Timo Turunen

TIETOTURVASTRATEGIAT TERVEYDENHUOLLON ORGANISAATIOISSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2018

TIIVISTELMÄ

Turunen, Timo
Tietoturvastrategiat terveydenhuollon organisaatioissa
Jyväskylä: Jyväskylän yliopisto, 2018, 63s.
Kyberturvallisuus, Pro gradu -tutkielma
Ohjaaja: Siponen, Mikko

Tietojärjestelmien roolin kasvaessa tämän päivän organisaatioiden liiketoiminnassa, myös tietoturvan merkitys liiketoiminnan turvaajana ja mahdollistajana kasvaa. Teknologian ja hyökkäysmenetelmien kehityksen seurauksena tietoturvan rooli strategisena ongelmana korostuu, organisaatioiden pyrkiessä turvaamaan omat liiketoimintaprosessit käytössä olevien resurssien puitteissa. Tietoturvastrategia on kuitenkin suhteellisen uusi konsepti tietoturvakirjallisuudessa ja se on voinut saada hyvinkin erilaisia määritelmä niin kirjallisuudessa kuin käytännössä. Tämä tutkimus pyrkii selkeyttämään tätä konseptia ja selvittämään tietoturvastrategioiden roolia terveydenhuolto-organisaatioissa, joiden toiminnan tavoitteet voivat erota suuresti muiden alojen vastaavista. Terveydenhuolto alalla muun muassa henkilöstön ammatilliset arvot, alan tarkka säätely ja pyrkimys väestön terveyden edistämiseen voi luoda oman haasteensa tietoturvan strategiselle suunnittelulle. Tutkimuksessa hyödynnettiin tutkimusmenetelmänä tapaustutkimusta, joka mahdollisti ilmiön tutkimisen sen luonnollisessa kontekstissa julkisen terveydenhuollon organisaatioissa. Tutkimuksen tulosten perusteella tietoturvalla oli keskeinen rooli tapauksissa, mutta tietoturvastrategiaa ei hyödynnetty tietoturvan suunnittelussa ja kehityksessä, vaikka tietoturvakirjallisuus on nostanut esille strategiasta mahdollisesti saatavia hyötyjä. Tietoturvastrategioiden puute voi johtua niiden selkeiden hyötyjen puutteella suhteessa esimerkiksi tietoturvapolitiikkaan ja riskienhallintaan. Tutkimuksen tulosten ja aiemman tietoturvastrategiaan keskittyvän kirjallisuuden pohjalta tutkimuksessa esitettiin huomioitavia tekijöitä, kuten liiketoiminnalliset tarpeet, riskit, kulttuuri, lainsäädäntö ja tietojärjestelmät, jotka terveydenhuolto-organisaation tulisi ottaa huomioon päättäessään kehittää tietoturvastrategia. Puutuvista selkeistä tietoturvastrategian hyödyistä huolimatta, tässä tutkimuksessa esitetty viitekehys voi auttaa organisaatiota kohti strategisempaa lähestymistapaa tietoturvan suunnitteluun ja toteutukseen.

Avainsanat: tietoturva, terveydenhuolto, tietoturvastrategia, tietoturvapolitiikka, tietoturvakulttuuri

ABSTRACT

Turunen, Timo
Information security strategies in healthcare organizations
Jyväskylä: University of Jyväskylä, 2018, 63 pp
Cyber Security, master's thesis
Instructor: Siponen, Mikko

The role of information systems in today's organization's business processes is increasing. At the same time the role of information security as business enabler and protector is increasing. Continually evolving technologies and attack methods creates a need to think the information security as a strategic problem, as organizations aims to protect their business within their available resources. The concept of information security strategy is fairly new concept and it has been given multiple different definition in prior literature and practice. This research aims to clarify the concept and study information security strategies in healthcare context. The objectives of information security can differ in healthcare sector when compared to other sectors. In healthcare employees' values, legal requirements and the aim to improve the well-being of citizens can create challenges for strategic information security planning. This study used case study as a research method to understand this phenomenon in its natural setting in public healthcare organizations. Based on the findings, information security has important role in the study cases, but information security strategies are not being used to plan and maintain organizations' information security practices, although prior information security literature has highlighted the possible benefits of the strategies. The lack of clear benefits compared to information security policies and risk management could explain why organizations have not created these strategies. Based on the findings and prior literature this thesis proposed factors (i.e. business needs, risks, culture, legal compliance and information systems) that organizations need to consider while creating information security strategy. Despite the lack of clear benefits, the proposed model of this research could help organizations to move toward strategic approach to information security and improve and maintain their overall security posture.

Keywords: information security, healthcare, information security strategy, information security policy, information security culture

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Tietojärjestelmillä ja niiden sisältämällä tiedolla on keskeinen rooli tämän päivän organisaatioissa. Tietoturvalla pyritään suojaamaan organisaation voimavaroja, siten että arvonluonti niiden avulla on mahdollista. Organisaation kohtaamat tietoturvatapahtumat ovat yleistyneet verkossa toimivien haitallisten toimijoiden (mm. hakkerit ja verkkorikolliset) pyrkiessä omien tavoitteiden saavuttamiseen. Kyberuhkat on nähty organisaatioissa yhdeksi suurimmista tulevaisuuden uhkista. Organisaatioilta voi kuitenkin puutua keinoja tehokkaan tietoturvan saavuttamiseen, ja esimerkiksi riittämätön investointi tietoturvaan voivat olla yleisiä. Toimintaympäristön muutoksen seurauksena myös tietoturvavaatimukset voivat muuttua, johon organisaation olisi kyettävä reagoimaan käytössä olevilla resursseilla. Lisäksi tietojärjestelmien monimutkaisuus, kehittyneet hyökkäysmenetelmät ja tietovuodon mahdolliset suuret taloudelliset tappiot tekevät tietoturvasta tärkeä strateginen ongelman (Posthumus & von Solms 2004).

Tästä huolimatta tietoturva usein ajatellaan tekniseksi ongelmaksi. Vaikka strategisella suunnitelulla on vakiintunut rooli organisaatioiden liiketoiminnassa, tietoturvastrategiat ovat saaneet suhteellisen vähän huomiota tietoturvakirjallisuudessa. Kirjallisuudessa tietoturvastrategialla on vaihtelevia määritelmiä, jotka usein painottavat tietoturvan teknisen puolen strategiseen suunnitteluun, vaikka myös henkilöstö tulisi ottaa huomioon tietoturvassa. Tästä syystä tämä tutkimus pyrkii tarkastelemaan tietoturvaa ylemmältä tasolta, joka kattaa sekä teknisen että hallinnollisen tietoturvan, jolloin myös ihmiset osana tietojärjestelmää tulee huomioiduksi. Tietoturvastrategia voidaan nähdä tavoitteellisena menetelmänä suunnitella tietoturvaa sen kehittämiseksi ja ylläpitämiseksi pitkällä aikavälillä. Nämä strategiat tyypillisesti sisältävät käsityksen organisaation nyky- ja tavoitetilasta ja menetelmistä tavoitteeseen pääsemiseksi.

Tämä tutkimus pyrkii tuottamaan uutta tietoa tietoturvastrategioihin liittyen keskittyen tarkastelemaan näitä strategioita terveydenhuollon organisaatioissa, jossa tiedolla on erityislaatuinen luonne. Terveydenhuollossa käsiteltävä tieto voidaan luokitella kriittiseksi sekä potilaiden että organisaation toiminnan kannalta. Tästä syystä mm. tietoturvan perinteisillä tavoitteilla luottamuksellisuudella, eheydellä ja saatavuudella, voidaan nähdä olevan keskeinen

rooli organisaatioiden toiminnassa. Terveydenhuoltosektorin toiminnan tavoitteet, tarkka säätely ja henkilöstön vahvat ammatilliset arvot asettavat oman haasteensa tietoturvan toteutukselle. Nämä seikat tarjoavat mielenkiintoisen, ja aiemmasta kirjallisuudesta poikkeavan lähestymistavan tietoturvastrategioihin, joka voi auttaa niiden ymmärtämisessä.

Tutkimuksen tavoitteena on tuottaa uutta tietoa kokonaisvaltaisiin tietoturvastrategioihin liittyen, joiden tarpeellisuus on tullut esille aiemmassa kirjallisuudessa (Ahmad ym. 2014). Tutkimus pyrkii tarjoamaan tieteellisiä ja käytännöllisiä hyötyjä. Tutkimus pyrkii tuottamaan uutta tietoa tietoturvastrategioista - varsinkin terveydenhuoltoalalla. Käytännöllisestä näkökulmasta tutkimus pyrkii auttamaan terveydenhuoltosektorilla toimivia organisaatioita tarkastelemaan heidän nykyistä lähestymistä tietoturvaan ja arvioimaan onko kaikki tarvittavat tekijät arvioitu heidän nykyisessä tietoturvan strategisessa suunnitelmassa. Tutkimus esittää teoreettisen viitekehyksen tietoturvastrategioissa huomioitavista tekijöitä kirjallisuuskatsaukseen perustuen, ja hyödyntää mallia tietoturvan ymmärtämisessä terveydenhuollon organisaatioissa.

1.1 Tutkimuskysymys

Tietoturvastrategioihin keskittynyt tietoturvakirjallisuus ei ole aiemmin tutkinut näitä strategioita keskittyen yksittäiseen alaan, vaikka eri alojen toimintaympäristö voi vaikuttaa organisaation tiedon turvaamisen. Terveydenhuoltoalan tietoturvaa ja alan tietoturvastrategioita on tutkittu vähän, jonka vuoksi tämä tutkimus pyrkii tuottamaan uutta tietoa alan tietoturvan merkityksestä ja tietoturvastrategioista. Tutkimuksen tarkoituksena on selvittää kuinka terveydenhuoltoalan toimintaympäristö ja sisäiset tekijät vaikuttavat tietoturvastrategioiden kehitykseen ja valintaan. Aiemmat teoriat eivät ole täysin riittäviä vastaamaan tutkimuksen kohteena olevaan ilmiöön. Pro gradun päätutkimuskysymys on:

- Millainen on toimiva tietoturvastrategia terveydenhuoltosektorilla?

Pääkysymys jaetaan kolmeen alakysymykseen, jotka helpottavat pääkysymykseen vastaamista:

- Mikä on tietoturvastrategia ja siihen vaikuttavat tekijät?
- Mikä on tietoturvan merkitys terveydenhuollon organisaatioissa?
- Millainen on terveydenhuollon organisaatioiden tietoturvaprosessit suhteessa tietoturvastrategiaan?

Ensimmäiseen alakysymykseen haetaan vastausta kirjallisuuskatsauksen avulla ja kahteen jälkimmäiseen alakysymykseen pyritään vastamaan tapaustutkimuksella kerätyn empiiriseen aineiston avulla. Empiirisen aineiston analyysiä pyritään helpottaa hyödyntämällä kirjallisuuskatsauksen pohjalta luotua viitekehystä tietoturvastrategioista. Alakysymyksiin vastaaminen mahdollistaa tutkittavan ilmiön ymmärtämisen ja lopulta päätutkimuskysymykseen vastaamisen.

Tämän tutkimuksen kahdessa ensimmäisessä luvussa käsitellään tutkimuksen kannalta keskeisimmät konseptit ja niihin liittyvää kirjallisuutta. Luvussa 4 tarkastellaan kirjallisuuskatsaukseen perustuen tietoturvastrategioiden edellytyksiä ja ehdotetaan teoreettista viitekehystä tietoturvastrategioiden kehitykseen ja arviontiin. Luvussa 5 esitellään tutkimusmenetelmä ja luvussa 6 käsitellään kerätty empiirinen aineisto ja pohditaan tulosten perusteella huomioitavia tekijöitä terveydenhuolto-organisaatioiden tietoturvastrategioissa. Tutkimuksen viimeinen luku on yhteenveto tutkimuksesta ja sen tuloksista.

