Tampereen yliopisto

Manu Mäki-Rajala

SUORITUSPALAUTTEEN ROOLI ORGANISAATION TIETOTURVAKULTUURIN KEHITTÄMISESSÄ

Kandidaatintutkielma
Johtamisen ja talouden tiedekunta
Tarkastaja: Jussi Myllärniemi
Toukokuu 2023

TIIVISTELMÄ

Manu Mäki-Rajala: Suorituspalautteen rooli organisaation tietoturvakulttuurin kehittämisessä
The role of performance feedback in the development of an organization's information security culture
Kandidaatintyö
Tampereen yliopisto
Tietojohtamisen tutkinto-ohjelma
Toukokuu 2023

Digitaalisen transformaation myötä organisaatioiden mahdollisuudet kerätä tietoa kehittyvät. Tiedon määrän kasvaessa ja digitaalisten toimintaympäristöjen laajentuessa organisaatiot altistuvat suuremmalle määrälle digitaalisia haavoittuvuuksia. Näin ollen organisaatioiden tietoturvallisuuden merkitys korostuu digitaalisen transformaation myötä. Vaikka tietoturvallisen organisaation edellytyksenä on tietoturvallinen teknologia, on tietotekniikkaa käyttävän henkilöstön havaittu olevan teknologiaa yleisempi tietoturvapoikkeamien aiheuttaja. Tietoturvakulttuuri ilmentää henkilöstön valmiuksia toimia tietoturvallisesti. Tämän takia tutkimuksessa pyritään selvittämään tietoturvakulttuurin kehittämismahdollisuuksia.

Tietoturvakulttuuri mielletään organisaatiokulttuurin osaksi. Jotta organisaatiokulttuuri voisi kehittyä, vaaditaan organisaatio-oppimista. Tällaista kollektiivista henkilöstön oppimista voi saavuttaa hyödyntämällä suorituspalauteteoriaa. Siinä tietylle organisaation toiminnalle asetetaan tavoitteet valitulla mittarilla, ja toteutetaan suorituskyvyn mittausta kyseisellä mittarilla. Tavoitteita ja toteutunutta suoriutumista vertaamalla saadaan toiminnasta suorituspalautetta, jonka tarkoitus on tukea organisaation johdon päätöksentekoa. Tutkimusta suorituspalautteen potentiaalista tietoturvakulttuurin kehittämiseksi on suhteellisen vähän. Tässä kandidaatintyössä tutkitaankin suorituspalauteteorian yhteensopivuutta tietoturvakulttuurin kehitystyöhön. Työssä vastataan päätutkimuskysymykseen ”Mikä on suorituspalautteen rooli organisaatioiden tietoturvakulttuurin kehittämisessä?”.

Kirjallisuuskatsauksena toteutetun tutkimuksen aineisto koostuu konferenssi- ja artikkelijulkaisuista sekä yhdestä e-kirjasta. Tutkimus osoittaa suorituspalauteteorialla olevan potentiaalia tietoturvakulttuurin mittaamisen ja arvioimisen viitekehyksenä. Koska tietoturvakulttuuria voidaan mitata ja sille voidaan määrittää tavoitetaso, suorituspalauteteoria on sovellettavissa tietoturvakulttuurin kehittämiseen. Kirjallisuuskatsauksen perusteella suorituspalauteteorian hyödyntäminen tietoturvakulttuurin kehittämiseksi vaatii oman organisaation tuntemista, koska tietoturvakulttuurin mitattavat ulottuvuudet ovat organisaatiokohtaisia. Tutkimus korostaa lisäksi vertaisorganisaatioiden sekä ulkopuolisen näkökulman hyödyntämisen merkitystä tietoturvakulttuurin tavoitteiden määrittelyssä. Suorituspalaute ei itsessään takaa tietoturvakulttuurin kehitystä, vaan vastuu sen tulkinnasta on organisaation johdolla, jonka tehtävä on käynnistää ongelmahakuja organisaatio-oppimisen aikaansaamiseksi. Kirjallisuuskatsauksen perusteella palautteen välittäminen koko henkilöstölle on oleellista.

Avainsanat: organisaatio-oppiminen, suorituspalaute, suorituspalauteteoria, tietoturvakulttuuri

ALKUSANAT

Tämä kandidaatintyö on toteutettu osana Tietojohtamisen koulutusohjelmaa keväällä 2023. Mielenkiinto tietoturvallisuuteen sekä organisaatio-oppimisen mahdollisuuksiin johdatteli minua aiheeni valintaan. Henkilökohtaisten mielenkiinnonkohteiden lisäksi halusin aiheeni olevan ajankohtainen. Tämä kriteeri johdatteli niin ikään tietoturvakulttuurin näkökulman valintaan.

Tutkimusprosessi oli melko raskas, mutta samalla mielenkiintoinen ja erittäin opettavainen. Haluan kiittää ohjaajaani Jussi Myllärniemeä laadukkaista neuvoista sekä ajatuksieni haastamisesta kannustavasti. Sain häneltä lisäksi paljon apua tutkimukseni tarkentamisessa. Ajatuksen suorituspalautteen valinnasta näkökulmaksi sain Tampereen yliopiston professori Hannu Kärkkäiseltä, mistä olen kiitollinen. Lisäksi suuri kiitos kuuluu koko opponointiryhmälleni. Ryhmä antoi kehittävää palautetta, mutta ennen kaikkea toimi erinomaisena vertaistukena prosessin aikana. Haluan kiittää myös läheisiäni tuesta ja motivoinnista läpi prosessin.

Toivon, että työni valaisee lukijoille tietoturvakulttuurin tärkeyttä ja antaa uusia näkökulmia sen kehittämiselle suorituspalautteen avulla. Toivon sen myös kannustavan tietoturvakulttuurin kehittämisen jatkotutkimuksiin.

Tampereella, 3.5.2023

Manu Mäki-Rajala

SISÄLLYSLUETTELO

LYHENTEET

BTOF	Behavioral theory of the firm Suomeksi: Yrityksen käyttäytymisteoria
ISCFF	Information security culture key factors framework Suomenksi: Tieturvakulttuurin avaintekijöiden viitekehys

1. JOHDANTO

Tutkimuksen aiheena on suorituspalautteen rooli tietoturvakulttuurin kehitystyössä. Suorituspalauteteoriaa pyritään soveltamaan tekstissä tietoturvakulttuurin kontekstissa. Tutkimus suoritetaan kirjallisuuskatsauksena.

1.1 Taustoitus

Digitalisaatio tuo organisaatioille uusia mahdollisuuksia muun muassa saatavissa olevan tiedon määrän kasvaessa. Tiedon määrän ja arvon kasvaessa korostuu kuitenkin myös teknologisien epäonnistumisien vakavuus (Say & Vasudeva 2020). Näihin epäonnistumisiin luetaan tietoturvapoikkeamat. Vastatakseen näihin digitaalisten toimintaympäristöjen turvallisuuteen liittyviin haasteisiin organisaatioilla tulee olla kehittynyt tietoturvakulttuuri.

Organisaatioissa yleisesti työntekijät ovat merkittävimpiä tietoturvaloukkausten mahdollistajia. Ideaalitasolle kehittynyt tietoturvakulttuuri auttaakin minimoimaan juuri ihmisistä johtuvia tietoturvapoikkeamia. (da Veiga et al. 2020) Toisin sanoen kehittämällä tietoturvakulttuuria voidaan vaikuttaa erääseen tämän hetken merkittävimmistä tietoturvaongelmien lähteistä, mikä korostaa tietoturvakulttuurin tutkimisen tärkeyttä.

Tietoturvakulttuuri on yksi organisaatiokulttuurin tasoista (Van Niekerk & Von Solms 2010). Koska kulttuurin kehittämisessä on kyse organisaatio-oppimisesta, tietoturvakulttuurin kehittämistä on mielekästä lähestyä organisaation oppimisen ja uudistumisen periaatteiden näkökulmasta. Eräs organisaation oppimisen ja uudistumisen työkalu on suorituspalaute, jonka avulla tarkastellaan organisaation suoriutumista johdon määrittelemään tavoitetasoon nähden tietyllä mittarilla (Greve 2003; Kotiloglu et al. 2021; Ye et al. 2021). Suorituspalautteella pyritään siis määrittelemään, voidaanko tarkasteltua toimintaa pitää onnistuneena suhteessa tavoitteisiin.

Suorituspalaute nähdään tyypillisesti sosiaalisena tai historiaan perustuvana sen tavoitetason määrittelytavan mukaan. Sosiaalisessa suorituspalautteessa on kyse vertaisorganisaatioiden, kuten kilpailijayritysten, vastaavan toiminnan tarkasteluun perustuvasta suoritusten arvioinnista. Tällöin toiminnan tavoitetaso määrätään näiden arviointien perusteella. Historiaan perustuvassa suorituspalautteessa puolestaan tarkastellaan orga-

nisaation aikaisempaa suoriutumista tarkasteltavalla toiminnan alueella, jonka perusteella toiminnan tavoitetaso määritellään. (Kotiloglu et al. 2021) Tämän tutkimuksen tapauksessa tarkasteltavalla toiminnalla tarkoitetaan tietoturvallisuutta ja tietoturvakulttuuria.

Suorituspalautteella on aikaisempien tutkimuksien perusteella nähtävissä yhteys tietoturvakulttuurin kehittämiselle. Sayn ja Vasudevan (2020) tekemän tutkimuksen mukaan organisaatiossa realisoituneisiin tietomurtoihin liittyvä suorituspalaute voi vaikuttaa organisaation suhtautumiseen tietomurtoja kohtaan positiivisesti. Tämä on tutkimuksen kannalta merkittävää, koska tietomurtoihin suhtautumista voidaan pitää osana tietoturvakulttuuria. Kyseisessä tutkimuksessa tuodaan ilmi tarve suorituspalautteen merkityksen tutkimiselle tietoturvan näkökulmasta pelkkiä tietomurtoja laajemmin (Say & Vasudeva 2020).

1.2 Tutkimusongelma, tutkimuksen rajaaminen ja tavoite

Kotiloglun et al. (2021) tutkimuksessa on havaittu tarve lisätutkimukselle koskien organisaation strategisten päätösten suhdetta suorituspalautteeseen sen eri toiminnan osa-alueilla. Da Veigan et al. (2020) mukaan tietoturvakulttuurin kehittämisen tutkimiselle on tarvetta, koska tietoturvapoikkeamien nähdään edelleen olevan useimmiten ihmisistä johtuvia. Tietoturvakulttuurissa onkin kyse juuri organisaatioon kuuluvien ihmisten tietoturvallista toimintaa ohjaavista tekijöistä (da Veiga et al. 2020). Lisäksi tietoturvakulttuurin arviointiin ja kehittämiseen kohdistuvien työkalujen suuri merkitys on havaittu jo varhain (Kraemer & Carayon 2005). Tutkimusongelma on siis suorituspalautteen lisätutkimuksen tarve eri toiminnan osa-alueilla, yhdistettynä tietoturvakulttuurin ja sen tason arvioinnin kehittämisen tarpeeseen.

