoksu-rikollisten-kanssa-kiihtyy/>, haettu 26.1.2022.

Finanssiala (2021b) Vastuullisen finassialan teesit. <https://www.finanssiala.fi/aiheet/vastuullisen-finanssialan-teesit/>, haettu 24.8.2022.

Finanssialalle (2022a) Finanssiala on mainettaan inhimillisempi. <https://www.finanssialalle.fi/alalle-toihin/finanssiala-mainettaan-inhimillisempi.html>, haettu 16.10.2022.

Finanssialalle (2022b) Finanssimarkkinoiden toimijat. <https://www.finanssialalle.fi/opintomateriaalit/finanssialan-perusteet/finanssialalla-toimiminen/finanssimarkkinoiden-toimijat.html>, haettu 16.10.2022.

Finanssivalvonta (2014) Operatiivisten riskien hallinta rahoitussektorin valvottavissa. Finanssivalvonnan määräykset ja ohjeet 8/2014. <https://www.finanssivalvonta.fi/saantely/maarays-ja-ohjekokoelma/riskienhallinta/08_2014/>, haettu 26.10.2022.

Finanssivalvonta (2020) Finanssialan toimijoiden tietoturvallisuutta tarkastellaan useassa eri vaiheessa – sääntely tiukentuu todennäköisesti entisestään. <https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/verkkouutiset/2020/finanssialan-toimijoiden-tietoturvallisuutta-tarkastellaan-useassa-eri-vaiheessa--saantely-tiukentuu-todennakoisesti-entisestaan/>, haettu 6.4.2022.

Fishbein, M. – Ajzen, I. (1975*) Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research*. Addison-Wesley.

Fosnot, C. T. (2013) *Constructivism: Theory, perspectives, and practice*. Teachers College Press.

F-Secure (2022) Mitä on kyberturvallisuus? <https://www.f-secure.com/fi/home/articles/what-is-cyber-security>, haettu 24.8.2022.

Ghazvini, A. – Shukur, Z. (2018) A serious game for healthcare industry: Information security awareness training program for Hospital Universiti Kebangsaan Malaysia. *International Journal of Advanced Computer Science and Applications*, 9(9), 236–245.

Gibbs, J. P. (1968) Crime, Punishment, and Deterrence. *The Southwestern Social Science Quarterly*, 48(4), 515–530.

Gjertsen, E. G. B. – Gjære, E. A. – Bartnes, M. – Flores, W. R. (2017) Gamification of Information Security Awareness and Training, *ICISSP*, 59–70.

Haeussinger, F. J – Sieben, P. D. G. (2015) *Information Security Policy*, 1–16.

Helsingin Sanomat 14.10.2014 *Vielä 90-luvulla Suomessa tehtiin yli sata pankkiryöstöä vuodessa*. <https://www.hs.fi/ulkomaat/art-2000002769283.html>, haettu 24.10.2022.

Hiatt, J. (2006) *ADKAR: A model for change in business, government, and our community*. Prosci Research.

Hirsjärvi, S. – Hurme, H. (1995*) Teemahaastattelu*. Yliopistopaino, Helsinki.

HoxHunt (2022a) Behavioral Cybersecurity Statistics. Exclusive Data Report, tammikuu 2022. HoxHunt eBook. <https://www.hoxhunt.com/behavioral-cybersecurity-ebook>, haettu 26.10.2022.

HoxHunt (2022b) Etusivu. <https://www.hoxhunt.com>, haettu 18.10.2022.

Huoltovarmuuskeskus (2020) Kyberturvallisuuden nykytila eri toimialoilla – kartoituksen keskeiset havainnot. Huoltovarmuusorganisaation Digipooli. <https://www.digipooli.fi/en/node/1794>, haettu 31.1.2022.

Huoltovarmuuskeskus (2005) CIP – kriittisen infrastruktuurin turvaaminen, tammikuu 2015. Huoltovarmuuskeskus.

Hwang, I. – Wakefield, R. – Kim, S. – Kim, T. (2021) Security Awareness: The First Step in Information Security Compliance Behavior. *Journal of Computer Information Systems*, 61(4), 345–356.

ISACA (2015) Leveraging COBIT to Implement Information Security <https://www.isaca.org/resources/news-and-trends/industry-news/2015/leveraging-cobit-to-implement-information-security>, haettu 5.10.2022.