2 TERVEYDENHUOLLON ORGANISAATIOT

Tämä tutkimus on rajattu koskemaan terveydenhuoltosektorin organisaatioita, jotka toimivat potilaiden terveyden edistämiseksi ja varmistamiseksi. Tutkimuksessa keskitytään organisaatioihin, jotka käsittelevät, prosessoivat ja säilyttävät potilastietoja. Potilastiedoiksi lukeutuvat muun muassa tiedot potilaan henkilöllisyydestä, terveydentilasta, sairauksista ja lääkityksestä.

Terveydenhuollon organisaatio voi olla julkinen tai yksityinen toimija, jonka omistajuus ja liiketoiminnalliset tavoitteet voivat vaikuttaa organisaation käytössä oleviin hallintajärjestelmiin ja resursseihin. Tästä huolimatta terveysalan tarkka säädelty määrää kaikkien alalla toimivien tavoitteita ja prosesseja.

Suomessa on voimassa useita lakeja, jotka määrittävät terveydenhuollon toimintaa ja tavoitteita, esimerkiksi Terveydenhuoltolaki 30.12.2010/1326, Asetus yksityisestä terveydenhuollosta 24.8.1990/744, Kansanterveyslaki 28.1.1972/66 ja Erikoissairaanhoitolaki 1.12.1989/1062. Näiden lakien keskeisenä tarkoituksena on varmistaa, että alalla toimivat organisaatiot toimivat väestön terveyden, hyvinvoinnin ja sosiaalisen turvallisuuden edistämiseksi ja ylläpitämiseksi. Lisäksi nämä lait pyrkivät varmistamaan tarvittavien terveyspalveluiden yhdenvertaisen saatavuuden, laadun ja potilasturvallisuuden.

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 9.2.2007/159 määrittää potilastietoihin liittyviä käytänteitä muun muassa tietojen käsittelyyn, säilyttämiseen ja luovuttamiseen liittyen, pyrkien potilaan tietosuojan takaamiseen. Organisaatioiden on varmistettava lain vaatimusten noudattaminen, mutta on huomioitava, että laki ei määritä tarkkaan teknisiä ja hallinnollisia keinoja siitä, kuinka tietoturva tulisi toteuttaa. Tämän vuoksi riittävän tietoturvajärjestelmän ja sen lainmukaisuuden varmistaminen on organisaation tehtävä.

Tietoturvakirjallisuudessa alan organisaatioiden on todettu usein lähestyvän tietoturvaa teknisestä näkökulmasta, jota edistää osaltaan alan tarkka säätely. (Kwon & Johnson 2013b) Säätelyn seurauksena organisaatioiden tietoturvan toteutusta saattaa motivoida ensisijaisesti lainvaatimukset, varsinaisen tietoturvan sijasta. Tämä voi johtaa reaktiiviseen ja tehottomaan tietoturvaan (Kwon & Johnson 2013b). Lainsäädännön ei tuli toimia ensisijaisena syynä tietoturvainvestoinnille (Kwon & Johnson 2014), mutta ne tulee huomioida, sillä noudattamatta jättämisellä voi olla suuria taloudellisia ja maineellisia seurauksia.

Teknisen tietoturvan lisäksi organisaatioiden tulisi ottaa huomioon myös tietojärjestelmän sosiaaliset ulottuvuudet, sillä ihmisillä voi olla suuri vaikutus organisaation tietoturvan toimivuuteen (Furnell & Clarke 2012). Tämä on huomioitava varsinkin terveydenhuolto alalla, jossa työntekijät on todettu omaavan vahvoja ammatillisia arvoja, jota voivat olla myös ristiriidassa tiedon turvaamiseen liittyvien arvojen kanssa (Hedström, Kolkowska, Karlsson & Allen 2011). Näistä johtuen tietoturvassa olisi huomioitava sekä tekniset että sosiaaliset tietoturvakontrollit, organisaation tietoturvan parantamiseksi.

Tiedonkäsittely voi erota merkittävästi muiden alojen vastaavista, sillä alan ydintieto on potilastiedot (sisältäen mm. sairaudet ja lääkitykset), jota

hyödyntää useat yksittäiset potilaan hoitoon osallistuvat ammattihenkilöt. Näissä tapauksissa henkilö soveltaa suoraan käytössä olevaa tietoa potilaasta hoitoa päätettäessä. Potilaaseen hoitosuhteessa oleva lääkäri hyödyntää tietoa mm. hoitoa, lääkitystä ja terveydentilaa arvioitaessa. Näissä tilanteissa tiedon tulisi olla saatavilla ja eheää, jotta potilaan todelliseen terveydentilaan perustuva hoitopäätös kyetään tekemään.

Mikäli tieto ei ole saatavilla hoitopäätös tapahtuu potilaan sen hetkiseen kliiniseen tilaan ja saatavilla oleviin sekundaarisiin tietolähteisiin, kuten potilaan lähiomaisilta saatu tieto. Tästä prosessista johtuen tiedolle asetetut saatavuuden ja käytettävyyden vaatimukset voivat erota suuresti muiden alojen vastaavista, joissa ei käsitellä yhtä kriittistä tietoa, jolla voi olla suora vaikutus henkilön terveydentilaan.

2.1 Tietoturvan merkitys

Tiedon turvaamisen yleisillä tavoitteilla luottamuksellisuudella, eheydellä ja saatavuudella on tärkeä rooli terveydenhuollon organisaatioiden toiminnassa (Stahl, Doherty & Shaw 2012). Saatavuudella voidaan varmistaa hoidon tehokkuus ja turvallisuus, sillä esimerkiksi tiedot potilaan terveydentilasta, aiemmista diagnooseista ja lääkityksestä mahdollistavat tietoon perustuvan päätöksenteon hoitoon liittyen. Eheyden tarkoituksena on varmistaa tiedon oikeellisuus, ehkäisten muun muassa tietojen luvatonta muuttamista ja poistamista. Tavoitteen toteutuessa hoidon voidaan luottaa perustuvan todelliseen tietoon potilaan tilasta. Luottamuksellisuuden tavoite on varmistaa tiedon saatavuus vain niille henkilöille, joilla on oikeus (esimerkiksi hoitosuhde) käsitellä kyseisiä potilastietoja.

Tasapainotus näiden tietoturvavaatimusten välillä voi olla haastavaa, sillä jokaisella tavoitteella on oma vaikutus lopullisen järjestelmän käytettävyyteen ja tietoturvaan (Hedström ym. 2011). Lisäksi muun muassa terveydenhuoltosektorin hajanaisuus ja usein rajoittuneet resurssit asettavat oman haasteensa tietoturvan toteutukselle (Martin 2017).

Potilastieto voidaan luokitella kriittiseksi organisaation toiminnan kannalta ja arkaluontoiseksi potilaan näkökulmasta. Terveydenhuollossa tietoturvan päätavoitteena on usein varmistaa potilaan turvallisuus, yksityisyys ja luottamus palvelun tarjoajaa kohtaan (Martin 2017). Etenkin luottamuksellisuuden rikkoutumisella, esimerkiksi tietovuodon seurauksena, voi olla merkittävä vaikutus potilaan taloudelliseen, psykologiseen ja sosiaaliseen tilanteeseen (Romanou 2017). Tietovuodon seurauksena potilas voi menettää luottamuksen palvelun tarjoajaa kohtaan, jolloin se voi vaikuttaa suoraan organisaation liiketoimintaan.

Tiedon arkaluonteisuudesta johtuen, alan organisaatiot ovat usein kyberhyökkäysten kohteena, hyökkääjien pyrkiessä saavuttamaan taloudellista hyötyä anastettujen tietojen avulla. Martin (2017) tunnisti useita mahdollisia terveydenhuoltoon liittyviä tietoturvauhkia:

- henkilötietojen varastaminen, esim. rahallisen hyödyn saavuttamiseksi

- potilastietojen varastaminen, esim. poliittiseen hyödyntämiseen
- kiristysohjelmat
- tietojen korruptointi
- palvelunestohyökkäykset
- työntekijöiden aiheuttamat tietoturva uhat.

Terveydenhuollon organisaatiot on usein nähty erityisen haavoittuvaisiksi esimerkiksi sosiaalisenhakkeroinnin hyökkäyksille, johtuen organisaation kulttuurista pyrkiä auttamaan ihmisiä (Zerlang 2017). Lisäksi työntekijöiden ammatilliset arvot voivat olla ristiriidassa tietoturvatavoitteiden kanssa. (Hedström ym. 2011) Ammatilliset arvot voivat vahvasti säädellä työntekijöiden päätöksentekoprosessia potilas- ja henkilötietojen käsittelyyn liittyen.

Tietoturvalla on tärkeä merkitys etenkin alan organisaatioille, jotka pyrkivät hyödyntämään tieto- ja viestintäteknologiaa terveyspalveluiden tarjoamisessa. Esimerkkejä tällaisista sähköisistä terveydenhuoltopalveluista ovat, muun muassa etäterveydenhuolto, telelääketiede ja erilaiset sensoriteknologiat (esimerkiksi lääkinnällisissä laitteissa) diagnosoinnin, hoidon ja seurannan parantamiseksi (Romanou 2017). Teknologian tuomat mahdollisuudet luovat myös uusia haasteita yksityisyyteen ja tietoturvaan liittyen, sillä uudet teknologiat kasvattavat mahdollista hyökkäyspinta-alaa uusien teknologioiden kautta. Heikolla tietotuvalla voi olla suuri taloudellinen ja maineellinen vaikutus alan organisaatioihin (Martin 2017).

Terveydenhuollon tietoturvaan keskittynyt tutkimus on ollut erityisen kiinnostunut alan erityispiirteiden, kuten tavoitteiden, kulttuurin ja osaamisen vaikutuksesta organisaatioiden tietoturvaan. Kirjallisuudessa on kuitenkin kiinnitetty suhteellisen vähän huomiota kokonaisvaltaisen tietoturvan saavuttamiseen alan organisaatioissa. Tietoturvastrategia voi olla keino ylläpitää ja kehittää kokonaisvaltaisesti organisaation tietoturvaa käytössä olevien resurssien puitteissa. Varsinkin alalla, kuten terveydenhuolto, jossa muun muassa toiminnan tavoitteet, organisaation kulttuuri ja riskit luovat haasteen tietoturvalle, mutta olisi huomioitava tietoturvan toteutuksessa. Varsinkin tietoturvakulttuurin luominen tai muuttaminen vaatii pitkäaikaista sitoutumista ylemmältä johdolta (Da Veiga & Eloff 2007; Kayworth & Whitten 2012). Terveydenhuollossa tietoturvakulttuuriin voi liittyä omat haasteensa, johtuen terveydenhuoltoalalla työskentelevien henkilöiden vahvoista ammatillisista arvoista, jotka voivat alla myös riskiriidassa tietoturvaan liittyvien arvojen kanssa (Hedström ym. 2011).

Lähes kaikki organisaatiot, terveydenhuolto mukaan lukien, ovat kohdanneet haasteen jatkuvasti muuttuvasta toimintaympäristöstä, jonka riskit aiheuttavat haasteen tietoturvan toteutukselle. Tällaisessa ympäristössä terveydenhuolto-organisaatioilla on tarve kehittää tietoturvastrategioita, jotka varmistavat tietoturvan potilastiedoilla ja tietoturvan lain- ja säädöstenmukaisuuden. Näiden tavoitteiden saavuttaminen voi varmistaa organisaation tehokkaan tietoturvastrategian (Kwon & Johnson 2012).

3 TIETOTURVASTRATEGIA

Tietoturvastrategioiden ymmärtämiseksi on tärkeää määritellä tietoturvastrategia konseptina. Haasteelliseksi tietoturvastrategian määrittelyn tekee se, että vaikka termi esiintyy usein tietoturvakirjallisuudessa, sen selkeä määrittely on usein jäänyt puuttumaan (Horne, Ahmad & Maynard 2017). Tässä luvussa määritellään tämä tutkimuksen kannalta keskeinen konsepti perustuen aiempaan tietoturvakirjallisuuteen. Lisäksi luvussa tarkastellaan aiempaa tietoturvastrategioihin keskittynyttä kirjallisuutta ja tunnistetaan tarve lisätutkimukselle.