Tutkimuksessa keskitytään käsitteiden tietoturvakulttuuri ja suorituspalaute yhteensovittamiseen. Näitä käsitteitä poikkitieteellisesti tarkastelevia tutkimuksia ei toistaiseksi ole kovinkaan useaa. Kandidaatintutkielman päätutkimuskysymys onkin ”Mikä on suorituspalautteen rooli organisaatioiden tietoturvakulttuurin kehittämisessä?”. Alla on esitetty pääkysymykseen vastaamisen avuksi muotoiltuja alakysymyksiä:

- Voiko tietoturvakulttuurista kerätä suorituspalautetta? Minkälaista?
- Miten tietoturvakulttuuria mitataan?
- Miten tietoturvakulttuurin tavoitetaso määritellään?
- Miten suorituspalautteen avulla voidaan uudistaa organisaatiota?

Tutkimus rajataan käsittelemään organisaatioiden tietoturvallisuuden kehittämistä ihmiskeskeisesti paneutuen tietoturvakulttuuriin. Spesifit teknologiset ratkaisut rajataan tutkimuksesta pois. Suorituspalautetta puolestaan käsitellään Greven (2003) suorituspalauteteorian kautta. Sekä historiaan perustuva että sosiaalinen suorituspalaute ovat tutkimuksen kannalta tärkeässä roolissa. Koska tutkimuksella pyritään edistämään tietoturvakulttuurin kehittämistä ja tätä kautta organisaatio-oppimista, suorituspalautetta tarkastellaan organisaatio-oppimisen näkökulmasta. Suorituspalautteen riippuvuudet esimerkiksi kansalliseen kulttuuriin rajataan puolestaan pois, jotta tutkimuksen laajuus pysyisi sopivana.

Tutkimuksen tavoite on selvittää, voiko suorituspalautteen teoriaa soveltaa tietoturvakulttuurin kehittämiseen, ja jos voi niin miten. Tutkimuksen arvo kohdistuu tietoturvallisuuden sekä yleisen organisaatio-oppimisen tutkimisen edistämiseen. Koska tietoturvakulttuuria kehittämällä organisaatiot voivat vähentää henkilöstöstä johtuvia tietoturvauhkia (da Veiga et al. 2020), tutkimuksella voidaan saavuttaa myös yhteiskunnallista arvoa.

1.3 Työn rakenne

Tutkimuksen ensimmäinen luku on johdanto, jonka tarkoituksena on taustoittaa aihetta, perustella valittu tutkimusongelma sekä esitellä tutkimuskysymykset ja työn tavoitteet. Toinen luku esittelee käytettyä tutkimusmenetelmää sekä -aineistoa. Siinä pyritään tuomaan tutkimusprosessi mahdollisimman läpinäkyvästi ilmi, jotta se olisi toistettavissa. Lisäksi luvussa analysoidaan kerättyä tutkimusaineistoa.

Kolmas ja neljäs luku ovat teorialukuja. Kolmannessa luvussa tuodaan esille työn kannalta tärkein suorituspalautteen teoria ja muodostetaan sen perusteella viitekehys, jota käytetään luvun viisi rakenteen pohjana. Luku neljä esittelee puolestaan tietoturvakulttuuriin liittyvää teoriaa. Viides luku esittelee tutkimuksen tulokset. Siinä kootaan yhteen tietoturvakulttuurin teoria ja suorituspalauteteoria sekä arvioidaan niiden yhteensopivuutta tutkimusaineiston perusteella.

Kuudes luku on yhteenveto, jossa analysoidaan kirjallisuuskatsauksen löydöksiä ja tehdään niistä päätelmiä pyrkimyksenä tutkimuskysymyksiin vastaaminen. Luvussa arvioidaan myös tutkimuksen rajoitteita, jatkokehitysmahdollisuuksia sekä tutkimuksen toteuttamista.

2. TUTKIMUSMENETELMÄT JA -AINEISTO

Tässä luvussa kuvataan käytetyt tutkimusmenetelmät. Tarkoituksena on dokumentoida tutkimuksen toteutuksen yksityiskohdat siten, että tutkimus voitaisiin tarvittaessa toistaa. Lisäksi luvussa esitellään oleellisin aineisto ja siihen johtaneet valinnat. Lopuksi aineistoa vielä analysoidaan ja kuvataan, mitä siitä etsitään.

Kandidaatin tutkimus toteutetaan kirjallisuuskatsauksena ja sen perustana on Finkin (2014) seitsemän kohdan malli. Malli on seitsemänvaiheinen prosessi, joka koostuu seuraavista osuuksista:

1. Tutkimuskysymyksen asetus
2. Kirjallisuuden ja tietokantojen valinta
3. Hakusanojen ja -lauseiden valinta
4. Käytännön hakukriteerien valinta
5. Metodologinen rajaus
6. Katsauksen tekeminen
7. Tulosten syntetisointi (Fink 2014).

2.1 Tutkimusaineiston haku ja valinta

Tutkimusaineiston hakuun käytettävät tietokannat ovat Scopus, Google Scholar sekä Tampereen yliopiston Andor-hakupalvelu. Hakulauseet muodostetaan Boolen operaattoreilla: AND, OR ja NOT. Taulukossa 1 esitetään tärkeiden käytettävien hakulauseiden tulokset tietokannoittain rajoittamattomina.

Taulukko 1: Hakutuloksien määrät rajoittamattomassa haussa

Haku	Andor	Google Scholar	Scopus	Yhteensä
("information security" OR "cyber security" OR "data security") AND "performance feedback"	8	1 780	74	1 862
risk management AND "performance feedback" NOT "risk taking"	36	901	64	1 001
"Organisation culture" AND "performance feedback"	51	486	70	607
				3 470

Taulukon 1 ensimmäisellä hakulauseella pyritään etsimään tietoturvallisuutta, kyberturvallisuutta tai data turvallisuutta sekä suorituspalautetta poikkitieteellisesti käsittelevää aineistoa. Toisella haulla puolestaan yleisemmin suorituspalautteen merkitystä riskien hallinnassa. Tässä haussa ”risk taking” suljetaan hakujen ulkopuolelle. Tämä ratkaisu nähtiin järkeväksi, koska tämä käsite johtaa suureen määrään aiheeseen liittymättömiä

hakutuloksia. Nämä tulokset liittyvät pääasiassa tarkoituksenmukaiseen riskinottoon esimerkiksi investointipäätösten kontekstissa. Viimeisellä haulla pyritään etsimään aineistoa, joka käsittelee organisaatiokulttuurin kehittämistä suorituspalautteen avulla.

Taulukosta 1 huomataan, että rajoittamattomassa haussa hakutulosten määrät vaihtelevat huomattavasti riippuen tietokannasta. Rajoittamattoman haun tulosten yhteislukumäärä on kuitenkin liian suuri käsittelyyn. Rajataan seuraavaksi haut tieteellisiin artikkeleihin ja konferenssijulkaisuihin. Koska aineistoa ei juurikaan löydy suomeksi, rajataan kieleksi englanti. Jotta aineistoa voitaisiin pitää yhä relevantteina, rajataan hakutulokset aikavälille 2015─2023. Nämä kriteerit lisäämällä saadaan tietokannoista taulukon 2 mukainen määrä hakutuloksia.

Taulukko 2: Hakutuloksien määrät perusrajauksin

Haku	Andor	Google Scholar	Scopus	Yhteensä
("information security" OR "cyber security" OR "data security") AND "performance feedback"	2	86	51	139
risk management AND "performance feedback" NOT "risk taking"	7	51	42	100
"Organisation culture" AND "performance feedback"	8	13	31	52
				291

Lisätään tähän vielä tietokantakohtaisesti aihealuetta ja avainsanoja koskevat rajaukset. Tällaisia rajauksia ei voida tehdä Google Scholarissa, mutta Andor ja Scopus mahdollistavat ne. Aiheeseen liittyviä avainsanoja ovat muun muassa seuraavat:

- Behavioral Theory of the Firm
- Computer Science
- Decision Making
- Feedback
- Security
- Social Sciences
- Organization culture
- Learning
- Risk Management
- Information management.

Näin saadaan rajattua hakutulokset vielä taulukon 3 mukaiseen muotoon.

Taulukko 3: Hakutulosten määrät

Haku	Andor	Google Scholar	Scopus	Yhteensä
("information security" OR "cyber security" OR "data security") AND "performance feedback"	2	86	14	102
risk management AND "performance feedback" NOT "risk taking"	6	51	8	65
"Organisation culture" AND "performance feedback"	6	13	5	24
				191

Yhä edellä mainittujen rajausten jälkeenkin hakutuloksissa oli aiheeseen liittymättömiä artikkeleita. Hakutuloksissa esiintyi myös päällekkäisiä tuloksia eri tietokantojen välillä. Kuitenkin tulosten perusteella voitiin tehdä jo vallitsevilla rajauksilla läpikäyvää aineistojen seulomista, ja muodostaa tutkimuksen aineisto. Taulukossa 3 esitetystä aineistosta karsittiin tutkimuksen kannalta mielenkiintoiset aineistot otsikoiden ja tarvittaessa tiivistelmän perusteella.

2.2 Lopullinen aineisto

Taulukoissa esitetyillä hauilla saatiin kerättyä suurin osa tutkimuksessa käytetystä aineistosta. Aineistoa löytyi kuitenkin myös hakujen ulkopuolelta. Hyödyllistä aineistoa saatiin kerättyä esitettyjen hakujen lisäksi muiden aineistojen viitetiedoista sekä lähteistä. Lisäksi muutama teos valikoitui käytettyyn aineistoon hyödyntäen Tampereen yliopiston opintojaksojen ”Kyberturvallisuus 1: perusteet” sekä ”Organisaation oppiminen ja uudistuminen” vastuuopettajien aineistovinkkauksia. Myös näiden teosten relevanttiutta arvioitiin aiemmin esitetyin kriteerein.