ISACA (2022) COBIT. <https://www.isaca.org/resources/cobit>, haettu 12.10.2022.

ISF (2007) The Evolution of Security Awareness, The executive level summary of the ISF's Effective Security Awareness Report (2002), 2008. Information Security Forum Limited. <https://www.isflive.org/s/article/DOC-1338<, haettu 26.10.2022.

ISF (2014) From Promoting Awareness to Embedding Behaviors, helmikuu 2014. Information Security Forum Limited. <https://www.isflive.org/s/article/DOC-10973>, haettu 26.10.2022.

ISF (2022) Standards of Good Practice for Information Security 2022, maaliskuu 2022. Information Security Forum Limited. <https://www.isflive.org/s/article/Standard-of-Good-Practice-for-Information-Security-2022-PDF-Format>, haettu 26.10.2022.

ISO (2022) ISO/IEC 27001 information security management, <https://www.iso.org/isoiec-27001-information-security.html>, haettu 12.10.2022.

Johnson, C. N. (2002) The benefits of PDCA. *Quality Progress*, 35(5), 120.

Kaarbo, J. – Beasley, R. K. (1999) A practical guide to the comparative case study method in political psychology. *Political Psychology*, 20(2), 369–391.

Kajzer, M. – D'Arcy, J. – Crowell, C. R. – Striegel, A. – Van Bruggen, D. (2014) An exploratory investigation of message-person congruence in information security awareness campaigns. *Computers and Security*, 43, 64–76.

Karjalainen, M. – Suprateek, S. – Siponen, M. (2019) Toward a theory of information systems security behaviors of organizational employees: A dialectical process perspective. *Information Systems Research*, 30(2), 687–704.

Khan, B. – Alghathbar, K. S. – Nabi S. I. – Khan, M. K. (2011) Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management*, 5(26), 10862–10868.

Khando, K. – Gao, S. – Islam – S. M. – Salman, A. (2021) Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers and Security*, 106, 1–22.

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

Kruger, H. A. – Kearney, W. D. (2006) A prototype for assessing information security awareness. *Computers and Security*, 25(4), 289–296.

Kuluttajaliitto (2022) Varo, varoita, varmista: Suomalaisilta viety tänä vuonna jo kymmeniä miljoonia nettihuijauksilla – näin suojaudut, <https://www.kuluttajaliitto.fi/blog/2022/07/07/yhteistiedote-varo-varmista-ja-varoita-nettihuijaukset-ja-tietojenkalastelu-muuttavat-muotoaan-mutta-niilta-on-mahdollista-suojautua/, haettu 1.8.2022.

Lebek, B. – Uffen, J. – Neumann, M. – Hohler, B. – Breitner, M. H. (2014) Information security awareness and behavior: A theory-based literature review. *Management Research Review*, 37(12), 1049–1092.

Lebek, B. – Uffen, J. – Neumann, M. – Hohler, B. – Breitner, M. H. (2014) Information security awareness and behavior: A theory-based literature review. *Management Research Review*, 37(12), 1049–1092.

Lund, J. – Aarø, L. E. (2004) Accident prevention. Presentation of a model placing emphasis on human, structural and cultural factors. *Safety Science*, 42(4), 271–324.

McCormac, A. – Zwaans, T. – Parsons, K. – Calic, D. – Butavicius, M. – Pattinson, M. (2017) Individual differences and Information Security Awareness. *Computers in Human Behavior*, 69, 151–156.

Merriam-Webster (2022) Gamification. <https://www.merriam-webster.com/dictionary/gamification>, haettu 17.10.2022.

NIST (2022) Etusivu. <https://www.nist.gov>, haettu 12.10.2022.

OWASP (2022) OSWAP Security Culture, Security Champion. <https://owasp.org/www-project-security-culture/v10/4-Security_Champions/>, haettu 20.10.2022.

Parsons, K. – Calic, D. – Pattinson, M. – Butavicius, M. – McCormac, A. – Zwaans, T. (2017) The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers and Security*, 66, 40–51.

Parsons, K. – McCormac, A. – Butavicius, M. – Pattinson, M. – Jerram, C. (2014) Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers and Security*, 42, 165–176.

PCI (2022) Etusivu. <https://www.pcisecuritystandards.org>, haettu 12.10.2022.

Peltier, T. (2005) Implementing an Information Security Awareness Program. *Information Systems Security*, 14(2), 37–49.