3.1 Määritelmä

Strategia on yleinen konsepti sota- että liiketaloustieteissä. (Horne ym. 2017) Sotatieteissä strategia nähdään korkeimman tason suunnitteluna, johon alemman tason taktiset ja operatiiviset suunnitelmat perustuvat. Liiketaloustieteissä strategia on nähty organisaation laajuisena konseptina, joka kertoo organisaation hallinnon määrittämän suunnan ja toimenpiteet organisaation sisällä tavoitteisiin pääsemiseksi. Tätä valittua suuntaa pyritään kommunikoimaan organisaatiossa alaspäin työntekijöille ja muille sidosryhmille, jotka vaikuttavat strategian toteutukseen ja tavoitteiden saavuttamiseen. Strategian soveltaminen käytäntöön vaikuttaa organisaation kykyyn saavuttaa strategian tavoitteet kustannustehokkaasti (Horne ym. 2017; Beebe & Rao 2010).

Tietoturvastrategia on usein tietoturvakirjallisuudessa esiintyvä termi, mutta se on harvoin tarkkaan määritelty. (Horne ym. 2017) Lisäksi kirjallisuudessa, jossa tietoturvastrategia on määritelty, on antanut sille erilaisia määritelmiä eri näkökulmista. Yhtenäistä kirjallisuudessa on se, että niissä on korostettu strategioiden tarpeellisuutta organisaation tietoturvan toteutuksessa ja kehittämisessä (Anderson & Choobineh, 2008; Kayworth & Whitten 2010; Park & Ruighaver 2008). Tietoturvastrategialla voidaan muun muassa varmistaa riittävät resurssit tietoturvauhkien estoon (Beebe & Rao 2010).

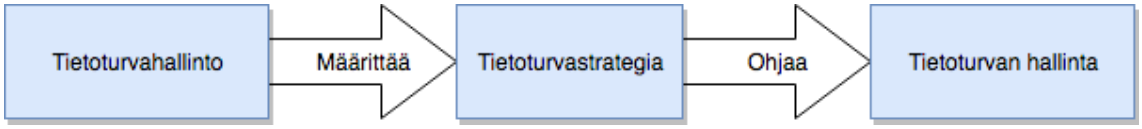
Tietoturvastrategia toimii kokonaisvaltaisena suunnitelmana tietoturvan kehitykselle ja hallinnalle (Baskerville & Dhillon 2008). Beebe ja Rao (2010) määrittelivät tietoturvastrategian suunnitelmaksi integroida organisaation tärkeimmät tietoturvatavoitteet, politiikat ja toimintaprosessit yhteneväiseksi kokonaisuudeksi. Tässä tyypillisesti dokumentoidussa suunnitelmassa, otetaan huomioon organisaation ulkoiset uhat suhteessa olemassa oleviin tietoturvakontrolleihin, sisältäen myös tietoturvakontrolleja tukevat tietoturvapolitiikat ja toimintaprosessit (Horne ym. 2017). Lisäksi Horne ym. (2017) näki strategian keinoina vaikuttaa organisaation sisäiseen tietoturvaympäristöön käytettyjen tietoturvakontrollien avulla. Tietoturvastrategialla yleensä pyritään kehittämään, kommunikoimaan and tukemaan organisaation tietoturvatavoitteita (Carcary, Renaud, McLaughlin & O'Brien 2016).

Kirjallisuudessa on tunnistettu useita eri tyyppisiä tietoturvastrategioita, kuten pelote, ehkäisy, tarkkailu, tunnistus, reagointi, ja harhautus, joita

voidaan hyödyntää tietoturvan strategisessa toteutuksessa. (Ahmad, Maynard & Park 2014) Useista strategiatyypeistä huolimatta, organisaatiot usein painottavat ehkäiseviin strategioihin, organisaatioiden pyrkiessä varmistamaan järjestelmien saatavuus.

Useat strategiat tarvitsevat ylemmän kokonaisvaltaisemman strategian niiden yhdistämiseksi tehokkaaksi puolustusjärjestelmäksi, sillä keskittymällä vain yksittäiseen strategiatyyppiin, voi puolustus jäädä puutteelliseksi (Ahmad ym. 2014). Lisäksi on huomioitava, että nämä strategiat vaativat sekä teknisten (mm. tietoturvateknologiat) että sosiaalisten tekijöiden (mm. tietoturvakulttuuri) huomioimista. Keskittymällä strategisesti implementoimaan vain teknisiä ratkaisuja, voi aikaansaatu puolustus olla puutteellinen (Furnell & Clarke 2012).

Hallinnollisesta näkökulmasta tietoturvastrategia toimii tietoturvahallinnon (information security governance) ja tietoturvan hallinnan (information security management) välissä (Kuva 1). Tietoturvahallinto voi määrittää strategian tietoturvan toteutukselle, joka puolestaan ohjaa tietoturvan taktista ja operatiivista toteutusta.



Kuvio 1: Tietoturvastrategia tietoturvan hallintajärjestelmässä

Kuten yrityshallinnolle (corporate governance) myös tietoturvahallinnolle on vaikea antaa yksiselitteistä määritelmää. Yleensä tietoturvahallinnolla tarkoitetaan hallinnointi- ja ohjausjärjestelmää, joka määrittelee mm. yritysjohdon roolin ja velvollisuudet tietoturvaan liittyen. Tämän järjestelmän tavoitteena on mahdollistaa tietoturvan johtaminen ja kontrollointi suhteessa organisaation liiketoimintaan. Tietoturvastrategian luominen on nähty ensimmäisiksi askeleiksi organisaation pyrkiessä tietoturvahallinnon käyttöönottoon (Carcary ym. 2016; Damenu & Beaumont 2017; Karanja 2017).

Tietoturvan hallinta on puolestaan tietoturvan operatiivista toteutusta, jossa tietoturvajärjestelmä implementoidaan tietoturvahallinnon antaman valtuutuksen pohjalta annettujen resurssien puitteissa. Tehokas tietoturvan hallinta ei tulisi olla liiketoiminnasta erillään olevaa toimintaa, vaan sen pitäisi perustua mietitylle tietoturvastrategialle (Barton, Tejay, Lane & Terrell 2016). Tietoturvan hallinta voi implementoida teknisiä (esim. palomuuri ja IDS), virallisia (esim. tietoturvapolitiikat) ja epävirallisia (esim. tietoturvakoulutus) tietoturvakontrolleja, tietoturvan hallinnan pyrkiessä tietoturvatavoitteiden saavuttamiseen (Sveen ym. 2009).

Myös tietoturvastrategian erot tietoturvapolitiikasta on tärkeä ymmärtää, sillä ne voivat dokumentteina muistuttaa toisiaan. Tietoturvapolitiikka on laajoja kannanottoja tietoturvatavoitteista, jotka organisaatio pyrkii saavuttamaan. (Doherty & Fulford 2006) Ne tyypillisesti sisältää yleisiä kannanottoja päämääristä, tavoitteista, uskomuksista ja vastuista tietoturvaan liittyen. Tietoturvastrategia puolestaan keskittyy enemmin ohjaamaan operatiivista toimintaa tarjoamalla suuntaviivat sen toteuttamiseksi. Sillä tietoturvapolitiikan olisi kyettävä

heijastamaan organisaation liiketoiminnallisia tarpeita (Doherty & Fulford 2006), tietoturvastrategia voi auttaa tietoturvapolitiikan kehityksessä varmistaen tietoturvan liiketoimintaa tukevan pyrkimykset. Strategisella tasolla tietoturvan hyödyt, kuten pienentyneet tietoturvaloukkauksen vahingot ja muut vaikutukset, tulisi tasapainottaa suhteessa tietoturvan hintaan (Anderson & Choobineh 2008).

Edellä esiteltyyn kirjallisuuteen perustuen, tietoturvastrategia määritellään tässä tutkimuksessa *koko organisaation kattavaksi tavoitteelliseksi suunnitelmaksi tietoturvan ylläpitämiseksi ja kehittämiseksi - pyrkien saavuttamaan sille asetetut tavoitteet ohjaamalla tietoturvan hallintaa, samalla huomioiden organisaation liiketoiminnalliset tavoitteet.*

3.2 Tietoturvastrategian tutkimus

Tietoturvakirjallisuudesta löytyy suhteellisen vähän tutkimuksia, jotka ovat keskittyneet nimenomaan tietoturvastrategioihin. Tämä on yllättävää, sillä tietoturva voidaan nähdä ennemmin strategisena kuin teknisenä ongelmana. Tietojärjestelmien monimutkaistuessa ja hyökkäysmenetelmien kehittyessä motivoituneiden ja rahallista hyötyä tavoittelevien toimijoiden toimesta, hyökkäyksien tunnistaminen ja niiltä puolustautumisen voi muuttua yhä haastavammaksi. Usein rajallisista resursseista johtuen organisaatiot voivat tarvita strategisempaa lähestymistapaa tietoturvan toteutukseen kyetäkseen vastaamaan toimintaympäristön muutoksiin. Tässä alaluvussa käydään läpi merkittävimpiä tietoturvastrategiaan keskittyneitä tutkimuksia ja niiden löydöksiä.

Baskerville ja Dhillon (2008) mukaan hyvin kehitetty tietoturvastrategia voi auttaa ohjaamaan tietoturvapolitiikan kehitystä. Tietoturvapolitiikka puolestaan vaikuttaa suuresti organisaation tietoturvan hallintaan ja tietoturvaprosesseihin ja -käytäntöihin. Baskerville ja Dhillon (2008) mukaan strateginen lähestyminen tietoturvan hallintaan voi olla välttämättömyys organisaation tavoitteiden saavuttamiselle. Organisaatiossa tulisi olla selkeästi tiedossa roolit ja vastuut tietoturvaan liittyen (Baskerville & Dhillon 2008).

Anderson ja Choobineh (2008) pyrki tarkastelemaan tietoturvainvestointeja strategisesta näkökulmasta, ja mitkä tekijät vaikuttavat päätöksentekijöiden suosimiin strategioihin tietoturvainvestointeihin liittyen. Heidän mukaan tietoturvan strategisessa toteutuksessa tulisi pyrkiä tasapainottamaan tietoturvan hyödyt, kuten tietoturvatapahtumien vaikutusten minimointi, suhteessa tietoturvatoiminnan hintaan. Anderson ja Choobineh (2008) näkivät, että strategisesta näkökulmasta on tärkeää määrittää tietoturvan toteutukseen vaadittavat resurssit (mm. työntekijät, raha ja aika).

Park ja Ruighaver (2008) puolestaan määrittelivät strategian konseptina organisaation tietoturvan kontekstiin, lainaten strategian määritelmää liiketalous- ja sotatieteistä. Heidän mukaan tietoturvastrategiaa voidaan hyödyntää organisaation tietoturvaohjelman kehityksessä. He esittelivät viitekehyksen tietoturvastrategioiden luokitteluun, jonka avulla strategioita voidaan luokitella perustuen ajallisiin, paikallisiin tai päätöksentekoprosessin tekijöihin. Esimerkiksi ajalliset strategiat jakautuvat aktiivisiin ja proaktiivisiin strategioihin, joissa

uhkiin reagoidaan joko ennakoivasti tai vasta uhkan toteuduttua. Heidän viitekehyksen tarkoituksena oli myös auttaa tietoturvastrategioiden tehokkuuteen vaikuttavien tekijöiden arvioinnissa.