Tutkimusaineistosta Greven (2003) kirja poikkeaa muusta aineistosta, sillä se on verrattain muuhun aineistoon kohtalaisen vanha teos, jota kuitenkin käytetään suorituspalauteteorian osalta tärkeänä lähteenä. Lisäksi se on ainoa tutkimusaineistoon kuuluva kirja. Sen käyttäminen melko laajasti etenkin suorituspalauteteorian avaamisessa katsottiin kuitenkin perustelluksi, sillä kyseinen teos on suorituspalauteteorian pohjateoksia Cyertin ja Marchin (1963) *a Befavioral Theory of the Firm* -teoksen ohella. Suurimmassa osassa tutkimuksen aineiston vertaisarvioituja suorituspalauteteoriaa koskevia artikkeleita, Greven teos on teoriaosuuksien tärkeä lähdeaineisto. Näin ollen Greven teoksen liittäminen tutkimusaineistoon nähdään alkuperäisteoksen kunnioittamisen nimissä oikeutetuksi. Teoksen tueksi on kuitenkin nostettu myös uusia artikkeleita, ja sen sisällön sopivuutta nykyaikaan arvioidaan.

Näin tutkimusaineistoon saatiin muodostettua 20 teosta. Aineiston tutkimukset ovat suurilta osin kvalitatiivisia ja empiirisiä. Osa aineistosta käsittelee suoraan suorituspalautteen ja tietoturvakulttuurin yhtymäkohtia. Näissä aineistossa koko teksti on tarkan keskittymisen kohteena. Suurin osa kuitenkin käsittelee suorituspalautteen tai tietoturvakulttuurin teoriaa erikseen. Näissä aineiston artikkeleissa huomio on tietoturvakulttuurin kehittämistä ja suorituspalauteteoriaa yhdistävissä seikoissa. Lisäksi keskitytään asioihin, jotka mahdollisesti argumentoivat suorituspalauteteorian ja tietoturvakulttuurin kehittämisen yhdistämistä vastaan. Näin tutkimus pyritään pitämään mahdollisimman objektiivisena.

3. SUORITUSPALAUTE

Tässä osiossa selvennetään suorituspalautetta käsitteellisesti ja avataan siihen liittyvää taustatietoa. Tekstiosiossa käsitellään suorituspalautetta organisaation oppimisen prosessina.

3.1 Suorituspalauteteoria

Suorituspalaute ja sen rooli organisaatio-oppimisessa perustuu Cyertin ja Marchin (1963) *Befavioral Theory of the Firm* -teoriaan (BTOF) ja siitä edelleen kehitettyyn suorituspalauteteoriaan (engl. Performance Feedback Theory) (Cyert & March 1963; Greve 2003; Kotiloglu et al. 2021). Suorituspalauteteoria selittää organisaation oppimisen ja strategisten päätösten yhteyttä (Ahn et al. 2021).

Suorituspalauteteorian ja BTOF:n mukaan organisaation toimintaa voidaan tarkastella suorituskyvyn mittaamisella tietyllä toiminnan osa-alueella. Tämän jälkeen mitattua suoritusta verrataan johdon määrittelemään tavoitetasoon (engl. aspiration level), jolloin saadaan suorituspalautetta. (Cyert & March 1963; Greve 2003 s. 1─9; Kotiloglu et al. 2021) Suorituspalauteteoria pitää suorituspalautetta oppimisen ja käyttäytymisen muutoksen ”avainmekanismina”, ja se voi näyttäytyä kokemuksista tai vertaisilta oppimisena (Greve 2003).

Tavoitteiden ja toteutuneen suoritustason suhdetta analysoimalla organisaation päätöksentekijät voivat havaita mahdollisia kehityskohtia organisaation toiminnassa. Suorituspalauteen vaikutus strategisten muutosten intensiteettiin riippuu organisaatiosta, tavoitetason määrittelytavasta sekä tarkasteltavasta toiminnan alueesta (Kotiloglu et al. 2021).

3.2 Tavoitetason määrittely

Toiminnan tavoitteet ovat suorituspalauteteorian lähtökohta (Greve 2003; Ye et al. 2021). Tavoitetason määrittelyn voidaan nähdä olevan suorituspalautteen arvioinnin edellytys, sillä erotus sen ja toteutuneen suoriutumisen välillä kuvaa organisaation onnistumista valitulla mittarilla. Tavoitetasoa kuvataankin pienimmäksi suoriutumisen tasoksi, jolla tarkastellun toiminnan voidaan katsoa olevan onnistunutta (Kotiloglu et al. 2021). Lienee selvää, että määritellyn tavoitetason tulisi olla mahdollisimman totuuden mukainen ja tarkka, sillä puutteellisesti määriteltynä se haittaisi onnistumisen arviointia.

Tämä voisi johtaa toiminnanmuutoksiin väärillä hetkillä tai tavoilla. Liian korkealle asetettu tavoitetaso voi johtaa tarpeettomaan resurssien käyttöön, kun taas sen liian matalalle asettaminen voi aiheuttaa organisaation vastatoimien vajavaisuutta.

Joissakin konteksteissa tavoitteiden määrittely voidaan toteuttaa verrattain vähäisillä resurssipanostuksilla. Tämä pätee, jos mitattavalle toiminnalle voidaan asettaa niin sanottu luonnollinen tavoitetaso. Tällaiselle tavoitetasolle on tyypillistä stabiilius sekä usean toisistaan riippumattoman päätöksentekijän samanmielisyys sen oikeellisuudesta. Luonnollinen tavoitetaso kuvaa usein nykytilaa tai niin sanottua ”nollatasoa”. (Greve 2003, s. 40─41) Tietoturvakontekstissa nollataso voisi tarkoittaa esimerkiksi nollaa tietoturvaloukkausta tietyllä aikavälillä. Mikäli päätöksentekijät käyttävät tavoitetasona nollatasoa, on oleellista tarkastella tavoitetason realistisuutta.

Yleisesti tavoitetaso tulisi kuitenkin määritellä organisaation sisäisen historian tai vertaisorganisaatioiden tietojen perusteella (Choi et al. 2019; Kotiloglu et al. 2021; Ye et al. 2021). Näitä tavoitetason yleisimpiä määrittelytapoja kutsutaan historiaan perustuvaksi (engl. Historical aspiration level) ja sosiaaliseksi (engl. Sosial aspiration level*)* tavoitetasoksi (Greve 2003; Kotiloglu et al. 2021; Ye et al. 2021). Nämä tavoitetason määrittelyperusteet voivat olla käytännössä työläämpiä, kuin luonnollisen tavoitetason käyttö. Niiden käyttö voi kuitenkin johtaa organisaatio-oppimisen kannalta tehokkaampiin tavoitetasoihin (Greve 2003, s. 40). Lisäksi kaikelle toiminnalle ei voida katsoa liittyvän luonnollista tavoitetasoa, vaan se on kontekstiriippuvaista.

Historiaan pohjautuvassa tavoitetason määrittelyssä organisaation päätöksentekijät arvioivat toiminnan tavoitetasoa sisäisesti tuotetun tiedon perusteella. Sen vahvuus on oman toiminnan hyvässä ennustettavuudessa, mutta sitä käyttämällä organisaation ulkoisten tekijöiden huomioiminen on usein tehottomampaa. Sisäisesti tuotettu tieto on myös helpompi ymmärtää organisaation sisällä. (Greve 2003, s. 42─43; Kotiloglu et al. 2021) Historiaan perustuva tavoitetaso on siis oletettavasti hyödyllinen toiminnassa, jossa ulkoisten tekijöiden vaikutus on pieni ja suoritustaso perustuu suurimmilta osin organisaation sisäisiin toimintatapoihin ja käytäntöihin. Koska historiaan pohjautuva tavoitetaso perustuu organisaation sisäisiin tietolähteisiin, on tiedon saaminen usein melko vaivatonta ja pieni kustanteista. Jos tarkasteltava muuttuja on organisaation johdolle kiinnostava, siitä luultavasti myös kerätään dataa (Greve 2003, s. 42). On kuitenkin syytä ottaa huomioon, että organisaation sisäisistä tietolähteistäkin relevantin tiedon löytäminen voi olla resursseja kuluttavaa, sillä dataa kerätään monissa organisaatioissa huomattavan paljon. Väitettä voidaan myös kyseenalaistaa, sillä organisaatioiden toimintaympäristöt muuttuvat. Näin ollen on mielekästä ajatella myös tärkeiden mittauskohteiden mahdollisesti muuttuvan.

Sosiaalinen tavoitetason määrittely tarkoittaa puolestaan vertaisorganisaatioiden käyttämistä tavoitetason määrittelyn tietolähteinä. Etuna sosiaalisessa tavoitetason määrittelyssä on ulkopuolisten tekijöiden vahva huomioiminen. Kerätty tieto tulisi kuitenkin sovittaa myös oman organisaation kontekstiin ja huomioida vertaisorganisaatioiden erilaisuus, jotta tietoa voitaisiin soveltaa oman tavoitetason määrittelyyn. (Greve 2003, s. 45─48; Ye et al. 2021) Tästä syystä oleellista onkin onnistunut vertailuryhmän valinta. Vertailuryhmän samankaltaisuus oman organisaation kanssa helpottaa tietojen soveltamista omaan organisaatioon (Greve 2003, s. 45). Sosiaalisesta tavoitetason määrittelystä tekee haastavaa myös tietojen saatavuuden vaikeus. Tiedot eivät välttämättä ole vapaasti saatavilla, ja niiden hankinta voi olla kallista (Greve 2003, s. 45─46).

Historiaan perustuvalla ja sosiaalisella suorituspalautteella on tyypillisesti erilaisia vaikutuksia organisaatio-oppimiseen. Merkittävä ero liittyy tarkasteltavan toiminnan pysyvyyteen ja vertailukelpoisuuteen. (Ye et al. 2021) Toisin sanoen sosiaalista tavoitteiden määrittelyä suositellaan todennäköisemmin muuttuvissa toimintaympäristöissä. Historiaan perustuvaa sen sijaan vahvasti organisaatiosidonnaisissa seikoissa.

Tavoitetasolähteet on havaittu todennäköisesti hyödyllisemmäksi erottaa, kuin käyttää sosiaalisia ja historiaperusteisia lähteitä sekaisin (Choi et al. 2019). Mikäli yhdistettyä tavoitetasoa käytetään, on sen syytä painottaa historiaan perustuvia tai sosiaalisia tavoitteita. Kuitenkin keskittymällä vain toiseen määrittelytapaan saavutetaan usein suurempia vaikutuksia organisaatiolle. (Kotiloglu et al. 2021) Kuten mainittu sosiaaliset ja historiaperusteiset tavoitelähteet sopivat erilaisiin tilanteisiin, joten väite on uskottava. Painotettava tavoitetasolähde on usein riippuvainen tarkasteltavaan toiminnan tasoon (Kotiloglu et al. 2021). Luvussa 5 paneudutaan tietoturvakulttuuriin soveltuvaan tapaan määritellä tavoitetaso.