Prosci (2022) The Prosci ADKAR Model. <https://www.prosci.com/methodology/adkar>, haettu 19.10.2022.

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

Rhee, H. S. – Kim, C. – Ryu, Y. U. (2009) Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers and Security*, 28(8), 816–826.

Rogers, R. W. (1975) A protection motivation theory of fear appeals and attitude change. *The journal of psychology*, 91(1), 93–114.

Saaranen-Kauppinen, A., – Puusniekka, A. (2009) *Menetelmäopetuksen tietovaranto KvaliMOTV*. Yhteiskuntatieteellisen tietoarkisto, Tampere.

SANS (2021) Measure and manage your human risk: Achieve Data-Driven Results with Behavioral Risk Assesment, kesäkuu 2021. SANS Institute.

SANS (2022) Managing Human Risk. SANS 2022 Security Awareness Report, SANS Security Awareness. <https://www.sans.org/blog/sans-2022-security-awareness-report/>, haettu 26.10.2022.

Saunders, M. – Lewis, P., – Thornhill, A. (2009) *Research methods for business students*. Pearson education.

Saxholm, Niko (2022) Niin kauan, kun pankkitunnuksia annetaan puhelimitse, on syytä olla huolissaan. Finanssiala 19.5.2022. [Kolumni]. <https://www.finanssiala.fi/kolumni/niin-kauan-kun-pankkitunnuksia-annetaan-

puhelimitse-on-suomalaisten-digitaidoista-syyta-olla-huolissaan/>, haettu 22.5.2022.

Shaw, R. S. – Chen, C. C. – Harris, A. L. – Huang, H. J. (2009) The impact of information richness on information security awareness training effectiveness. *Computers and Education*, 52(1), 92–100.

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

Siponen, M. T. (2000) Conceptual foundation for organizational information security awareness. *Information Management and Computer Security*, 8(1), 31–41.

SoSafe (2022) *Human Risk Review 2022*. SoSafe GmbH, Germany.

Suomen Pankki (2021) Pääjohtaja Olli Rehn: Kriisiherkkyys kasvanut myös maksamisessa – häiriöihin varaudutaan yhteisin toimin. Suomen Pankin pääjohtaja Olli Rehnin puhe maksufoorumissa 2021. <https://www.suomenpankki.fi/fi/media-ja-julkaisut/puheet-ja-haastattelut/2021/paajohtaja-olli-rehn-kriisiherkkyys-kasvanut-myos-maksamisessa -hairioihin-varaudutaan-yhteisin-toimin/>, haettu 26.1.2022.

Susanto, H. – Almunawar, M. N. – Tuan, Y. C. (2011) Information security management system standards: A comparative study of the big five. *International Journal of Electrical Computer Sciences IJECS-IJENS*, 11(5), 23–29.

TEPA-termipankki (2022) Kyberturvallisuus. <https://termipankki.fi/tepa/fi/haku/kyberturvallisuus>, haettu 13.4.2022.

Tietosuojavaltuutetun toimisto (2022) Tietosuoja. <https://tietosuoja.fi/tietosuoja>, haettu 13.4.2022.

Tilastokeskus (2022) Pienet ja keskisuuret yritykset. <https://www.stat.fi/meta/kas/pienet_ja_keski.html>, haettu 26.10.2022.

Traficom (2020) Tietoturva. <https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva>, haettu 19.10.2022.

Tsohou, A. – Karyda, M. – Kokolakis, S. (2015) Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers and Security*, 52, 128–141.

Tsohou, A. – Kokolakis, S. – Karyda, M. – Kiountouzis, E. (2008) Investigating information security awareness: Research and practice gaps. *Information Security Journal*, 17(5–6), 207–227.

Tuomi, J. – Sarajärvi, A. (2018) *Laadullinen tutkimus ja sisällönanalyysi*. Tammi, Helsinki.

Valtiovarainministeriö (2017) Ohje riskienhallintaan, kesäkuu 2017. Valtiovarainministeriön julkaisuja 22/2017. <https://julkaisut.valtioneuvosto.fi/handle/10024/80013>, haettu 26.10.2022.

Varmuuden Vuoksi (2020) Finanssialaa tarvitsevat kaikki. Huoltovarmuuskeskuksen verkkolehti. <https://www.varmuudenvuoksi.fi/aihe/finanssiala/506/finanssialaa_tarvitsevat_kaikki>, haettu 22.4.2022.