Ahmad, Maynard ja Park (2014) tarkastelivat kuinka organisaatiot implementoivat tietoturvastrategioita tietojärjestelmien suojaamiseksi. He havaitsivat, että useista erilaisista tietoturvastrategioista huolimatta, organisaatiot suosivat usein ehkäisyyn perustuvia strategioita tai käyttävät toisen tyyppisiä strategioita ehkäisyn näkökulmasta. Tämä oli perusteltavissa organisaatioiden pyrkimyksellä varmistaa järjestelmien saatavuus. (Ahmad ym. 2014) Heidän tutkimuksensa osoitti tarpeellisuuden lisätutkimukselle liittyen laajoihin koko organisaation kattaviin tietoturvastrategioihin, jotka yhdistävät useita eri strategioita tasapainoiseksi ja optimoiduksi kokonaisuudeksi. Kokonaisvaltainen tietoturvastrategia voi auttaa organisaatiota saavuttamaan tehokkaamman tietoturvan käytössä olevilla resursseilla.

Sveen, Torres ja Sarriegi (2009) pyrkivät ymmärtämään tietoturvan hallinnan strategioita sosioteknisten tietojärjestelmien hallinnassa, jossa ihmiset, organisaatio ja teknologia ovat vuorovaikutuksessa toisiinsa. Tutkijat pyrkivät kehittämänsä mallin avulla osoittamaan kuinka myös tietoturvakontrollit ovat vaikutuksessa toisiinsa. Tämän vuorovaikutuksen ymmärtäminen on edellytys toimiville tietoturvastrategioille. Proaktiivinen lähestyminen tietoturvaan voi auttaa organisaatiota parantaa muun muassa tietoturvakontrollien tehokkuutta ja riskienhallinnan prosesseja. (Sveen ym. 2009) Tietoturvastrategia on osa organisaation liiketoimintastrategiaa, jolla myös pyritään rakentamaan organisaation voimavaroja. On kuitenkin huomattava, että tietoturva ei välttämättä heijastu suoraan mittataviksi rahallisiksi hyödyiksi organisaatiossa, joka voi puolestaan rajoittaa tietoturvastrategian kontribuution ja tehokkuuden arviointia osana organisaation liiketoiminnan kehitystä. Lisäksi Sveen ym. (2009) tutkimus nosti esille tietoturvastrategian olemassaolon kykyä demonstroida organisaation asennoitumista tietoturvaa kohtaan. Esimerkiksi strategia voi kertoa organisaation pyrkimyksistä joko proaktiivisesti tai reaktiiviseen tietoturvan toteutukseen.

Kayworth ja Whitten (2010) puolestaan pyrkivät tarkastelemaan mikä on tehokkain lähestymistapa tai strategia tietoturvan toteutukseen. Heidän mukaan strategisesti linjattua tietoturvastrategiaa ohjaa sekä organisaation IT-infrastruktuuri että organisaation sisäiset tekijät (esim. kulttuuri). Tässä linjauksessa tulisi ottaa huomioon myös teknologian yhdenmukaisuus organisatoristen ja sosiaalisten tekijöiden kanssa.

Beebe ja Rao (2010) pyrkivät auttamaan organisaatioita kehittämään tehokkaampia tietoturvastrategioita mahdollistamalla heidän kehittämän mallin hyödyntämistä perinteisessä riskien hallinnassa. Beebe & Rao (2010) mukaan tyypilliset tietoturvastrategiat, jotka perustuvat pelkästään riskienhallintaan ja tietoturvastandardeihin eivät tuota aina parasta tulosta tietoturvan strategiseen toteutukseen. He pyrkivät osoittamaan empiirisen tutkimuksen kautta, kuinka heidän malli yhdistettynä riskienhallintaan voi tuottaa uusia tietoturvastrategioita, joihin pelkällä riskien hallinnalla ei kyetä. Tämä uusi lähestymistapa tietoturvan strategiseen suunnitteluun voi auttaa organisaatioita puolustautumaan yhä kehittyneempiä uhkia ja hyökkäyksiä vastaan.

Onibere, Ahmad & Maynard (2017) keskittyivät tarkastelemaan tietoturvapäällikön (CISO) roolia tietoturvan strategisessa suunnittelussa ja toteutuksessa. He listasivat CISO:lta vaadittavia ominaisuuksia, joita edellytetään tietoturvan strategiselta suunnittelijalta. Tutkijoiden mukaan organisaatiot tarvitsevat kokonaisvaltaisempaa ja tulevaisuuteen tähtäävää lähestymistapaa tietoturvan toteutukseen. Tietoturvastrategia voi auttaa tietoturvapäällikköä ohjamaan tietoturvan operatiivista toteutusta siten, että se ottaa huomioon myös organisaation liiketoiminnalliset tavoitteet ja päämäärät. Lisäksi tietoturvastrategia voi auttaa kommunikoimaan tietoturvan tarpeita ylimmän johdon, operatiivisen toiminnan ja loppukäyttäjien välillä.

Baskerville, Spagnoletti ja Kim (2014) keskittyivät tarkastelemaan kahden eri tietoturvastrategian - torjunnan ja reagoinnin vahvuuksia ja heikkouksia. Tutkimuksen pohjalta he esittivät, että organisaatiot tarvitsevat molempia strategioita kehittääkseen tehokkaan puolustusjärjestelmän. Siinä missä torjuntaan perustuvat strategiat ovat hyvin tunnettuja, niihin liittyy heikkouksia uhkien ja hyökkäysmenetelmien muuttuessa ja kehittyessä. Reagointiin perustuvat strategiat eivät yleensä vaadi uhkien ennakoivaa tunnistusta, jolloin organisaatio kykenee reagoimaan myös uusiin ja aiemmin tunnistamattomiin uhkiin. Näiden kahden strategian tyypin yhdistäminen toimivaksi kokonaisuudeksi voi vaatia erillisen strategian, jotta tavoitellut hyödyt kyetään saavuttamaan.

Nämä edellä esitellyt tutkimukset ovat tärkeitä edistyksiä tietoturvastrategioihin liittyvässä tutkimuksessa. Tästä huolimatta ne eivät kykene vastaamaan tämän tutkimuksen tutkimuskysymykseen, sillä ne tarkastelevat vain tiettyä osa-aluetta kokonaisvaltaisesta tietoturvastrategiasta. Kokonaisvaltaisella ylemmän tason strategialla voidaan kyetä saavuttamaan kustannustehokas puolustusjärjestelmä yhdistelemällä eri strategioiden vahvuuksia kokonaisuudeksi, joka pyrkii ylläpitämään ja edistämään organisaation tietoturvaa suhteessa liiketoiminnallisiin tavoitteisiin. Lisäksi tietoturvakirjallisuudesta ei löydy viitekehystä, joka olisi kerännyt yhteen kaikki organisaatiossa huomioitavat tekijät, jotka tulisi huomioida kokonaisvaltaisen tietoturvastrategian kehityksessä ja arvioinnissa. Tämä tutkimus pyrkii vastaamaan tähän tarpeeseen kirjallisuuskatsaukseen avulla, ja kehittämään viitekehyksen joka voi auttaa tietoturvastrategioiden tarkastelussa – tieteellisestä ja käytännöllisestä näkökulmasta.

4 KIRJALLISUUSKATSAUS

Kirjallisuuskatsauksen avulla pyrimme tunnistamaan aiemmasta kirjallisuudesta huomioitavia tekijöitä, jotka ovat edellytys toimivalle tietoturvastrategialle. Kirjallisuuskatsauksessa käytetty aineisto kerättiin tekemällä hakuja Web of Science palveluun, josta on mahdollista hakea vertailuarvioituja tieteellisiä artikkeleja. Hakutulokset rajattiin tietojärjestelmä- ja tietojenkäsittelytieteiden julkaisuihin. Hakuja tehtiin termeillä ”security strateg*” ja ”security governance”. Hakutermi ”security strateg*” kattoi artikkelit, joissa puhuttiin tietoturvastrategiasta yksikössä tai monikossa. Hakutermiä ”security governance” käytettiin aineiston haussa, koska tietoturvastrategian määritys on nähty yhtenä vaiheena tietoturvahallinnon perustamisessa organisaatioon (Carcary ym. 2016; Damenu & Beaumont 2017; Karanja 2017) Hakutuloksista tunnistettiin tutkimusaiheen kannalta keskeiset artikkelit, joissa käsiteltiin tietoturvastrategiaa tai puhuttiin tutkimuksen strategisista implikaatioista. Lisäksi tutkimuksessa hyödynnettiin oleellisia artikkeleita, joihin haun tuloksena saadut artikkelit olivat viitanneet.

Kirjallisuuskatsauksen pohjalta luotiin viitekehys, jota hyödynnetään tämän tutkimuksen empiirisessä osuudessa, tutkimuksen pyrkiessä määrittämään terveydenhuoltosektorilla toimivien tietoturvastrategioiden ominaisuuksia. Vastaavanlaista viitekehystä ei löydy aiemmasta kirjallisuudesta.

4.1 Huomioitavat tekijät

Organisaation olisi ymmärrettävä omaa toimintaympäristöä ja sisäisiä tekijöitä kyetäkseen luomaan toimiva tietoturvastrategia omaan käyttöön. Huomioimalla näitä ulkoisia ja sisäisiä tekijöitä organisaatio voi pyrkiä varmistamaan tietoturvan liiketoimintaa tukevat hyödyt.

4.1.1 Ulkoiset tekijät

Ulkoisista tekijöistä organisaation olisi hyvä huomioida sekä lainsäädännön että parhaiten käytäntöjen asettamia tietoturvavaatimuksia. Näiden vaatimusten aiheuttama ulkoinen paine on todettu vaikuttavan enemmän organisaation ylimmän johdon päätöksentekoon kuin sisäiset tekijät (Barton ym. 2016).

Lait ja säädökset toimivat usein suurimpana motivaatiotekijänä organisaation tietoturvan kehittämiselle. Lain noudattamatta jättämisen negatiivisten seurausten, kuten maineen menetys ja rahallisten sanktioiden pelko ajaa organisaatioita investoimaan tietoturvaan (Sveen ym. 2009; Kwon & Johnson 2013). Tämän lainsäädännön tarkoituksena on yleensä varmistaa tietoturvan minimitaso ja suojella loppukäyttäjää tietovuodon aiheuttamilta seurauksilta. Tästä johtuen lait tulee ottaa huomioon tietoturvan toteutukselta, jotta organisaatio kykenee varmistamaan toiminnan lainmukaisuuden ja suojaamaan loppukäyttäjää.

Lakien noudattaminen voi auttaa uudempia organisaatioita tietoturvan kehityksessä, mutta kehittyneemmille organisaatioille toiminnan tavoitteena tulisi olla tietoturvan saavuttaminen, samanaikaisesti pyrkien varmistamaan toiminnan lainmukaisuus (Kwon & Johnson 2014). Lain- tai säädösten ei ole kustannustehokkain vaihtoehto tietoturvan toteutuksessa, sillä tehokas tietoturva vaatii enemmän kuin vain tekniset kontrollit lainmukaisuuden varmistamiseksi (Doherty & Fulford 2006).

Posthumus ja Solms (2004) nostivat esille, kuinka tietoturvan hallinnossa tulisi huomioida tietoturvastandardien ja parhaisiin käytäntöjen (best practices) liittyvät vaatimukset, sillä ne tarjoavat laajan valikoiman yleisesti hyväksyttyjä ohjeita tietoturvan toteutukseen. Tästä syystä ne ovat hyvä tietolähde tietoturvan pohjaksi. Organisaation tietoturvastrategioissa nämä ohjeet olisi suhteutettava lakeihin ja säädöksiin, IT-infrastruktuurin ja liiketoimintaan.