3.3 Suorituspalautteesta organisaation oppimiseen ja uudistumiseen

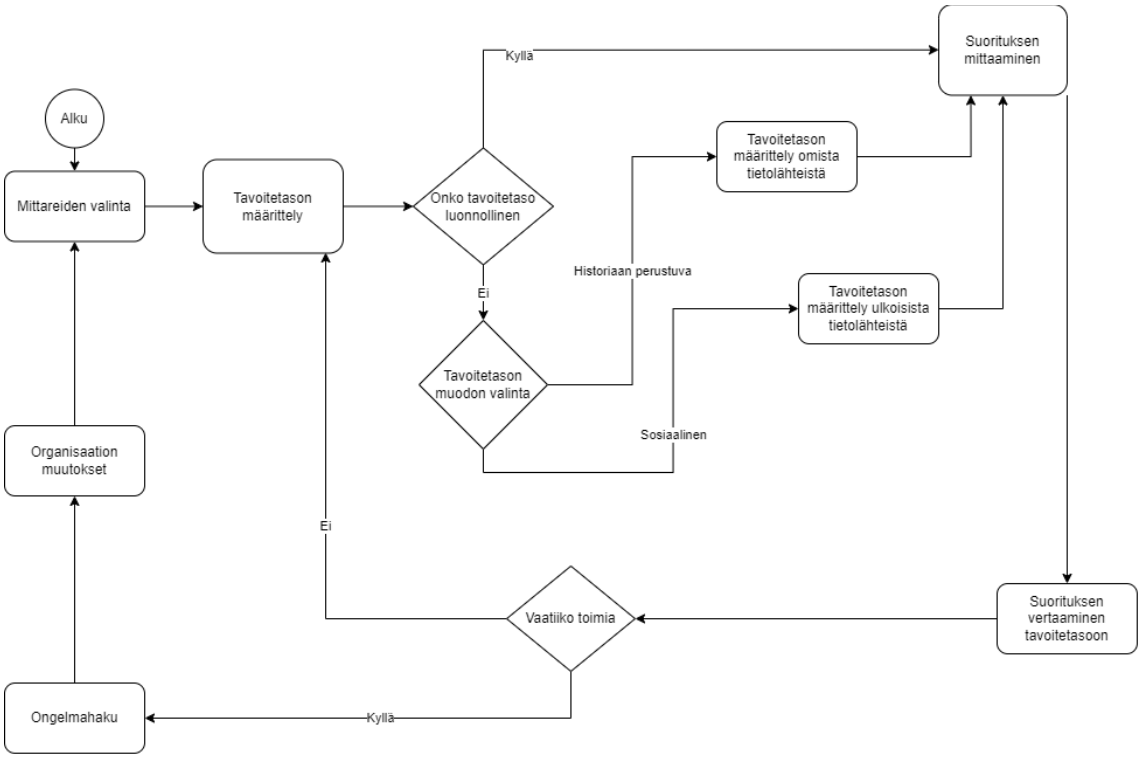
Kuten ensimmäisessä luvussa mainitaan, suorituspalaute voidaan nähdä organisaation oppimisen ja uudistumisen työkaluna. Yleisesti on havaittu suorituspalautteen laukaisevan eniten strategisia toimia organisaatioissa, kun organisaation koetaan alisuoriutuvan (Kotiloglu et al. 2021). Tämä tarkoittaa, että organisaatioiden päätöksentekijät pyrkivät kehittämään toimintaa intensiivisemmin, kun suoritustaso on tavoitetason alapuolella. Pelkkä negatiivinen suorituspalaute ei yksinään aikaansaa muutosta, vaan se pikemminkin viestii päätöksentekijöille muutoksen tarpeesta. Myös organisaation päätöksentekijöiden psykologisella suhtautumisella tavoitetasoon on suuri vaikutus muutosjohtamisen

intensiteettiin (Choi et al. 2019; Ahn et al. 2021). Käytännössä siis on lopulta päätöksentekijöistä kiinni, ajetaanko suorituspalautteen perusteella muutoksia, ja minkä suuntaisia ne ovat.

Organisaatio oppii harvoin suoraan suorituspalautteesta. Suorituspalautteesta voidaan kuitenkin havaita tarve oppia ja kehittyä, jolloin tavallisesti suorituspalaute laukaisee niin sanottuja ongelmahakuja (engl. Problemistic search), joilla etsitään aktiivisesti potentiaalisia uusia toimintatapoja, kun suoritus on todettu tavoitteita huonommaksi (Choi et al. 2019). Ongelmahaut ovat tavoitekeskeisiä vastausyrityksiä havaittuihin ongelmiin, joita pidetään merkittävimpänä keinona aikaansaada organisaatio-oppimista suorituspalautteesta (Greve 2003, s. 55─56). Ongelmahakuja voidaan suorittaa esimerkiksi investoimalla toimintaympäristön tutkimiseen (Choi et al. 2019). Niillä on osoitettu saavutettavan pidemmän ajanjakson strategisia muutoksia (Kotiloglu et al. 2021).

3.4 Suorituspalautteen viitekehys

Kuva 1 havainnollistaa tässä luvussa opitut seikat. Kuva pohjautuu suorituspalauteteoriaan ja havainnollistaa prosessia tavoitetason määrittelystä varsinaiseen organisaatio-oppimiseen. Sitä käytetään viitekehyksenä suorituspalauteteoriaa ja tietoturvakulttuuria yhdistelevässä osiossa (Luku 5).



Kuva 1: Organisaatio-oppiminen suorituspalautteen avulla

Kuvan 1 prosessissa alkupisteeksi on esitetty mittareiden valinta, sillä ennen tavoitteiden määrittelyä tai suoritusmittauksia on valittava millä mittarilla toimintaa tarkkaillaan. Tämä lienee selvää, sillä tavoitteiden ja suoritusmittausten on oltava vertailukelpoisia, koska suorituspalaute perustuu niiden suhteeseen. Kuvassa nuolet ilmaisevat toiminnan kulun suuntaa ja vinoneliöt prosessin vaiheita, joissa prosessin kulku voi vaihdella tilanteen mukaan. Pyöristetyt laatikot puolestaan kuvaavat eri prosessin vaiheita. Kuva on määritelty itseään toistavaksi. Tämä on mielekästä, sillä mikäli organisaatio oppii suorituspalautteesta, voi ilmetä tarve määritellä esimerkiksi tavoitteet uudella tavalla tai käyttää erilaisia mittareita. Viitekehyksen ei ole tarkoitus tuoda varsinaisesti mitään uutta suorituspalauteteoriaan, vaan havainnollistaa sitä visuaalisesti ja auttaa teoreettisessa yhteensovittamisessa tietoturvakulttuurin kehittämiseen.

4. TIETOTURVAKULTTUURI

Tässä osiossa selvennetään tietoturvakulttuurin käsitettä ja siihen liittyvää teoriaa. Tekstissä pohditaan tietoturvakulttuurin tekijöitä. Lisäksi osion viimeisessä kappaleessa käsitellään tietoturvakulttuurin mittaamista.

4.1 Tietoturvakulttuurin käsite ja sen tekijät

Organisaation tietoturvakulttuurilla tarkoitetaan sen tietoturvaympäristön inhimillisiä näkökulmia. Usean lähteen mukaan tietoturvakulttuurin keskiössä ovatkin organisaation työntekijät, sekä heidän tietämyksensä, normit, arvot, asenteet ja käyttäytyminen liittyen tietoturvallisuuteen. (da Veiga & Eloff 2010; Van Niekerk & Von Solms 2010; da Veiga et al. 2020; Orehek & Petrič 2021)

Tietoturvakulttuuri siis ohjaa organisaation yksilöitä tietoturvakäytäntöjen noudattamisessa tai noudattamatta jättämisessä. Heikko tietoturvakulttuuri vaarantaakin koko organisaation turvallisuuden (Orehek & Petrič 2021). Alhaisella tasolla oleva tietoturvakulttuuri voi vaarantaa oman organisaation tietojen lisäksi sidosryhmien ja asiakkaiden tietojen turvallisuuden.

Vaikka tietoturvakulttuurin käsitteeseen yleisesti mielletään edellisessä tekstikappaleessa mainitut työntekijöiden tietoturvallisuuteen liittyvät tekijät, ei tietoturvakulttuurin tarkasta käsitteestä ole täyttä yksimielisyyttä. Tämä johtuu siitä, ettei tietoturvakulttuurin eri osatekijöistä ja dimensioista ole yksiselitteisesti hyväksyttyä määritelmää (Nasir et al. 2019).

Da Veiga et al. (2020) määrittelevät tietoturvakulttuuriin vaikuttavien seikkojen koostuvan sisäisistä ja ulkoisista tekijöistä. Henkilöstö on osa sisäisiä tekijöitä, mutta niihin luetaan myös organisaation johtaminen sekä luottamus johdon, työntekijöiden ja asiakkaiden välillä. Lisäksi sisäisiin tekijöihin luetaan organisaatiolliset tekijät, kuten resurssit, elinkaaren vaihe ja yleinen organisaatiokulttuuri. Ulkoisiin ympäristötekijöihin lukeutuu puolestaan muun muassa lainsäädännölliset seikat, kansallinen kulttuuri ja teknologiset tekijät. (da Veiga et al. 2020) Kaiken kaikkiaan edellä mainitun näkemyksen perusteella tietoturvakulttuuriin voidaan nähdä vaikuttavan hyvin laajasti erilaiset seikat.