Verdict (2018) 88 % of UK data breaches caused by human error. <https://www.verdict.co.uk/uk-data-breaches-human-error/>, haettu 1.2.2022.

Wall, J.D. – Palvia, P. (2022) "Understanding employees' information security identities: an interpretive narrative approach", *Information Technology & People*, 35(1), 435–458.

Warkentin, M. – Willison, R. (2009) Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems*, 18(2), 101–105.

Wiley, A. – McCormac, A. – Calic, D. (2020) Computers & Security More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security*, 88, 1–8.

Wilson, M. – Hash, J. (2003) Building an Information Technology Security Awareness and Training Program. *NIST Special publication*, 800(50), 1–39.

Liitteet

Liite 1: Haastattelurunko

Lämmittelykysymykset: Organisaation ja haastateltavan tausta

1. Kerro lyhyesti organisaation taustasta (koko, ikä jne.)?
2. Miten tietoturva on organisoitu organisaatiossa?
3. Kerro lyhyesti omasta kokemuksestasi tietoturvan parissa?

Teema 1: Organisaation tietoturvatietoisuus

4. Miten näette tietoturvan ja tietoturvatietoisuuden roolin finanssialalla? Miten finanssiala eroaa muista kriittisen infrastruktuurin toimijoista/toimialoista?
5. Onko teillä käytössä tietoturvatietoisuusohjelma tai yleisesti tietoturvaohjelma, jonka puitteissa tietoturvatietoisuutta kehitetään?
6. Kerro hieman yleisesti organisaation tietoturvatietoisuudesta. Miten ja milloin tietoturvatietoisuutta on lähdetty kehittämään?
7. Onko tietoturvatietoisuuden kehittämisen pohjana käytetty viitekehystä?
8. Mikä oli tietoturvatietoisuuden lähtötaso? Mihin lähtötason mittaus perustuu?
9. Ketkä ovat osallistuneet tietoturvatietoisuuden kehittämiseen?
10. Mikä on teillä ollut tietoturvatietoisuuden kehittämisen juurisyy?
11. Miten tietoturvatietoisuuden kehittäminen sitoutuu koko organisaation strategiaan ja arvoihin?

Teema 2: Tietoturvatietoisuuteen vaikuttavat tekijät

12. Mitä yksilöllisiä ja organisatorisia tekijöitä olette tunnistaneet vaikuttavan tietoturvatietoisuuden kehittämiseen?
13. Minkä näette johdon rooliksi tietoturvatietoisuuden kehittämisessä?
14. Miten olette huomioineet nämä tekijät tietoturvatietoisuuden kehittämisessä?

15. Miten näette tietoturvan osana organisaatiokulttuurianne ja miten se näkyy? Mihin suuntaan sen pitäisi kehittyä?

16. Mitkä näette avaintekijöiksi positiivisen tietoturvakulttuurin luomisessa?

Teema 3: Tietoturvatietoisuuden kehittämisen menetelmät

17. Mitä menetelmiä olette hyödyntäneet tietoturvatietoisuuden parantamiseen organisaatiossa?

18. Mitä/minkälaisia viestinnän keinoja/tietoturvakampanjoita olette hyödyntäneet tietoturvatietoisuuden kehittämiseen?

19. Minkälaisen viestinnän olette kokeneet vaikuttavimmiksi?

20. Minkälaista tietoturvakoulutusta teette/minkälaisia tietoturvaharjoituksia hyödynnätte tietoturvatietoisuuden parantamiseen (jos hyödynnätte)?

21. Minkälaiset harjoitukset olette kokeneet vaikuttavimmiksi?

22. Oletteko hyödyntäneet palkitsemista tai rankaisemista tietoturvatietoisuuden kehittämisessä?

23. Tietoturvatietoisuutta tutkivassa kirjallisuudessa on tullut usein esille niin sanottu kuilu tiedon ja tekemisen välillä, joka tarkoittaa, että työntekijät tietävät organisaation tietoturvakäytännöistä, mutta eivät silti toteuta niitä. Oletteko tunnistaneet tämän ja jos olette, miten olette pyrkineet korjaamaan ongelmaa?