Näiden ohjeiden tärkeydestä huolimatta tietoturvakirjallisuudessa on nostettu esille lain- tai standardinmukaisuuden riittämättömyys tehokkaan tietoturvajärjestelmän saavuttamiselle. Ne voivat toimia erinomaisena tietolähteenä tietoturvan toteutukselle ja tietoturvan minimitason saavuttamiselle (Sveen ym. 2009), mutta "raksiruutuun"-lähestymistapa tietoturva ei välttämättä tarjoa riittävää puolustusta uhkien ja teknologioiden hyvinkin nopean kehityksen seurauksena. Esimerkiksi tietoturvastandardien kehitys- ja hyväksymisprosesseista johtuen, standardit voivat kulkea jäljessä ajantasaisesta tietoturvasta (Sveen ym. 2009)

Lain- ja standardinmukaisuuteen pyrkiminen voi ajaa organisaation kohti reaktiivista suhtautumista tietoturvaan (Kwon & Johnson 2014). Lisäksi varsinkin tietoturvastandardien heikkoudeksi voidaan nähdä niiden yleisluontoinen suhtautuminen tietoturvaan (Flores ym. 2014). Tästä johtuen ne eivät kohdistu tietylle alalle, vaikka toimintaympäristö voi vaikuttaa suuresti tietoturvan toimivuuteen rajallisilla resursseilla. Lisäksi standardit kiinnittävät vähän huomiotta organisaatioiden kulttuurisiin tekijöihin.

Standardien ja parhaiden käytäntöjen tarjoaman tietolähteen ja lainmukaisuuden laiminlyönnin aiheuttamat sanktiot tekevät niistä tärkeitä huomioitavia tekijöitä organisaatioiden tietoturvastrategiassa. Tietoturvanstrategioiden suunnittelussa tulisi kuitenkin välttää pelkästään lain- tai standardinmukaisuuteen pyrkimistä. Sen sijaan strategiassa tulisi pyrkiä asettamaan tietoturva toiminnan tavoitteeksi, ja huomioida nämä ulkoiset tekijät mahdollisina tieto- ja riskilähteinä.

4.1.2 Tietojärjestelmät

Historiallisesti tietoturvastrategioita on ohjannut vahvasti teknologiset tekijät, kuten käytetyt ohjelmat ja muut järjestelmät. Tästä syystä myös tietoturva on usein pyritty toteuttamaan erilaisilla teknologioilla huomioimatta mm. työntekijöitä osana tietojärjestelmää (Kayworth & Whitten 2012).

Organisaation IT-infrastruktuurin huomioiminen tietoturvan toteutuksessa on tärkeää sillä se määrittää käytössä olevat teknologiat osana organisaation arvonluontiprosesseja. Nämä teknologiat voivat sisältää haavoittuvaisuuksia, joita hyökkääjät voivat pyrkiä hyödyntämään.

Teknologian tärkeydestä huolimatta organisaatiossa tietoturva tulisi toteuttaa huomioiden sekä teknologia, prosessit että ihmiset osana suojaattavaa tietojärjestelmää (Da Veiga & Eloff 2007). Vaikka teknologiset tietoturvakontrollit ovat välttämättömyys, ne eivät riitä tietoturvan saavuttamiseen näissä usein monimutkaisissa ja muuttuvissa sosioteknisissä järjestelmissä (Williams, Hardy & Holgate 2013). Ihmiset ovat usein lähteenä tietoturvauhkille, joko tahallisen tai tahattoman toiminnan seurauksena. Tämän vuoksi tekniset tietoturvakontrollit tarvitsevat rinnalleen ei-teknisiä ratkaisuja, kuten tietoturvapolitiikat ja tietoturvakoulutusta sosiaalisen kontekstin huomioimiseksi puolustusjärjestelmässä (Damenu & Beaumont 2017).

Tietoturvan hallinnassa on siirrytty kohti kokonaisvaltaisempaa lähestymistapaa, jossa pyritään ottamaan huomioon sekä teknologiset, organisatoriset ja sosiaaliset tekijät (Kayworth & Whitten 2010). Tämä kokonaisvaltainen lähestymistapa korostaa ihmisten huomioimista osana organisaation tietoturvan toteutusta. Muun muassa asenteilla, normeilla, käyttäytymisellä, johtamisella ja kulttuurilla on oma vaikutuksensa tietoturvaan (Flores, Antonsen & Ekstedt 2014).

Tietoturvastrategian tulisi ottaa huomioon teknologian lisäksi sekä ihmiset että prosessit, sillä ne ovat usein lähteenä potentiaalisille tietoturvauhkille (Furnell & Clarke 2012; Horne ym. 2017). On kuitenkin huomattava, että tietojärjestelmien ihmiselementin arviointi ja sitä kautta huomioiminen on usein haastavaa, johtuen muun muassa sen mittaamisen haasteellisuudesta (Furnell & Clarke 2012). Esimerkiksi aikomus noudattaa tietoturvapolitiikkaa voi erota todellisesta toiminnasta.

Sveen ym. (2009) mukaan tietojärjestelmien tietoturva tulisi miettiä sosioteknisestä näkökulmasta, jossa sosiaaliset, organisatoriset ja teknologiset tekijät vaikuttavat toisiinsa. Sosioteknisestä luonteesta johtuen myös tietoturvakontrollien (teknisiä, virallisia tai epäviralliset) välisiä vaikutussuhteita tulisi ymmärtää. (Sveen ym. 2009) Näiden vaikutussuhteiden olemassa olon huomiotta jättäminen voi johtaa tehottomiin tietoturvastrategioihin, ja yhteistyön ongelmiin johdon ja työntekijöiden välillä.

Siinä missä tekniset kontrollit ovat yleensä nopeita implementoida tietoturvakulttuurin rakentaminen organisaatioon voi viedä vuosia (Sveen ym. 2009). On kuitenkin huomattava, että tietoturvakulttuuri voi tarjota organisaatiolle pitkäaikaisemman suojan kuin tekniset kontrollit, jotka vaativat jatkuvaa tarkkailua ja päivitystä suojaustehon ylläpitämiseksi.

Organisaation olisi kyettävä integroimaan tietoturvapolitiikka, liiketoimintaprosessit ja liiketoimintastrategia yhtenäiseksi kokonaisuudeksi (Oshri, Kotlarsky, Hirch 2007). Tietoturvastrategia voi ohjata tätä tavoitetta pyrkien samalla varmistaa tasapaino järjestelmien käytettävyyden ja tietoturvan välillä.

Yleinen virhe organisaatioissa on kehittää tietoturvastrategia, -politiikka ja -prosessit huomioimatta organisaation kulttuuria. (Damenu & Beaumont 2017) Kulttuurilla voi olla suuri vaikutus käytetyn tietoturvakontrollien toimivuuteen.

4.1.3 Kulttuuri

Monimutkaiset sosioteknisten tietojärjestelmien tietoturva vaatii toimiakseen oikeanlaisen tietoturvakulttuurin. (Damenu & Beaumont 2017) Organisaation kulttuuri muodostuu ajan kuluessa organisaation strategian, hallintajärjestelmien ja työntekijöiden käyttäytymisen seurauksena. Tietoturvakulttuuri muodostuu organisaatioon, sen valittujen ja toteutettujen toimenpiteiden seurauksena (Da Veiga & Eloff 2007), jonka vuoksi tietoturvastrategialla voidaan nähdä olevan tärkeä rooli tietoturvakulttuurin kannalta.

Tietoturvakulttuuria ei tulisi tarkastella erillään muusta organisaation muusta kulttuurista, sillä ne vaikuttavat toisiinsa (Ruighaver, Maynard & Chang 2007). Lisäksi organisaation tulisi pyrkiä hallinnoimaan tietoturvan toteutusta siten, että kaikki tarvittavat tietoturvakomponentit, kuten tietoturvakontrollit ja prosessit on implementoitu organisaation riittävän tietoturvakulttuurin aikaansaamiseksi (Da Veiga & Eloff 2007).

Aiemmassa kirjallisuudessa on tunnistettu muuttujia, jotka vaikuttavat tietoturvakulttuurin muodostumiseen. Nämä muuttujat ovat informaatioteknologia, tietoturvastandardit, organisaatiossa koetut tietoturvariskit, uhkat ja haavoittuvaisuudet, työntekijöiden motivaatio, koetut roolit ja vastuut (Damenu & Beaumont 2017).

Ylimmän johdon olisi kyettävä kommunikoimaan tietoturvakulttuuria ja sen merkitystä alaspäin organisaatiossa, sillä kulttuuri vaikuttaa työntekijöiden tietoturva käyttäytymiseen (Da Veiga & Eloff 2007). Ylimmän johdon tuki tietoturvan toteutukselle voi toimia ennustavana tekijänä tietoturvakulttuurin kehityksen suunnalle. Tietoturvan prioriteetin määritys ja tietoturvan ongelmien huomioiminen strategisissa suunnitelmissa kommunikoi eri sidosryhmille tietoturvan merkitystä organisaatiossa.

Tietoturvakulttuurin kehittäminen ja työntekijöiden hyödyntäminen osana organisaation kokonaispuolustusta vaatii tietoturva hallinnolta kykyä saada työntekijät ymmärtämään oman roolinsa organisaation voimavarojen turvaamisessa (Da Veiga & Eloff 2007). Työntekijöiden tietoturvakäyttäytymistä olisi kyettävä seuraamaan ja ohjaamaan pyrittäessä kohti tietoturvatavoitteita.

Tietoturvakulttuurin kehittäminen on kuitenkin usein haastavaa, sillä se vaatii kaikkien työntekijöiden ja muiden sidosryhmien osallistumista kulttuurin kehittämiseen (Kwon & Johnson 2012). Organisaation tulee varmistaa tietoturvan kulttuurinen sopivuus omaan organisaatioon. (Kayworth & Whitten 2012) Kulttuurinen konflikti voi tulla esille tilanteissa, joissa tieturvan arvot ovat ristiriidassa organisaation työntekijöiden arvojen kanssa. Ristiriidan seurauksena työntekijät voivat jättää huomiotta esimerkiksi tietoturvapolitiikan ja -prosessienvaatimukset toimiakseen omien ammatillisten arvojen mukaisesti (Hedström ym. 2011).

Organisaatio voi pyrkiä yhdenmukaistamaan liiketoimintaa tietoturvan kanssa luomalla kulttuuria, joka korostaa tietoturvan arvoa ja tärkeyttä organisaation tavoitteiden kannalta (Kayworth & Whitten 2012). Tietoturvan toteutusta voidaan tukea organisaation arvoilla. (Kwon & Johnson 2013) Lisäämällä työntekijöiden tietoturvatietoisuutta ja parantamalla heidän motivaatiota toimia tietoturvapolitiikan mukaisesti, voi organisaatio pyrkiä tietoturvan tehokkuuteen ja lainmukaisuuteen käytössä olevilla resursseilla.

4.1.4 Liiketoiminnalliset tarpeet

Tietojärjestelmäkirjallisuudessa on kiinnitetty paljon huomiota liiketoiminta- ja IT-strategian yhdenmukaisuuden tarpeellisuudelle (Chen ym. 2010), mutta näiden strategioiden yhdenmukaisuus tietoturvastrategian kanssa on saanut suhteellisen vähän huomiota (McFadzean ym. 2011). Tietoturvakontrollit usein vaikuttavat suoraan järjestelmien käytettävyyteen, sillä ne pyrkivät estämään potentiaalisten riskien toteutumista, esimerkiksi ylimääräisten varmennusvaiheiden avulla. Tämä voi puolestaan vaikuttaa organisaation arvonluonti prosesseihin. Tästä syystä liiketoiminnan tarpeiden huomiotta jättäminen tietoturvastrategiassa voi johtaa organisaation epäonnistumiseen.

Tietoturvastrategia tulisi olla linjassa liiketoiminta- ja IT-strategian kanssa, jotta myös tietoturvassa kyetään huomioimaan organisaation todelliset liiketoiminnalliset tarpeet estämättä liiketoiminnan strategista ja operatiivista toimintaa (McFadzean, Ezingeard & Birchall 2007; Flores ym. 2014). Huomioimalla liiketoiminta- ja IT-strategian tietoturvastrategiassa voidaan liiketoiminnan lyhyen ja pitkän aikavälin tavoitteet todennäköisemmin saavuttamaan (Da Veiga & Eloff 2007).

Liiketoimintastrategia on ensisijainen strategia, jota ilman organisaation on lähes mahdotonta toimia. Se sisältää organisaation vision tulevaisuudesta ja tavoitteet, jotka saavuttamalla organisaation kykenee selviytymään ja kasvamaan omassa toimintaympäristössä. Tietoturvastrategia voidaan nähdä välttämättömyydeksi organisaatiolle, joka haluaa saavuttaa kustannustehokkaan tiedon turvaamisen (Ahmad ym. 2014).