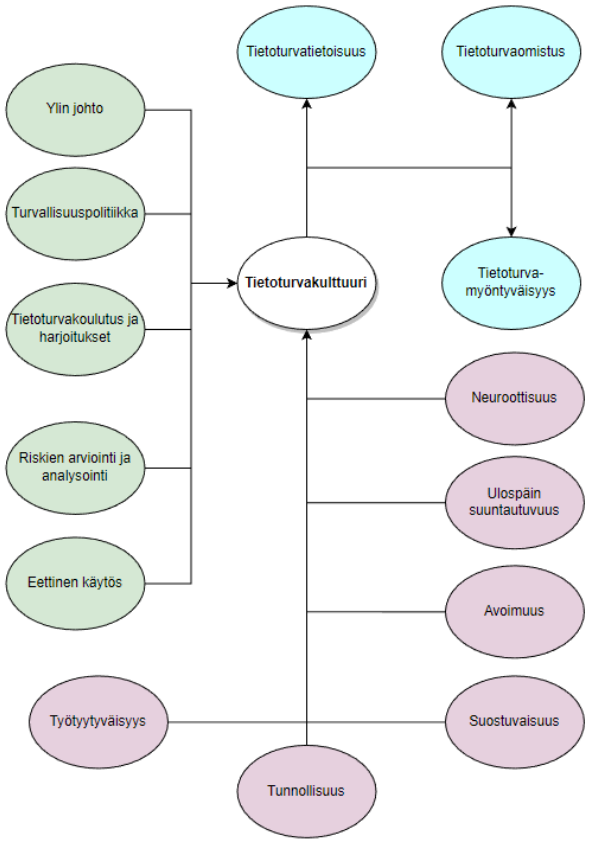
4.2 Tietoturvakulttuurin tason mittaaminen organisaatiossa

Tietoturvakulttuurin tasoa on tärkeää mitata säännöllisesti, jotta työntekijöiden turvallisuuskäyttäytymisestä saadaan palautetta ja voidaan tunnistaa mahdollisia kehityskohtia

(Orehek & Petrič 2021). Tämä viestii siitä, että tietoturvakulttuurista tulisi kerätä suoritus-palautetta. Euroopan unioniin kuuluvissa maissa tietoturvakulttuurin tason mittaaminen on pakollista (ENISA 2017; Orehek & Petrič 2021). Kuten edellisessä kappaleessa mainittiin, tietoturvakulttuuriin voi vaikuttaa myös ulkoiset tekijät, joina EU:n lainsäädöllisiä seikkoja voidaan pitää.

Koska tietoturvakulttuuri on inhimillisiin tekijöihin perustuva, sitä mitataan usein empiirisin metodein, kuten henkilöstökyselyin. Tämänkaltaisissa tutkimuksissa on oleellista minimoida subjektiivisuus. (Orehek & Petrič 2021) Toisin sanoen mittaus tulisi järjestää niin, että vastaukset olisivat mahdollisimman puolueettomia ja totuudenmukaisia. Niiden tulisi kuvata tietoturvakulttuurin todellista tasoa. Orehekin & Petričin (2021) mukaan totuudenmukaisten ja kattavien tulosten saamiseksi on tärkeää, että kyselyihin vastaa koko henkilökunta. Lisäksi henkilökunnalle on tärkeää viestiä, ettei heille tule vastausten perusteella negatiivisia seuraamuksia (Orehek & Petrič 2021).

Tietoturvakulttuuria voidaan myös mitata erilaisien viitekehyksien avulla. Esimerkkinä voidaan käyttää Tolahin et al. (2021) esittelemää tietoturvakulttuurin avaintekijöiden viitekehystä (ISCFF), joka esitetään alla kuvassa 2.



Kuva 2: Tietoturvakulttuurin avaintekijöiden viitekehys (Tolah et al. 2021).

ISCFF-mallissa tietoturvakulttuuria katsotaan kuvaavan siihen vaikuttavat tekijät (engl. influencing factors; kuvassa 2 vihreällä), organisaation käyttäytymisen tekijät (engl. organisational behaviour factors; kuvassa 2 violetilla) sekä sen muodostavat tekijät (engl. constituting factors; kuvassa 2 sinisellä), joista viimeiset ovat tietoturvakulttuuria heijastavia tekijöitä ja ensimmäiset siihen vaikuttavia tekijöitä. Näitä tekijöitä mittaamalla voidaan kuvata organisaatioiden tietoturvakulttuuria. (Tolah et al. 2021) Malli on esimerkki tietoturvakulttuurin mittaamisesta ottamalla huomioon tietoturvakulttuuriin vaikuttavat dimensiot pelkkää henkilöstöä monipuolisemmin. On kuitenkin mainittava, että viitekehys on valittava organisaatiokohtaisesti (Nasir et al. 2019), ja ISCFF-malli on vain esimerkki vaihtoehtoisesta viitekehyksestä.

5. TIETOTURVAKULTTUURIN KEHITTÄMINEN SUORITUSPALAUTTEELLA

Tässä luvussa yhdistetään tutkimusaineiston avulla tietoturvakulttuurin kehittämisen teoriaa suorituspalauteteoriaan. Tekstiosiossa tuodaan ilmi tietoturvakulttuurin ja suorituspalautteen tutkimuksien yhtymäkohtia sekä käsitellään teorioita suoraan yhdisteleviä tutkimuksia. Luvun alaotsikoiden rakenne muodostetaan kuvan 1 viitekehyksen mukaisesti. Näin pyritään arvioimaan tietoturvakulttuurin yhteensopivuutta suorituspalauteteorian eri vaiheisiin.

5.1 Mittareiden valinta

Ennen tavoitteiden määrittelyä ja suorituksen mittausta niille on määriteltävä yhteiset mittarit. Kuten kappaleessa 3 mainittiin, Greven mukaan (2003, s. 42) organisaation suoriutumisen kannalta oleellista dataa luultavasti myös kerätään. Tämän voidaan katsoa pitävän ainakin osittain paikkansa tietoturvakulttuurin kontekstissa, koska sen mittaamista edellytetään jopa lainsäädännöllisesti Euroopan unionin alueella (ENISA 2017; Orehek & Petrič 2021). Tietoturvakulttuurin tasoa mitataan siis aktiivisesti ainakin EU:n jäsenvaltioiden organisaatioissa.

Mittaamisen pakollisuus ei kuitenkaan varmista sitä, että mittarit ovat totuudenmukaisia. Tietoturvakulttuurin kontekstissa haasteelliseksi voikin osoittautua sopivien mittareiden valinta ja mittaustavat. Ensinnäkin tietoturvakulttuurin eri dimensioista ei ole vielä tieteellistä yksimielisyyttä (Nasir et al. 2019). Toisekseen ideaalisen tietoturvakulttuurin on havaittu olevan riippuvainen organisaatiosta, kuten sen koosta, toimivaltiosta sekä yleisestä organisaatiokulttuurista (Nasir et al. 2019; Tolah et al. 2021). Näin ollen vaihtoehtoisia mittareita on useita. Kuten kappaleessa 4 mainittiin, yhteistä eri näkemyksille tietoturvakulttuurista on henkilöstön tietämyksen, normien, arvojen, asenteiden ja käyttäytymisen korostaminen, joten ainakin näitä tietoturvakulttuurin osatekijöitä olisi suositeltavaa mitata.

Eräänä lähtökohtana tietoturvakulttuurin mittaamiseen voidaan pitää luvussa 4 esitettyä ISCFF-mallia. Siinä avaintekijät ovat mitattavissa, ja Tolahin et al. (2021) mukaan niitä mittaamalla voidaan kuvata validisti tietoturvakulttuuria. Mittareiden toimivuutta on arvioitava säännöllisesti (Li et al. 2019).

5.2 Tavoitetason määrittely

Kappaleessa 3 opittiin, että suorituspalaute toimii organisaation oppimisen ja uudistumisen ajurina todennäköisimmin, kun suoritukset alittavat tavoitteet. Tietoturvallisuuden toiminnan arvioimiselle on tyypillistä piilevät ajanjaksot, jolloin uusia uhkia ei välttämättä ole havaittu (Li et al. 2019). Alati muuttuvassa tietoturvaympäristössä onkin päivitettävä jatkuvasti tavoitteita vaatimusten mukaan ja etsittävä uusia ongelmia (Say & Vasudeva 2020). Kappaleessa 3 todettiin sosiaalisen tavoitetason määrittelyn sopeutuvan muuttuvissa ympäristöissä toimimiseen. Näin ollen sosiaalisen tavoitteiden määrittelyn voidaan nähdä soveltuvan tietoturvakontekstiin.

Toisaalta ideaalin tietoturvakulttuurin määritelmä on riippuvainen organisaatiosta, kuten todettu edellä. Tämä osaltaan viestii historiaan perustuvan tavoitetason määrittelyn eduista tietoturvakulttuuria arvioitaessa, sillä aiemmin tekstissä opittiin sosiaalisen tavoitetason määrittelyn tuovan haasteita vahvasti organisaatiosta riippuvaisissa asioissa. Näin ollen voidaan todeta sosiaalisen tavoitetason määrittelyn vaativan tarkkaa sopivien vertaisorganisaatioiden valintaa. Mikäli päätetään määritellä tavoitteet historiaan perustuen, on puolestaan pidettävä aktiivisesti huolta, että toimintaympäristön muuttuvista vaatimuksista ollaan tietoisia.

On myös mahdollista käyttää historiaan perustuvan ja sosiaalisen tavoitetason yhdistelmää. On kuitenkin todettu, että tavoitetason määrittely on todennäköisesti tehokkaampaa, mikäli tapoja ei yhdistetä (Choi et al. 2019).

Realisoituneiden tietoturvapoikkeamien yksityiskohdat tulisi raportoida ja dokumentoida organisaatiossa riippumatta niiden vaikutusten suuruudesta (Bartnes et al. 2016). Realisoituneita tietoturvapoikkeamia voidaankin pitää oleellisena tietoturvakulttuuriin vaikuttavina suorituspalautteen muotoina. Tällöin voidaan soveltaa suorituspalauteteorian ”nollatason” eli luonnollisen tavoitetason käsitettä (Greve 2003, s. 40─41). Jos organisaatiossa realisoituu tietoturvapoikkeamia, edellytetään strategisia toimia ja virheistä oppimista. Näin ollen tietoturvakulttuurissa luonnollisena tavoitetasona voidaan pitää nollaa tietoturvapoikkeamaa. Kuten luvussa 3 mainittiin, ei nollatason käyttäminen kuitenkaan usein ole kaikista optimaalisin ratkaisu.

Vaikka edellä mainittujen tavoitetason määrittelytapojen voidaan nähdä olevan hyödyllisiä tietoturvakulttuurille, voidaan sosiaalinen suorituspalaute nähdä näistä tärkeimpänä ja eniten suositeltuna. Esimerkiksi arvioitaessa tietoturvauhkia kohtaan tehtyjen vastatoimien arvoa on sosiaalinen suorituspalaute nähty tehokkaimmaksi (Havakhor et al. 2018). Myös Porthouse et al. (2021) korostavat ulkopuolisen näkemyksen tärkeyttä arvioitaessa suuria ulkopuolisia riskejä. Näin ollen sosiaalista suorituspalautetta voidaan

pitää lähtökohtaisesti parhaana lähestymistapana tietoturvakulttuurin tavoitteita määriteltäessä.