Teema 4: Tietoturvatietoisuuden mittaaminen ja arviointi

24. Miten mittaatte tietoturvatietoisuutta organisaatiossa?

25. Mikä on muuttunut ja mihin suuntaan? Onko mittarit muuttuneet?

26. Mitä haasteita olette kokeneet tietoturvatietoisuuden kehittämisessä, ja missä olette onnistuneet erityisen hyvin?

Liite 2: Aineistonhallintasuunnitelma

Tutkimusaineisto

Aineistotyyppi	Sisältää henkilötietoja*	Tuotan aineiston itse	Joku muu on tuottanut aineiston	Muuta huomioitavaa
Aineistotyyppi 1: *Haastattelut*	x	x		
Aineistotyyppi 2: *Nauhoitukset*	x	x		
Aineistotyyppi 2: *Henkilökohtaiset muistiinpanot*		x		

Henkilötietojen käsittely tutkimuksessa

Laadin tutkittavilleni tietosuojailmoituksen ja toimitan sen heille ennen aineiston keruuta ☒

Henkilötietojen osalta rekisterinpitäjänä toimii opiskelija ☒ yliopisto ☐

Aineistoni ei sisällä henkilötietoja ☐

Aineiston käyttöön liittyvät luvat ja oikeudet

Itse tuotettu aineisto

Aineistotyyppi 1: Haastattelut, nauhoitukset ja henkilökohtaiset muistiinpanot

Ennen haastatteluja, tuon esiin aineiston hallintaan liittyvät asiat:

- Haastattelut nauhoitetaan tutkimusten analysointia varten ja teen haastatteluiden aikana henkilökohtaisia muistiinpanoja.
- Muistiinpanot säilytetään tutkimuksen aikana toimeksiantoyrityksen OneDrivessä sekä Yliopiston verkkokansiossa.
- Nauhoitukset säilötään toimeksiantoyrityksen OneDriveen sekä yliopiston verkkokansioon siihen asti, kunnes litterointi on valmis.

- Litteroidut tulokset eivät sisällä henkilökohtaisia tietoja haastateltavasta tai tunnistettavia tietoja yrityksestä.
- Litteroidut tulokset säilytetään Turun Yliopiston verkkokansiossa, kunnes tutkielma on valmis ja arvioitu.
- Kerättyä dataa hyödynnetään ainoastaan tutkimustarkoituksiin.

Toimeksiaintoyritys on tietoinen haastateltavista ihmisistä ja yrityksistä, mutta aineisto/tulokset ovat täysin anonymisoituja.

Aineiston säilyttäminen tutkimuksen aikana

Jossakin muualla, missä? ☒

Nauhoitan haastattelut joko toimeksiantoyrityksen Teams -alustalla tai puhelimen Voice Memos -sovelluksella. Nauhoitukset siirretään välittömästi yrityksen One Driveen ja säilytetään siellä yksityisessä kansiossa.

Aineiston dokumentointi ja metadata

Aineiston dokumentointi

tutkimuspäiväkirjaa ☐
erillistä dokumenttia, johon kirjaan aineiston pääasiat, kuten tehdyt muutokset, analyysin vaiheet sekä esim. muuttujien merkitykset ☒
aineiston mukana kulkevaa readme-tiedostoa, jossa kuvataan aineiston pääasiat ☐
jotain muuta, mitä? ☐

Aineiston järjestys ja eheys

Säilytän alkuperäisen aineiston erillään tutkimuksenteon aikana käyttämästäni aineistosta, jotta voin palata alkuperäiseen, jos tarvetta ilmenee. ☒

Versionhallinta: mietin jo ennen tutkimuksenteon alkua, miten tulen nimeämään eri aineistoversiot ja noudan sitä systemaattisesti ☐

Tiedostan jo tutkimuksen alussa aineistoni elinkaaren, ja varaudun tilanteisiin, joissa data saattaa huomaamatta muuttua, kuten esim. nauhoitus, litterointi, konversio toiseen tiedostomuotoon, tallentaminen jne. ☐

Metadata

Tallennan aineistoni arkistoon tai tietopankkiin, joka huolehtii metadatasta puolestani. ☐

Minun pitää luoda metadata, koska arkisto, johon tallennan aineiston edellyttää sitä. ☐

En tallenna aineistoani julkiseen arkistoon, enkä tarvitse metadataa. ☒

Aineisto tutkimuksen valmistuttua

Poistan kaiken aineiston, kun tutkielma ja hyväksytty ja arvioitu.