Myös Posthumus ja Solms (2004) korosti liiketoiminnan huomioimista tietoturvassa, sillä organisaation tarpeet vaikuttavat yleisiin tietoturvatavoitteisiin ja keinoihin suojata tärkeimmät voimavarat. Voimavarojen saatavuus ja luottamuksellisuus ovat edellytys arvonluontiprosesseille (Posthumus & Solms 2004). Jotta organisaatio kykenee saamaan hyötyä tietoturvainvestoinneista, tulee tietoturvastrategian olla linjassa liiketoiminnallisten tavoitteiden kanssa (Karanja 2017).

Tietoturvan merkityksen kasvaessa se nähdään yhä enemmän strategisena investointina liiketoimintaan kuin vain pakollisena kuluna IT:n toteutuksessa (Herath ym. 2010). Tämän myötä myös investointien strategisen suunnittelun merkitys kasvaa. Päättäjien olisi kyettävä arvioimaan auttaako tietoturvainvestointi organisaation päämäärien ja tavoitteiden saavuttamisessa.

Tietoturvastrategia vaatii ylimmän johdon tuen (Horne ym. 2017). Tietoturvastrategian voi ohjata ja varmistaa riittävän budjetin tietoturvan toteutukseen, jolloin operatiiviseen toimintaan saadaan riittävät resurssit. Tämä on tärkeää, sillä tietoturvalle on harvoin määritetty erillinen budjetti IT:n operatiivisesta toteutuksesta.

Valitut strategiat vaikuttavat tietoturvan investointikohteisiin. Esimerkiksi estämiseen perustuvat strategiat vaativat investointeja tunnistettujen riskien ehkäisyyn (esim. palomuuri tai tietoturvapolitiikka), kun taas reagointikykyyn perustuva strategia pyrkii vastaamaan tunnistamattomiin uhkiin, esim. ylläpitämällä resursseja tietoturvatapahtumien reaaliaikaiseen tunnistukseen (esim. SOC- ja IDS-ratkaisut). Päätöstentekijöiden olisi kyettävä suhteuttamaan tietoturvan höydyt suhteessa sen hintaan (Anderson & Choobineh 2008). Tässä tietoturvastrategia voi auttaa varmistamalla näiden investointien hyöty myös koko liiketoimintaan.

Organisaation tulee tasapainottaa tietoturva suhteessa liiketoiminnallisiin tavoitteisiin. (Kayworth & Whitten 2012) Liiketoimintaprosessien tulisi olla mahdollisia ilman, että voimavaroille aiheutuu tarpeetonta riskiä. Tästä syystä tietoturvastrategian tulisi olla liiketoiminnan määräämä, ja pyrkien turvaamaan arvonluontiprosessien kannalta keskeiset voimavarat, kuten tieto, prosessit, teknologia ja työntekijät.

4.1.5 Riskit

Tyypilliset organisaatioiden tietoturvastrategiat perustuneet vahvasti riskienhallinnan prosesseihin, joissa hyödynnetään tietoturvastandardeja tietolähteenä (esim. ISO27000-standardit). (Beebe & Rao 2010) Tyypillisesti nämä strategiat pyrkivät tekemään tietoturvaloukkausten toteutuksen mahdollisimman haastavaksi ja lisäämään kiinnijäämisen todennäköisyyttä. Nämä ehkäisevät ja tunnistavat tietoturvastrategiat ovat tärkeitä, mutta ne eivät aina riitä tehokkaimman puolustuksen saavuttamiseen rajallisilla resursseilla.

Muun muassa kohdennetut ja erittäin motivoidut hyökkäykset luovat haasteen ehkäisyyn pyrkiville tietoturvastrategioille (Baskerville ym. 2014). Tietoturvastrategiat ovat keino reagoida organisaation voimavaroihin kohdistuviin riskeihin. Kaikkien riskien tunnistaminen ja arviointi voi kuitenkin olla haastavaa jatkuvasti muuttuvasta teknologioista ja niihin liittyvistä uhkista johtuen.

Lisäksi riskienhallintaan liittyy ongelmia, jotka johtuvat muun muassa riskienhallinnan pohjalla toimivan tiedon ja sen tulkinnan subjektiivisuudesta. (Taylor 2015) Esimerkiksi uhkien toteutumisen todennäköisyys ja toteutuneiden uhkien vaikutusten ennustaminen objektiivisesti on lähes mahdotonta. Riskiarvioon perustuva tieto on usein subjektiivista ja arvion tulos perustuu arvioijan näkemykseen riskeistä. Lisäksi on huomioitava, että arvioitaessa riskejä, arvioija luottaa usein ennemmin omaan näkemykseen kuin todelliseen tietoon (Taylor 2015). Tämän vuoksi riskiarvion tulos on usein valistunut arvaus.

Päätöksenteko riskienhallintaan liittyen on yleensä strategista, jolloin päätetään muun muassa mitä riskejä pyritään hallitsemaan, millä keinoilla

ja kuinka paljon resursseja tähän toimintaan on varattu (Beebe & Rao 2010). Strategian luottaminen pelkästään riskiarvioon voi olla ongelmallista, sillä uhkat korkeimmalla riskipisteytyksellä saa suurimman prioriteetin ja näin suurimman huomion tietoturvan toteutuksessa. Mikäli riskiarvio on perustunut virheelliseen näkemykseen riskistä, organisaatio voi hukata resursseja väärän voimavaran suojaukseen.

Olemassa oleva tietoturvastrategia voi auttaa välttämään tarpeen mukaan (ad-hoc) implementoituja tietoturvastrategioita uusien uhkien hallintaan. Nopeasti implementoidut strategiat eivät välttämättä ota systemaattista lähestymistapaa ja mahdollisesti jättävät huomiotta organisaation pitkäaikaiset tavoitteet ja liiketoiminnan (Ahmad ym. 2014). Tämän vuoksi ennakoiva ylemmän tason tietoturvan strateginen suunnittelu voi ehkäistä subjektiivisuus riskienhallinta prosesseissa.

Riskienhallinta tuottaa tärkeää tietoa potentiaalisista uhkista, jotka huomioimalla tietoturvastrategiassa tarvittavia tietoturvakontrolleja kyetään määrittämään. Järjestelmien monimutkaistuessa ja hyökkääjien toimiessa arvaamattomasti potentiaalisten uhkien tunnistaminen on yhä hankalampaa, vaikuttaen myös riskienhallinnan tehokkuuteen (Baskerville ym. 2014). Tämän vuoksi riskienhallintaan perustuvat strategiat voivat tarvita rinnalleen uusia reagointikykyyn nojautuvia strategioita.

Puhtaasti riskien motivoima tietoturvastrategia voi olla ongelmallinen, sillä mikäli organisaatio ei kykene tunnistamaan ja mittaamaan oleellisia riskejä, se on kykenemätön ohjaaman riittäviä resursseja näiden riskien hallintaan (Sveen ym. 2009). Lisäksi jatkuvasti muuttuva informaatioteknologia ja sen infrastruktuuri asettaa haasteen uhkien tunnistukselle ja sitä kautta hankaloittaa riskienhallintaa (Neghime & Scarlat 2013).

Riskienhallinnalla on strateginen merkitys organisaatiossa, sillä siihen liittyy arviointi riskin ja hyödyn välillä. (Anderson & Choobineh 2008) Organisaation olisi kyettävä vastaamaan kysymykseen, mikä on optimaalinen tietoturvabudjetti koko organisaation kattavan tietoturvan toteutukseen, ottaen samalla huomioon tietoturvan vaatimukset ja sen hinta. Tähän päätöksentekoprosessiin vaikuttaa kuitenkin useat tekijät, kuten saatavalla olevan tiedon määrä ja laatu uhkista, haavoittuvaisuuksista, uhkien todennäköisyyksistä ja vaikutuksista. (Anderson & Choobineh 2008) Lisäksi ylemmän johdon päätöksentekoon vaikuttaa heidän kokemat vastuut ja riskiensietokyky. Tietoturvastrategia voi osaltaan auttaa ohjaamaan päätöksentekoa riskienhallintaan liittyen ja varmistaa riittävät oikein ohjatut resurssit tietotototurvan toteutukseen.

4.2 Tavoitteet ja niiden mittaaminen

Tietoturvastrategian määritelmään perustuen tietoturvastrategian tärkeimmäksi tavoitteeksi voidaan nähdä organisaation tietoturvan ylläpito ja kehittäminen. Tähän tavoitteeseen voidaan päästä implementoimalla suunnitelmallisesti teknisiä, virallisia ja epävirallisia kontrolleja suhteessa riskeihin ja liiketoiminnan tavoitteisiin. Investoimalla strategisesti tietoturvaan ja kehittämällä organisaation

tietoturvakulttuuria, organisaatio voi kyetä kehittää omaa tietoturvaa kokonaisvaltaisesti. Systemaattinen ja kokonaisvaltainen lähestymistapa tietoturvaan auttaa organisaatiossa huomioimaan sen sisäisiä tekijöitä, ja kehittämään kulttuuria haluttuun suuntaan.

Tietoturvastrategiaa voidaan hyödyntää tietoturvapolitiikan arvioinnissa ja kehityksessä, mahdollistaen yhteneväisen tietoturvan koko organisaatiossa (Baskerville & Dhillon 2008). Yhtenäinen tietoturva auttaa organisaatiota kohti proaktiivisempaa tietoturvaa, jolloin tietoturvauhkiin kyetään varautumaan ennen niiden toteutumista. Proaktiivinen tietoturva on todettu olevan jossain tapauksissa kustannustehokkaampi verrattuna reaktiiviseen tietoturvaan (Kwon & Johnson 2013).

Reaktiivisesti tietoturvaan suhtautuva organisaatio voi tietoturvaloukkausten seurauksena reagoida tapahtumiin ottamatta huomioon organisaation liiketoiminnallisia ja tietoturvan pitkän aikavälin tarpeita. Tämä voi johtaa mahdollisesti tehottomiin tai jopa tarpeettomiin tietoturvainvestointeihin. Uutisointi tietoturvaloukkauksista tai teknologioiden haavoittuvaisuuksista voi auttaa rahoituksen saamisessa tietoturvatoimintaan. Tästä huolimatta organisaation olisi kuitenkin kyettävä jatkuvaan tietoturvan kehitykseen, riippumatta siitä ilmeneekö mahdollisia uhkia toimintaympäristössä tietyllä ajanhetkellä.

Tietoturvatapahtuma voi tehdä organisaation tietoiseksi oman tietoturvajärjestelmän puutteista, ja toisaalta tietoturvatapahtumien puute voidaan tulkita tietoturvajärjestelmän tehokkuudeksi. On kuitenkin huomattava, että tietoturvatapahtumien puute voi johtua myös uhkien puutteesta tietyllä ajanhetkellä tai organisaation kyvyttömyydestä havaita hyökkäyksiä.

Tietoturvastrategia voi mahdollisesti auttaa organisaatiota varmistamaan jatkuvan tietoturvan huomioimisen liiketoiminnassa. Näin voidaan varmistaa sekä johdontuki, että riittävät resurssit tietoturvan toteutukseen. Tietoturvan budjetti on usein sidottu osaksi IT-budjettia, jolloin IT-investoinnit voivat saada suuremman painoarvon niiden tarjoamista rahallisista hyödyistä johtuen.

Tietoturvastrategia voi toimia kommunikaation työkaluna muun muassa ylimmän johdon ja operatiivisen toiminnan välillä. Sen avulla organisaatio voi kyetä demonstroimaan omaa sitoutumista tietoturvaan ja sen kehitykseen kaikille sidosryhmille. Saavuttamalla tietoturvastrategian mukaisia tavoitteita organisaatio voi osoittaa muutoksen tietoturvaan liittyen. Tämä voi auttaa halutun tietoturvakulttuurin aikaansaamisessa ja toteutettujen tietoturvainvestointien arvioinnissa.