5.3 Suorituksen mittaaminen

Kuten mainittu organisaatioiden on suositeltavaa, ja joskus myös pakollista, mitata tietoturvakulttuurin tasoa. Orehekin & Petričin (2021) mukaan tietoturvakulttuuria mitattaessa mittaustulosten validiteetti ja reliabiliteetti ovat kaikki kaikessa. Tietoturvakulttuurin dimensiot ovat yleensä kvalitatiivisia mittauksia, ja niitä toteutetaan usein esimerkiksi henkilöstökyselyin. Validin ja luotettavan mittaustuloksen saavuttaminen edellyttää mahdollisimman objektiivisia kysymyksen asetteluja. (Orehek & Petrič 2021) Mittausten tulisi siis aidosti kuvastaa arvioitavia tietoturvakulttuurin dimensioita.

Mittaukset koskevat tavallisesti tietoturvatietämystä ja -käyttäytymistä, mutta myös esimerkiksi arvoja, uskomuksia ja asenteita voidaan mitata (Orehek & Petrič 2021). Tämä voidaan nähdä oleelliseksi, sillä henkilöstön tietämyksen, normien, arvojen, asenteiden ja käyttäytymisen nähdään yleisesti kuvastavan tietoturvakulttuuria. Näin ollen niitä mittaamalla suorituspalautteesta saadaan todennäköisemmin totuudenmukaisempaa. Tietoturvakulttuuriin voidaan nähdä kuuluvan kuitenkin myös muita dimensioita (da Veiga et al. 2020). Dimensioita olisikin syytä myös mitata laajemmin (Tolah et al. 2021).

Jotta mittauksista saataisiin maksimaalista arvoa, niitä on toistettava säännöllisesti (Orehek & Petrič 2021). Tämä lienee ilmeistä tietoturvaympäristölle tyypillisen muuttuvan toimintaympäristön vuoksi. Tietoturvakontekstissa tulisi siis ottaa huomioon suorituspalauteprosessin iteroinnin tärkeys. Uusilla opeilla ympäristöstä voidaan oppia uusia vaatimuksia, jolloin myös tavoitteita on syytä päivittää.

5.4 Ongelmahaut

Kuten mainittu varsinaisia organisaation muutoksia ajetaan hauilla, joissa etsitään uusia tapoja toimia. Toisin sanoen on kyse suorituspalautteella havaittujen ongelmien analysoimisesta ja niistä oppimisesta. Hakuja voidaan tehdä esimerkiksi sidosryhmien kanssa kommunikoimalla, työtapojen kokeilullisella vaihtelulla, vaihtoehtoisten strategioiden puntaroinnilla ja konferenssikäynneillä (Greve 2003, s. 53─54).

Tietoturvaharjoitukset tuovat kokeilulliselle työtapojen vaihtelulle mahdollisuuksia tietoturvakontekstissa. Esimerkiksi pelillistäminen tuo tietoturvaturvaharjoituksiin uusia oppimisen mahdollisuuksia ja kokeilullisuutta (Mäses et al. 2022). Tietoturvaharjoitukset ja -koulutukset on tunnistettu tietoturvakulttuurin tärkeimmäksi positiiviseksi vaikuttajaksi ja ne lisäävät esimerkiksi tietoturvatietoisuutta (Tolah et al. 2021). Tämän perusteella niitä voidaan pitää tehokkaana ongelmahakuna etenkin, jos tietoturvatietoisuudessa havaitaan puutteita suorituspalautteessa. Myös vertaisorganisaatioiden ja muiden organisaation ulkopuolisten tahojen kanssa käyty dialogi on tietoturvakontekstissa tärkeä haun muoto, koska suurten riskien tapauksessa ulkopuolisen näkemyksen hyödyntäminen on tärkeää (Porthouse et al. 2021).

Koska erilaisia lähestymistapoja tietoturvakulttuurin on useita (Nasir et al. 2019), jotka sopivat eri organisaatioille, voidaan vaihtoehtoisten strategioiden punnitsemista pitää perusteltuna toimittaessa ali tavoitetason. Strategian vaihtona voidaan tässä tapauksessa pitää kokonaan uutta lähestymistapaa tietoturvakulttuuriin vaihtamalla esimerkiksi viitekehystä omaan organisaatioon mahdollisesti paremmin sopivaan.

5.5 Organisaation muutokset

Suorituspalautteen on havaittu aiheuttavan voimakkaimpia strategisia toimia tietoturvakulttuuriin erilaisten tietoturvariskien realisoituessa. Negatiivinen suorituspalaute liittyen korkean tason tietoturvariskien realisoitumiseen on johtanut monesti vastuuhenkilöiden erottamiseen (Say & Vasudeva 2021). Radikaalit ratkaisut, kuten vastuuhenkilöiden erottaminen voivat parantaa tietoturvakulttuuria, mutta niissä piilee myös riskejä. Epäonnistumisista oppiminen voi saada vastuuhenkilöt suhtautumaan tietoturvakulttuuriin vakavammin ja pienentää tehtyjen virheiden uusimisen todennäköisyyttä (Say & Vasudeva 2021). Toisin sanoen epäonnistumisten tuomat opit ilmenevät todennäköisesti vastuuhenkilöstön hiljaisena tietona, joka menetetään henkilöstövaihtamisilla. Tässä voidaan havaita yhteys kappaleen 3 opeille siitä, että suorituspalautteen avulla ei tehdä automaattisesti organisaatio-oppimisen kannalta hyviä päätöksiä. Suorituspalautteen tulkinta on lopulta päätöksentekijästä riippuvaista. Näin ollen päätöksentekijöiden vastuuta on syytä korostaa, kun suorituspalauteteoriaa sovelletaan tietoturvakontekstiin. Tämä tukee Choin et al. (2019) ja Ahnin et al. (2021) löydöksiä, joiden mukaan johtajien inhimilliset ominaisuudet vaikuttavat lopulta suorituspalautteen tulkintaan.

Monesti tietoturvakulttuuriin puututaan strategisin toimin tietoturvapoikkeamien näkyessä negatiivisesti organisaation taloudellisien mittarien kuten kannattavuuden suoritus-

palautteessa (Say & Vasudeva 2021). Näin ollen tietoturvakulttuurin tasoa mitataan organisaatiossa myös epäsuorasti esimerkiksi taloudellisten tunnuslukujen suorituspalautteella.

Säännöllisellä suorituspalautteella on havaittu positiivinen rooli henkilöstön työtyytyväisyyteen ja sitoutumiseen (Tagliabue et al. 2020), jotka ovat Tolahin et al. (2022) esittämiä tietoturvakulttuurin avaintekijöitä. Organisaatio-oppimisen kannalta onkin oleellista, että suorituspalaute välitetään henkilöstölle, ja että henkilöstö saa myös henkilökohtaista palautetta (Shah et al. 2019). Palautetta on siis suositeltavaa kerätä sekä organisaatio, että henkilöstötasolla.

Henkilöstölle tulisi välittää laadukkaasti sekä positiivinen, että negatiivinen suorituspalaute (Tagliabue et al. 2020). Aiemmin opittiin, että strategisia toimia ajaa voimakkaammin negatiivinen suorituspalaute. Positiivisella suorituspalautteella voidaan kuitenkin nähdä tietoturvakulttuuria ylläpitävä vaikutus, sillä positiivisella ja kannustavalla palautteella on havaittu tehokkaampi vaikutus esimerkiksi henkilöstön suhtautumiseen tietoturvapolitiikkaan (Balozian et al. 2019). Organisaatio-oppimisessa on kyse organisaation jäsenten kollektiivisesta oppimisesta. Näin ollen välittämällä tietoturvakulttuurin suorituspalautetta laadukkaasti kaikille organisaation jäsenille, voidaan saavuttaa organisaatiotason oppimista.

6. JOHTOPÄÄTÖKSET

Tässä luvussa kootaan yhteen toteutetun kirjallisuuskatsauksen löydökset. Lisäksi käsitellään tutkimuksessa ilmenneitä rajoitteita sekä tarpeita jatkotutkimuksille. Luvussa arvioidaan myös tutkimuksen tavoitteiden toteutumisen astetta ja vastataan alakysymysten kautta tutkimuskysymykseen.

6.1 Johtopäätökset ja löydökset

Organisaatioiden ja niiden toimintaympäristöjen digitalisoituessa tietoturvallisuus on yhä keskeisempi osa-alue riskien hallinnassa. Organisaatiot tarvitsevat paitsi tietoturvallista teknologiaa, myös turvallisen henkilöstön ja sitä kautta tasokkaan tietoturvakulttuurin, sillä valtaosa tietoturvapoikkeamista johtuu itse teknologioiden sijasta niitä käyttävistä ihmisistä. Tietoturvakulttuurin on yleisesti katsottu koostuvan organisaation henkilöstön tietoturvallisuuteen liittyvistä tiedoista, normeista, arvoista, asenteista ja käyttäytymisestä. Tietoturvakulttuuri on siis inhimillinen lähestymistapa tietoturvallisuudelle. Tietoturvakulttuurin mittaamisen, arvioinnin ja kehittämisen työkaluille ja viitekehyksille on havaittu tarve. Suorituspalauteteoria puolestaan tuo viitekehyksen organisaation suoritusmittausten analysointiin ja lopulta organisaatio-oppimiseen.

Päätutkimuskysymys oli: ”Mikä on suorituspalautteen rooli tietoturvakulttuurin kehittämisessä?”. Tässä osiossa vastataan kirjallisuuskatsauksen perusteella päätutkimuskysymykseen neljän alakysymyksen avulla, jotka on lueteltu alla.

- Voiko tietoturvakulttuurista kerätä suorituspalautetta? Minkälaista?
- Miten tietoturvakulttuuria mitataan?
- Miten tietoturvakulttuurin tavoitetaso määritellään?
- Miten suorituspalautteen avulla voidaan uudistaa organisaatiota?

Pohditaan ensin löydöksiä *suorituspalautteen keräämisestä* ja *tietoturvakulttuurin mittauksesta*. Suorituspalautteen kerääminen edellyttää, että tietoturvakulttuuri on mitattavissa ja sille voidaan asettaa tavoitteet samalla mittaristolla. Tietoturvakulttuurin tapauksessa mitattavina kohteina voivat olla esimerkiksi erilaiset mitattavat tietoturvakulttuurin dimensiot, kuten tietoturvatietoisuus, johdon sitoutuneisuus, tietoturvaomistus, organisaation tietoturvapolitiikka tai henkilöstön arvoihin ja käyttäytymiseen liittyvät kognitiiviset

ominaisuudet. Tietoturvakulttuurin dimensioista ei ole tieteellistä yksimielisyyttä. Sen sijaan erilaisten viitekehysten toimivuus on osoitettu tietyillä organisaatioilla. Organisaatioiden suositellaankin käyttävän yleiseen organisaatiokulttuuriinsa sopivaa tietoturvakulttuurin viitekehystä ja arvioivan sen toimivuutta.

Tutkimuksessa selvisi, että tietoturvakulttuuria on EU:n sisällä jopa pakollista seurata mittauksilla. Tietoturvakulttuuria suoraan mitattaessa erityisen tärkeää on validiteetiltaan ja reliabiliteetiltaan kuvaavien mittareiden löytäminen. Lisäksi on oleellista toistaa mittauksia säännöllisen usein. Tavallisin tapa suoralle tietoturvakulttuurin mittaukselle on empiirinen henkilöstökysely, jolla voidaan mitata esimerkiksi henkilöstön tietoja, arvoja ja asenteita liittyen tietoturvakulttuuriin.

Seuraavaksi keskitytään kolmanteen alakysymykseen, koskien *tavoitetason määrittelyä*. Mittaukset eivät yleensä luo itsenäisesti suurta arvoa organisaatioiden tietoturvakulttuurin kehittämiseksi, vaan niitä on voitava verrata suorituspalauteteorian mukaan tavoitetasoon. Tavoitetaso voidaan joskus määritellä luonnollisesti. Tietoturvakontekstissa luonnollinen tavoitteenmäärittely voisi sopia tietoturvapoikkeamien ”nollataso”, eli tavoite nollasta tietoturvapoikkeamasta. Tällöin tavoitteiden alittaminen eli yksikin realisoitunut poikkeama voisi laukaista ongelmahakuja poikkeamien juurisyiden selvittämiseksi. Tämän lähestymistavan ongelma on kuitenkin sen reaktiivinen luonne. Jos organisaatio puuttuu tietoturvakulttuuriin vain tietoturvapoikkeamien realisoituessa voi niistä seuranneiden oppien kustannukset olla suuret realisoituneen riskin myötä.

Historiaan perustuvan suorituspalautteen etu on sen suhteellisen matalat kustannukset sekä oman organisaation vahva tunteminen. Tavoitetason vertailukelpoisuus on oleellista, koska tietoturvakulttuurien määrittelyissä on eroavaisuuksia, jotka sopivat eri organisaatioille. Historiaan perustuvalla suorituspalautteella ei kuitenkaan välttämättä saavuteta sosiaalisen suorituspalautteen mahdollistamaa ennakointikykyä ja esimerkiksi tietoa päivitetyistä tietoturvallisuuden vaatimuksista.

Suositeltavimmaksi lähestymistavaksi voidaan tutkimuksen perusteella todeta sosiaalinen tavoitteiden määrittely, eli tavoitteiden määritteleminen vertaisorganisaatioiden suoritusten perusteella. Sosiaalinen suorituspalaute on todettu toimivammaksi toiminta-alueilla, joita ei pidetä stabiileina. Tämä kuvaus pätee tietoturvallisuuden toimintaympäristöön, jolle on tyypillistä erilaiset muutokset, kuten uusien uhkien tuomat uudenlaiset vaatimukset. Heikkoutena sosiaalisessa suorituspalautteessa voidaan nähdä vertaisyrityksistä kerätyn tiedon mahdollisesti korkeat kustannukset sekä vertailukelpoisten organisaatioiden löytämisen vaikeus.

Käsitellään vielä suorituspalautteen vaikutuksia *organisaation muutoksiin.* Organisaation muutoksia ajavat ongelmahaut, kuten uusien toimintatapojen kokeilut, strategioiden muuttaminen, konferenssikäynnit ja sidosryhmien kanssa kommunikointi. Nämä haut käynnistyvät tietoturvakulttuurin tapauksessa todennäköisimmin negatiivisella suorituspalautteella. Eräs tärkeä keino kehittää suorituspalautteen avulla heikoksi todettua tietoturvakulttuuria on tietoturvallisuuskoulutukset. Tietoturvakulttuurin muutoksia voi ajaa myös epäsuora suorituspalaute. Tällä tarkoitetaan suorituspalautetta, joka ei varsinaisesti mittaa tietoturvakulttuurin tasoa, vaan johon tietoturvakulttuurin taso vaikuttaa. Esimerkiksi tietoturvapoikkeamat voivat näkyä negatiivisesti organisaation kannattavuudessa. Muutokset eivät aina vaikuta tietoturvakulttuuriin odotetusti, vaan ne voivat harkitsemattomina ja juurisyihin perehtymättä aikaansaada negatiivisia vaikutuksia.

Tietoturvakulttuurin kehittämiseksi palaute on välitettävä henkilöstölle säännöllisesti. Positiivinen ja laadukkaasti toimitettu palaute voi parantaa henkilöstön sitoutumista ja motivaatiota ja näin parantaa tietoturvakulttuuria.

Yllä esitetyt löydökset esitetään vielä tiivistettynä taulukossa 4. Alakysymyskohtaisten havaintojen perusteella voidaan vastata päätutkimuskysymykseen: ”Mikä on suorituspalautteen rooli organisaatioiden tietoturvakulttuurin kehittämisessä?”. Suorituspalauteteorian voidaan katsoa soveltuvan tietoturvakulttuurin kehittämiseen. Pelkkä suorituspalautteen kerääminen ei kuitenkaan takaa tietoturvakulttuurin kehitystä tai organisaatio-oppimista, vaan lopulta vastuu on päätöksentekijöillä. Suorituspalautetta voidaan kuitenkin ajatella tietoturvakulttuurin arvioimiseen hyödyllisenä työkaluna. Itse muutos voi tapahtua suorituspalautteesta saadun informaation perusteella. Tutkimuksen perusteella ainakin henkilöstön suhteesta tietoturvallisuuteen on suositeltavaa kerätä monipuolisesti suorituspalautetta. Monipuolisempi tietoturvakulttuurin kehittäminen suorituspalauteteorialla vaatii kuitenkin tietoturvakulttuurin tarkempaa käsitteellistä selvitystä. Tutkimuksen tärkeimpänä löydöksenä voidaan kuitenkin pitää suorituspalauteteorian potentiaalia tietoturvakulttuurin arvioimisen viitekehyksenä. Tärkeänä löydöksenä voidaan pitää myös oman organisaatiokulttuurin tuntemisen tärkeyttä, koska tietoturvakulttuuri olisi voitava sovittaa siihen mahdollisimman hyvin, jotta suorituspalaute voisi toimia tietoturvakulttuurin arvioinnin työkaluna. Lisäksi tutkimus korostaa päätöksentekijöiden vastuuta muutoksesta.

Taulukko 4: Löydökset tiivistetyssä muodossa

Kysymys	Löydökset
Voiko tietoturvakulttuurista kerätä suorituspalautetta? Minkälaista?	- Suorituspalautetta voidaan kerätä organisaatioiden tietoturvakulttuurista, koska sen taso on mitattavissa ja sille voidaan asettaa tavoitteet samoilla mittareilla.
Miten tietoturvakulttuuria mitataan?	- Esimerkiksi tietoturvakulttuurin mitattavien dimensioiden kautta. - Mittaukset toteutetaan usein laadullisina henkilöstökyselyinä. - Mittauksia on tärkeä toistaa säännöllisesti.
Miten tietoturvakulttuurin tavoitetaso määritellään?	Tavoitetaso voidaan määritellä usealla tavalla. - *Luonnollisella määrittelytavalla* voidaan pyrkiä reagoimaan tietoturvapoikkeamiin ja oppimaan virheistä. Ongelmana on sen reaktiivinen luonne. - *Historiaan perustuva* tyyli on usein kustannuksiltaan matalampaa ja omaan organisaatioon personoitua. Haasteena on kuitenkin muuttuvan toimintaympäristön havainnoinnin niukkuus. - *Sosiaalisella määrittelyllä* voidaan hyödyntää vertaisorganisaatioiden tietoa ja saada kattavampi kuva toimintaympäristön tietoturvavaatimuksista. Kustannukset voivat nousta kuitenkin tässä tyylissä suuriksi ja yhteensopivien organisaatioiden löytäminen voi tuottaa haasteita. Todettiin suositeltavimmaksi tyyliksi.
Miten suorituspalautteen avulla voidaan uudistaa organisaatiota?	- Muutosta ajetaan useimmiten, kun suoriudutaan alle tavoitteiden. Tällöin ongelmahauilla etsitään ratkaisukeinoja. - Ulkopuolista näkemystä syytä hyödyntää. - Muutosta ajaa myös epäsuora-suorituspalaute. - Palautteen välittäminen henkilöstölle sekä henkilökohtainen palaute ovat oleellinen osa muutosta.

Työn tavoitteena oli selvittää suorituspalautteen rooli tietoturvakulttuurin kehittämisessä. Tutkimuksessa selvisi, että suorituspalauteteoria on yhteensopiva tietoturvakulttuurin arvioinnin tarkoitukseen, jonka kautta tietoturvakulttuurin kehityskohtia voidaan löytää. Työn voidaan siis katsoa täyttävän tavoitteensa.

6.2 Tutkimuksen arviointi, rajoitteet ja tarpeet jatkotutkimukselle

Tutkimus toteutettiin Finkin (2014) mallin perusteella. Tässä kappaleessa arvioidaan tutkimusta mallin vaiheita tarkastellen. Mallin vaiheet olivat

1. Tutkimuskysymyksen asetus
2. Kirjallisuuden ja tietokantojen valinta
3. Hakusanojen ja -lauseiden valinta
4. Käytännön hakukriteerien valinta
5. Metodologinen rajaus
6. Katsauksen tekeminen
7. Tulosten syntetisointi (Fink 2014).

Tutkimuskysymys asetettiin mielekkäästi. Kysymys tuntui helpolta perustella viitaten lähdeaineistoon. Onnistunut tutkimuskysymyksen asetus helpotti tutkimuksen tavoitteellisuutta. Mallin vaiheet 2─5 toteutettiin luvun 2 mukaisesti. Hankaluuksia kyseisissä vaiheissa toi suorituspalautetta ja tietoturvakulttuuria poikkitieteellisesti käsittelevän kirjallisuuden niukkuus. Aineisto saatiin kuitenkin koottua suhteellisen mielekkäästi. Lisäksi käytettyjen menetelmien ja tehtyjen valintojen dokumentoinnilla pyrittiin mahdollisimman hyvään toistettavuuteen. On todettava, että entistä parempi toistettavuus olisi voitu saavuttaa dokumentoimalla omaa ajatustyötä tutkimuksen alkuvaiheessa systemaattisemmin.