Tietoturva hallinnon tulisi varmistaa tietoturvastrategian yhdenmukaisuus liiketoimintastrategian, riskienhallinnan, resurssienhallinnan, suorituskyvynmittauksen ja organisaation arvonluonnin välillä (Karanja 2017). Kayworth ja Whitten (2012) mukaan tehokas tietoturva on liiketoiminnan määräämä ja strategisesti keskittynyt. Tietoturvastrategia voi auttaa tämän tavoitteen saavuttamisessa ja varmistaa että tietoturva ei toimi erillään liiketoiminnasta.

Tietoturvastrategian suunnittelussa tulisi huomioida tietoturvan keskeiset tavoitteet, kuten tietoturvan lainmukaisuus. (Horne ym. 2017) Tehokas tietoturvastrategia suhtautuu tietoturvaan proaktiivisesti tunnistaen uhkia ennakoivasti. Riskienhallinnalla on keskeinen rooli näiden uhkien tunnistuksessa ja

niiltä puolustautumisessa (Taylor 2015). Lisäksi huomioimalla useita edellä esiteltyjä ulkoisia ja sisäisiä tekijöitä tietoturvastrategiassa, organisaatio voi pyrkiä kohti mahdollisimman kustannustehokasta tietoturvajärjestelmää.

Strategisten tietoturvatavoitteiden saavuttamisen arviointiin organisaatiot tarvitsevat erilaisia mittareita, joiden avulla muutoksen seuraaminen on mahdollista. Strategian pyrkiessä tiettyihin tavoitteisiin, niihin pääsemisen arviointi vaatii mittareiden olemassa oloa, jotta alkutilaa kyetään vertaamaan lopputulokseen, johon on päästy strategian toteutuksella.

Mittarit kuten Balanced score card voi auttaa motivoimaan organisaatiota kohti muutosta ja strategisia tavoitteita. (Harath ym. 2010) Tietoturvan strategiset tavoitteet olisi kyettävä muuttamaan tavoitteiksi ja niiden mittareiksi, jotka mahdollistaisivat toiminnan mittauksen operatiivisella tasolla, esimerkiksi yksilötasolla.

Pidemmän aikavälin tavoitteiden pyrkimyksenä on varmistaa suurempi organisaation muutos (esim. tietoturvakulttuurin suhteen) 3-5 vuoden aikavälillä. (Harath ym. 2010) Nämä pitkän aikavälin tavoitteet tulisi olla yhteydessä tavoiteltuun päämäärään, esimerkiksi organisaation visioon. Jotta suurempi organisaation muutos on mahdollinen, ylemmän johdon olisi kyettävä sitoutumaan valittujen mittareiden käyttöön. Nämä mittarit voivat mitata rahallista (esim. tietoturvatapahtuman suorat rahalliset vaikutukset) tai aineetonta muutosta (esim. työntekijöiden tietoturvatietoisuus).

Erilaisia mittareita tulisi sisällyttää eri osa-alueisiin liittyen, kuten liiketoimintaan, sidosryhmiin, sisäisiin prosesseihin ja tulevaisuuteen liittyen. Esimerkkejä tietoturvastrategian mitattavista alueista voivat olla riskienhallinta, tavoitteiden saavuttaminen ja tietoturvaprosessien laatu (Horne ym. 2017). Huomioimalla ja mittaamalla useita eri osa-alueita voidaan välttää tietoturvan keskittymistä tiettyyn toimintaan, operatiivisen toiminnan pyrkiessä saavuttamaan mittareille asetetut tavoitteet. Lisäksi on tärkeää mitata suoraan tietoturvastrategiaan liittyviä muuttujia (Horne ym. 2017).

4.3 Yhteenveto ja viitekehys

Perustuen edellä esitettyyn kirjallisuuskatsaukseen ja sen löydöksiin, tässä alaluvussa esitellään teoreettinen viitekehys tietoturvastrategiassa huomioitaville tekijöille, katso kuvio 2. Tätä viitekehystä tullaan hyödyntämään tämän tutkimuksen aineiston keräyksessä ja analysoinnissa.

Organisaation tulisi huomioida useita tekijöitä sen toimintaympäristöstä ja organisaation sisältä päättäessään kehittää tietoturvastrategia ohjaamaan tietoturvan toteutusta ja kehitystä. Tämä mahdollistaa tietoturvan toiminnan liiketoiminnan mahdollistajana. Tietoturvastrategia voi mahdollistaa tasapainon muun muassa tietoturvan ja käytettävyyden välillä, jolloin esim. tietoturvaprosessit eivät estä organisaation arvonluontiprosesseja. Tietoturvastrategiaa voidaan hyödyntää tietoturvaohjelman kehityksessä, mutta tämän tyypillisesti edellyttää liiketoimintastrategian huomioinnin tietoturvastrategiassa. (Ahmad ym. 2014)

Tietoturvastrategia voi varmistaa tietoturvan johtamisen ylhäältä alaspäin, jolloin liiketoiminnalliset tarpeet tulee huomioiduksi suhteessa toimintaan (Ahmad ym. 2014). Huomioimalla liiketoiminnalliset prosessit ja tavoitteet voidaan varmistaa tietojärjestelmien käytettävyys loppukäyttäjille. Lisäksi huomioimalla organisaation kulttuurin, tietoturvastrategia voi ohjata tietokulttuurin kehitystä haluttuun suuntaa, muun muassa implementoimalla kulttuuriin soveltuvia tietoturvakontrolleja, ja auttaa tietoturvapolitiikan kehittämisessä. Kulttuurin kehittäminen vie aikaa, jonka vuoksi organisaation on kyettävä sitoutumaan pitkäksi aikaa tämän tavoitteen saavuttamiseksi.

Organisaation olisi kyettävä mittaamaan strategisesti tärkeitä tietoturvan osa-alueita, jotta strategialla aikaansaatua muutosta kyetään seuraamaan. Käytetyillä mittareilla on mahdollista muun muassa kommunikoida tietoturvan merkitystä ja motivoida työntekijöitä tietoturvaan liittyen. Mittarit tarjoavat myös uuden tavan arvioida mahdollisten tietoturvainvestointien hyötyjä. Esimerkiksi mikäli tietoturvapolitiikkaa ja sen soveltuvuutta ei arvioida on haastavaa saavuttaa ja ylläpitää tehokasta tietoturvakulttuuria, joka kykenisi vastaamaan toimintaympäristön muutoksiin ja uusiin uhkiin (Flores ym. 2014).

Tietoturvakulttuurin arvioiminen erilaisten mittareiden avulla voi olla tarpeellista, sillä kulttuurin kehittäminen vaatii ymmärrystä sen monimuotoisesta ja dynaamisesta luonteesta, sekä sitoutumista kulttuurisen muutoksen aikaansaamiseksi (Damenu & Beaumont 2017). Lisäksi on huomioita, että mikäli organisaatio ei seuraa ja arvioi mitä tietoturvaloukkauksia organisaatiossa tapahtuu ja miksi ne tapahtuvat, organisaation on haastavaa arvioida tietoturvastrategian toimivuutta, ja sitä kuinka näitä strategioita voitaisiin parantaa.

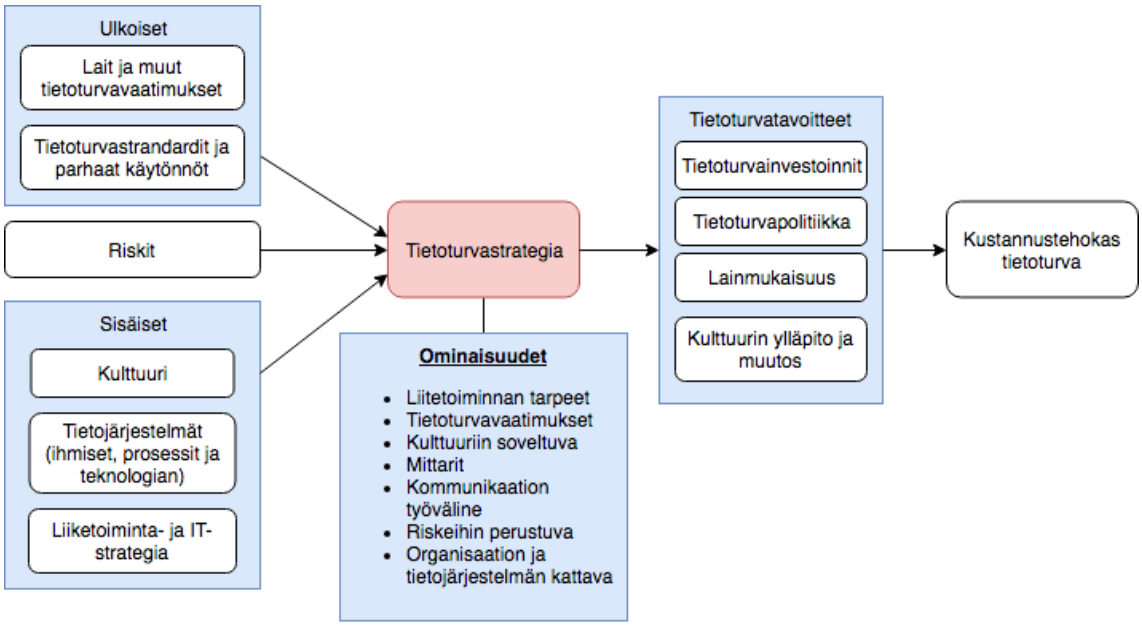
Tietoturvastrategian ja sen hallinnan tulisi olla riittävän dynaaminen, jotta se kykenee heijastamaan muutoksia organisaation toimintaympäristössä (Doherty & Fulford 2006; Onibere ym. 2017). Tunnistamalla toimintaympäristössä tapahtuvia muutoksia, organisaatio voi reagoida tietoturvaan liittyviin uusiin riskeihin ja mahdollisuuksiin ja muuttaa tarvittaessa strategiaa sillä haettavien hyödyn saavuttamiseksi.

Aivan kuten liiketoiminta- ja IT-strategia myös tietoturvastrategian olisi kyettävä reagoimaan muuttuviin vaatimuksiin, jotka voivat olla peräisin eri sidosryhmiltä, teknologioista tai toimintaprosesseita. Tietoturvastrategioissa on huomioitava, että mikäli organisaatio ulkoistaa osan tietoturvan toteutuksesta, organisaation tietoturvastrategiat ja -politiikat tulisi ulottaa koskemaan myös palveluntarjoajaa (Baskerville ym. 2014).

Tietoturvastrategiaa olisi kommunikoitava organisaatiossa liiketoiminta- ja IT-strategian yhdenmukaisuuden varmistamiseksi, jotta myös työntekijät ymmärtävät oman roolinsa strategioihin liittyen (McFadzean ym. 2007). Strategian kommunikoinnilla on tärkeyttä rooli organisaation pyrkiessä kontrolloimaan tietoturvan toteutusta ja seurantaa (Posthumus & Solms 2004).

Tietoturvastrategian kehitys ja toteutus ei tulisi tapahtua erillään muusta liiketoiminnasta, ja siksi ne vaativat kommunikointia, yhteistyötä, motivointia koko niiden elinkaaren ajan. Tietoturvan hallinnan kommunikoinnissa voi esiintyä ongelmia muun muassa ylimmän johdon, operatiivisen toiminnan ja työntekijöiden välillä (Onibere ym. 2017), jolloin keinolla lievittää tätä ongelmaa voi olla organisaatiossa tärkeä rooli.

Tietoturvastrategiassa on tärkeää muistaa, että ei ole olemassa strategiaa, joka toimisi kaikissa organisaatioissa. Tämän vuoksi tietoturvastrategia tulisi kehittää suhteessa organisaation toimintaympäristöön, sisäisiin tekijöihin ja tavoitteisiin. Varsinkin kulttuurisilla tekijöillä on vaikutus tietoturvastrategian toimivuuteen (Flores ym. 2014). Organisaatio kohtaisen tietoturvastrategian kehityksessä ja arvioinnissa voidaan hyödyntää esiteltyä viitekehystä (Kuva 2), mahdollisimman kustannustehokkaan ja organisaatioon soveltuvan tietoturvan aikaansaamiseksi.