Itse katsauksen tekeminen sujui suhteellisen vaivattomasti, kun aineisto oli selvä. Katsausta tehdessä ja tuloksia syntetisoidessa pyrittiin mahdollisimman objektiiviseen lähestymistapaan. Tutkimus olisi kuitenkin ollut todennäköisesti objektiivisempi, mikäli sitä olisi tehnyt useampi henkilö.

Kokonaisuudessaan tutkimuksen voidaan katsoa onnistuneen. Työ saavutti tavoitteensa. Lisäksi hyviä tieteellisiä käytäntöjä pyrittiin noudattamaan. Tämäkin tavoite nähdään saavutetuksi. Tutkimuksen merkitys on rohkaista tutkijoita tarkastelemaan suorituspalauteteorian ja tietoturvakulttuurin välistä yhteyttä tarkemmin. Työn yhteiskunnallinen merkitys puolestaan painottuu sen tarjoamaan apuun organisaatioiden tietoturvakulttuurin jatkuvassa kehittämisessä.

Tutkimuksessa ilmeni joitain rajoitteita sekä tarpeita jatkotutkimukselle. Suorituspalautteen sekä tietoturvakulttuurin kehittämisen teoria oli hyvin yhteensopivaa, mutta niitä oli yhdistetty aiemmissa tutkimuksissa melko niukasti. Tämä osaltaan rajoitti kirjallisuuskatsauksen toteuttamista. Tutkimusten löydöksissä havaittiin kuitenkin suorituspalautteen

potentiaali tietoturvakulttuurin arvioinnin viitekehyksenä. Näin ollen jatkotutkimus suorituspalauteteorian soveltamisesta tietoturvakontekstiin nähdään tarpeellisena.

Täysin yksiselitteistä määritelmää suorituspalautteen roolista tietoturvakulttuurin kehittämisessä oli vaikea muodostaa, koska tietoturvakulttuurin määritelmä ei ole tieteellisesti yksiselitteinen. Tutkimuksessa ilmeni siis tarve jatkotutkimukselle tietoturvakulttuurin määrittelyn yhtenäistämiseksi.

LÄHTEET

Ahn, S., Cho, C.K. & Cho, T.S. (2021). Performance feedback and organizational learning: the role of regulatory focus. Management decision, Vol.59 (3), pp.616–637. Saatavilla (1.4.2023): https://www.proquest.com/docview/2526824180?accountid=14242&parentSessionId=PWjrpA1o9bvAjAaGJnTT99PQwKQVuDELR%2BLjl7mR0Y0%3D&pq-origsite=primo

Balozian, P., Leidner, D. & Warkentin, M. (2019). Managers' and Employees' Differing Responses to Security Approaches. The Journal of computer information systems, Vol.59 (3), pp.197–210. Saatavilla (10.4.2023): https://www-tandfonline-com.libproxy.tuni.fi/doi/full/10.1080/08874417.2017.1318687

Bartnes, M., Moe, N.B. & Heegaard, P.E. (2016). The future of information security incident management training: A case study of electrical power companies. Computers & security, pp.6132–45. Saatavilla (10.4.2023): https://www-sciencedirect-com.libproxy.tuni.fi/science/article/pii/S0167404816300530?via%3Dihub

Choi, J., Rhee, M. & Kim, Y.C. (2019). Performance feedback and problemistic search: The moderating effects of managerial and board outsiderness. Journal of business research, Vol. 102, pp.21—33. Saatavilla (23.3.2023): https://www-sciencedirect-com.libproxy.tuni.fi/science/article/pii/S0148296319302929?via%3Dihub

Cyert, R.M. & March J.G. (1963). A Behavioral Theory of the Firm. Englewood Cliffs, NJ: Prentice Hall.

European Union Agency for Network and Information Security (ENISA). (2017). Cyber security culture in organisations. Saatavilla (14.4.2023): http://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations

Fink, A. (2014). Conducting research literature reviews: From the Internet to paper. California: SAGE Publications, Inc.

Greve, H. R. (2003). Organizational learning from performance feedback: a behavioral perspective on innovation and change. Cambridge, Cambridge University Press. Saatavilla: (10.3.2023): https://web.p.ebscohost.com/ehost/detail/detail?vid=0&sid=581771be-54b4-4ab5-906d-ad5d1ac97799%40redis&bdata=JkF1dGhUeXBlP-WNvb2tpZSxpcCx1aWQmc2l0ZT1laG9zdC1saXZlJnNjb3BlPXNpdGU%3d#AN=120383&db=e000xww

Havakhor, T., Tianjian, Z. & Bryan, H. (2018). The Business Value of Engaging in Counter-Breach Initiatives. Oklahoma State University. Saatavilla (2.4.2023): https://web.archive.org/web/20200323184802id_/https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1322&context=amcis2018

Kotiloglu, S., Chen, Y. & Lechler, T. (2021). Organizational responses to performance feedback: A meta-analytic review. SAGE Publications, London England. Strategic organization, Vol. 19 (2), pp.285-311. Saatavilla (14.2.2023): https://journals-sagepub-com.libproxy.tuni.fi/doi/full/10.1177/1476127019883361

Kraemer, S. & Carayon, P. (2005). Computer and Information Security Culture: Findings from Two Studies. Proceedings of the Human Factors and Ergonomics Society, Vol.49 (16), pp.1483–1487. Saatavilla (17.4.2023): https://journals-sagepub-com.libproxy.tuni.fi/doi/abs/10.1177/154193120504901605

Li, J., Ren, B., Zhang, T., Li, C. & Liu, Z. (2019). Research on optimal control model of complex networks security risk. Journal of Physics: Conference Series, Vol.1345 (4), p.42048. Saatavilla (1.4.2023): https://www.proquest.com/docview/2568058626?accountid=14242&parentSessionId=eWIjeNmdj13owh7SUGrfKVaJXjoB4uTUGtGNtrrteK0%3D&pq-origsite=primo

Mäses, S., Maennel, K. & Brillingaitė, A. (2022). Trends and challenges for balanced scoring in cybersecurity exercises: A case study on the example of Locked Shields. Frontiers in education (Lausanne), Vol.7. Saatavilla (5.4.2023): https://www.frontiersin.org/articles/10.3389/feduc.2022.958405/full

Nasir, A., Arshah, R.A., Hamid, M.R. & Fahmy, S. (2019). An analysis on the dimensions of information security culture concept: A review. Journal of information security and applications, Vol.44, pp.12─22. Saatavilla (14.4.2023): https://www-sciencedirect-com.libproxy.tuni.fi/science/article/pii/S2214212617306828?via%3Dihub

Orehek, Š. & Petrič, G. (2021). "A systematic review of scales for measuring information security culture", Information and Computer Security, Vol. 29 (1), pp. 133-158. Saatavilla (21.3.2023) https://www.proquest.com/docview/2526829225?accountid=14242&parentSessionId=g9f5%2FL%2FQ6zbaqU5qdLQbtc%2FH9Qjnwoq5dRAA2jnI1l8%3D&pq-origsite=primo

Porthouse, A., Clancy, H. Lax, P. (2021). Training for major incidents. Surgery (Oxford), Vol.39, (7), pp.388-392. Saatavilla (14.4.2023): https://doi.org/10.1016/j.mpsur.2021.05.007

Say, G. & Vasudeva, G. (2020). Learning from Digital Failures? The Effectiveness of-Firms' Divestiture and Management Turnover Responses to Data Breaches. INFORMS.
Strategy science, Vol.5 (2), pp.117-142. Saatavilla (5.2.2023): https://pubsonline-informs-org.libproxy.tuni.fi/doi/full/10.1287/stsc.2020.0106

Shah, M., Maitlo, A., Jones, P. & Yusuf, Y. (2019). Journal of knowledge management, Vol.23 (9), pp.1857–1884. Saatavilla (15.4.2023): https://www.proquest.com/docview/2323322297?accountid=14242&parentSessionId=3Aeb4CYHk2iUzDxT%2F4or6qjmk2hCOx4lyV6L3oLTWLg%3D&pq-origsite=primo

Tagliabue, M., Sigurjonsdottir, S.S. & Sandaker, I. (2020). The effects of performance feedback on organizational citizenship behaviour: a systematic review and meta-analysis. European journal of work and organizational psychology. Vol.29 (6), pp. 841─861. Saatavilla (12.4.2023): https://www.frontiersin.org/articles/10.3389/feduc.2022.958405/full

Tolah, A., Furnell, S.M. & Papadaki, M. (2021). An empirical analysis of the information security culture key factors framework. Computers & security, Vol.108, p. 102354. Saatavilla (12.4.2023): https://www-sciencedirect-com.libproxy.tuni.fi/science/article/pii/S0167404821001784?via%3Dihub

Van Niekerk, J.F. & Von Solms, R. (2010). Infromation security culture: A management perspective. Elsevier Ltd, Amsterdam. Computers & security, Vol.29 (4), pp.476-486. Saatavilla (5.2.2023): https://www-sciencedirect-com.libproxy.tuni.fi/science/article/pii/S0167404809001126?via%3Dihub

da Veiga, A. & Eloff, J.H.P. (2010). A framework and assessment instrument for information security culture. Comput. Secur, Vol.29 (2), 196–207.

da Veiga, A., Astakhova, L.V., Botha, A. & Herselman, M. (2020). Defining organizational information security culture—Perspectives from academia and industry. Elsevier Ltd, OXFORD. Computers & security, Vol.92, pp.101713-23. Saatavilla (16.2.2023): https://www-sciencedirect-com.libproxy.tuni.fi/science/article/pii/S0167404820300018?via%3Dihub

Ye, Y., Yu, W. & Nason, R. (2021). Performance Feedback Persistence: Comparative Effects of Historical Versus Peer Performance Feedback on Innovative Search. Journal of management, Vol.47 (4), p.1053-1081. Saatavilla (13.4.2023): https://openurl-ebsco-com.libproxy.tuni.fi/openurl?sid=Primo&volume=47&atitle=performance+feedback+persistence&date=20210401&spage=1053&issn=0149-2063&issue=4&genre=article&title=Journal+of+management.&epage=1081&doi=10.1177%2F0149206320916225