Kuvio 2: Tietoturvastrategian viitekehys

5 TUTKIMUSMENETELMÄ

Tutkimuksen tavoitteena on ymmärtää tietoturvastrategioita terveydenhuoltosektorilla. Tästä tavoitteesta johtuen laadulliset tutkimusmenetelmät toimivat paremmin tutkimuksen pyrkiessä vastaamaan päätutkimuskysymykseen: *millainen on toimiva tietoturvastrategia terveydenhuoltosektorilla?*

Tapaustutkimus mahdollistaa laadullisen aineistonkeräämisen eri organisaatioista, ja mahdollistaen ilmiön tutkimisen sen luonnollisessa kontekstissa (Benbasat ym. 1987). Ymmärtämällä terveydenhuoltosektorin organisaatioiden tietoturvan toimintaprosesseja ja tavoitteita, kyetään paremmin määrittämään vaadittavat ominaisuudet terveydenhuoltosektorilla toimivalle tietoturvastrategialle. Tämän ymmärryksen saavuttamisessa auttaa alan organisaatioissa työskentelevien asiantuntijoiden näkemykset ja ohjeistukset liiketoimintaan ja tietoturvaan liittyen.

5.1 Tapaustutkimus

Tutkimuksessa hyödynnettiin laadullista lähestymistapaa, jotta tutkimuksessa voidaan kerätä rikasta laadullista aineistoa tutkimuskysymykseen vastaamiseksi. Tätä lähestymistapaa voidaan paremmin hyödyntää ilmiön ymmärtämiseen sen luonnollisessa kontekstissa kuin, jos käytettäisiin määrällistä lähestymistapaa tutkimusaiheeseen (Darke ym. 1998).

Tapaustutkimus on erityisen pätevä tutkimusmenetelmä tapauksissa, joissa aiheesta ei ole olemassa vakiintuneita teorioita, jotka auttaisivat tutkimusongelmaan vastaamisessa. (Eisenhardt & Graebner 2007) Lisäksi tapaustutkimus on hyödyllinen tutkimuksen pyrkiessä uuden teorian luontiin aiemman teorian testaamisen sijasta. Tutkimuksella pyritään lisäämään ymmärrystä tietoturvastrategian ilmiöstä terveydenhuollon kontekstissa.

Tutkimuksen odotetaan tuottavan uutta tietoja tekijöistä, jotka vaikuttavat terveydenhuollon organisaatioiden tietoturvastrategioiden muodostumiseen ja valintaa. Lisäksi ymmärtämällä alalla toimivien organisaatioiden tietoturvatavoitteita ja -prosesseista kyetään paremmin määrittämään tietoturvastrategialta mahdollisesti vaadittavia ominaisuuksia ja huomioitavia tekijöitä.

Tutkimukseen osallistuvien organisaatioiden motivoimiseksi korostettiin tutkimuksen mahdollisia hyötyjä organisaatiolle. Tällä pyrittiin minimoimaan motivaation aiheuttama vääristymä tutkimuksen tuloksiin. Ymmärtämällä tutkimuksen tarkoituksen ja hyödyt haastateltavat todennäköisemmin osallistuvat tutkimukseen.

Tapaustutkimus tutkimusmenetelmänä mahdollistaa eri tyyppisten aineistojen (muun muassa haastattelut, havainnot, kyselyt ja dokumentit) hyödyntämisen tutkimuksessa. (Benbasat ym. 1987; Darke ym. 1998) Tapaustutkimus mahdollistaa myös määrällisen aineiston käytön tutkimuksessa, mutta tämä tutkimus keskittyy laadulliseen aineistoon, joka tarjoaa rikkaan lähteen analyysiä

varten. Benbasat ym. (1987) ohjeistuksen mukaisesti vähintään kahta aineistonkeräysmenetelmää hyödynnettiin empiirisen aineiston keräykseen ja löydösten tukemiseen. Hyödynnetyt menetelmät olivat haastattelut ja dokumentaatio.

Tapaustutkimuksen tuloksista on huomattava, että niiden pohjalta ei voida tehdä hyvin pitkälle johdettuja yleistyksiä, vaikka tapaustutkimus auttaa ilmiön ymmärtämisessä. Tulosten merkitystä ja oikeellisuutta voidaan pyrkiä vahvistamaan tarjoamalla perusteellinen kuvaus aineistosta ja sen analyysistä.

5.2 Aineistonkeräys menetelmät

Tutkimuksen ensisijaisena empiirisen aineiston keräysmenetelmänä hyödynnettiin haastatteluja. Haastattelut on nähty tärkeäksi tietolähteeksi tapaustutkimuksissa (Darke ym. 1998) Haastattelut mahdollistavat haastateltavien näkemyksien keräämisen tutkittavaan ilmiöön liittyen. Haastattelut mahdollistavat haastateltavien näkemyksien ja ajatuksien ymmärtämisen tutkimuskysymykseen liittyen.

Yksi keino välttää haastatteluiden aiheuttamaa vääristymää on käyttää useampia haastateltavia (Eisenhardt ym. 2007). Tästä syystä tutkimuksessa hyödynnettiin useiden organisaatioiden asiantuntijoita, jotka olivat vastuussa organisaatioin tietoturvan suunnittelusta ja toteutuksesta. Useat haastateltavat antavat erinäkökulmia aiheeseen ja ilmiöön (Eisenhardt ym. 2007). Samalla useat tapaukset mahdollistivat henkilöiden haastattelun saman tasoisessa tehtävässä eri organisaatioissa. Tämä mahdollisti erojen ja yhteneväisyyksien esiintulon kerätystä aineistosta (Eisenhardt ym. 2007).

Tutkimuksessa hyödynnetty teemahaastattelu mahdollistaa haastattelun aikana esille nousevien mielenkiintoisten asioiden tarkemman selvittämisen. Nämä voivat osaltaan auttaa ilmiön ymmärtämisessä ja asetettuun tutkimuskysymykseen vastaamisessa. Lisäksi sillä tietoturvastrategian määritelmän ja hallinnollisen tietotototurvan odotettiin eroavan organisaatioiden välillä, teemahaastattelu soveltui paremmin aineiston keräysmenetelmäksi, kuin tarkkaan määritellyt kysymykset aiheeseen liittyen. Haastatteluiden odotettiin tuottavan vaihtelevia vastauksia organisaatiosta ja haastateltavasta riippuen.

Teemahaastattelun runko on nähtävissä Liite 1. Haastattelulla pyrittiin selvittämään organisaatioiden asiantuntijoiden näkemyksiä tietoturvan nyky- ja tavoitetilaan liittyen. Lisäksi haastattelussa pyrittiin ymmärtämään organisaatioiden prosesseja tietoturvan kehittämiseen liittyen. Haastattelun teemoihin sisällytettiin kysymyksiä, muun muassa asiantuntijoiden näkemyksiä tietoturvan merkityksestä terveydenhuollossa, nykyisistä ja tulevaisuuden uhkista ja mahdollisuuksista ja tietoturvan kehittämisen kohteista. Teemat valittiin, siten että ne auttavat ymmärtämään tietoturvan luonnetta terveydenhuollossa mahdollisimman laajasti. Tämä mahdollistaa aineiston hyödyntämisen kokonaisvaltaisten tietoturvastrategioiden ominaisuuksien määrityksessä. Viitekehyksen näkökulmasta (Kuvio 2) oli tärkeää ymmärtää mm. liiketoiminnan tavoitteita, organisaation kulttuuria, ja tietoturvan hallinta- ja kehitysprosesseja.

Toinen tutkimuksessa hyödynnetty aineisto oli organisaatiosta vapaasti saatavilla oleva dokumentaatio. Tämä aineisto kerättiin organisaatioiden

Internet-sivuilta, ja nämä dokumentit sisälsivät muun muassa liiketoimintastrategian, IT-strategian, tietoturvapolitiikka, tietoturvaohjeet, eettiset ohjeet. Nämä dokumentit mahdollistavat ymmärryksen siitä, kuinka toimintaa on ohjeistettu organisaatioissa ja kuinka haastateltavien näkemykset ovat linjassa näiden dokumenttien kanssa. Haastattelun tulokset voivat vaihdella haastattelun ajankohdan, haastateltavan motivaation ja haastattelijan vaikutuksesta, esimerkiksi haastattelu eri päivänä voi tuottaa eri tuloksen. Tästä johtuen dokumentaatio tarjoaa hyödyllisen tietolähteen laadulliselle aineistolle ja minimoi haastattelun aiheuttaman mahdollisen vääristymän tutkimuksen tuloksiin. Lisäksi esimerkiksi IT- ja liiketoimintastrategia auttaa ymmärtämän mm. organisaation visioita ja toiminnalle valittua suuntaa.

5.3 Empiirisen aineiston analyysi

Tapaustutkimuksessa kerätty aineisto analysoitiin hyödyntäen kirjallisuuskatsauksen pohjalta kehitettyä viitekehystä (Kuvio 2) ja aiempaa kirjallisuutta tietoturvastrategiasta. Analyysi toteutettiin ensin keskittymällä jokaiseen organisaatioon erikseen ja pyrkien löytämään esiin nousseita havaintoja tutkimuskysymykseen liittyen. Tämän jälkeen jokaisesta tapauksesta saatuja tuloksia verrattiin toisiinsa pyrkien löytämään yhteneväisyyksiä ja eroja tapausten välillä.

Tapaustutkimus tutkimusmenetelmänä mahdollistaa rikkaan laadullisen aineiston hyödyntämisen aineiston analyysivaiheessa (Eisenhart & Graebner 2007). Ilmiön ymmärtäminen tapahtuu iteratiivisen prosessin kautta, kerätystä aineistosta esiin nousevia havaintoja verrataan aiempaan kirjallisuuteen (Eisenhardt 1989).

Tutkimuksessa sovellettiin Eisenhardt (1989) esittämäkolmivaiheista prosessia aineistonanalyysille tapaustutkimuksessa. Ensimmäinen vaihe oli tutustua kerättyyn aineistoon tapaus kerrallaan ja tunnistaa esiin nousseet teemat. Tutustumalla jokaiseen tapaukseen erikseen auttaa se ymmärtämään ilmiötä yksittäisessä ympäristössä, ja voi helpottaa ilmiön ymmärtämistä eri organisaation kontekstissa. (Eisenhardt 1989) Tämä voi auttaa tunnistamaan yhteneväisyyksiä ja eroja organisaatioiden välillä. Tunnistamalla toistuvia kaavoja tapausten välillä voidaan tunnistaa tietoturvastrategialta vaadittavia ominaisuuksia, jotka ovat edellytys toimivalle tietoturvalle. Vertaamalla näitä löydöksiä aiempaan kirjallisuuteen, voidaan vahvistaa löydösten validiutta ja yleistettävyyttä (Eisenhardt 1989). Tässä viimeisessä vaiheessa analyysissä auttaa kirjallisuuskatsauksen pohjalta luotu viitekehys.

Tutkimuksen aineistonkeräys ja analyysivaiheessa on tärkeää huomioida tekijöitä, jotka voivat aiheuttaa vääristymää tutkimuksen tuloksiin. (Darke ym. 1998) Tutkijan tulisi mm. tiedostaa omat ominaisuudet ja henkilökohtainen näkökulma aiheeseen, jotka voivat vaikuttaa sekä aineistonkeräykseen että kerätyn aineiston analyysiin. Varsinkin haastatteluiden toteutuksessa tulisi välttää vaikutusta haastateltavaan ja näin kerättyyn aineistoon. Aineiston analyysissä tutkijan tulisi tiedostaa omat uskomukset, arvot ja olettamukset aihee-

seen liittyen (Darke ym. 1998). Eri aineistoiden ja useiden tapausten hyödyntämisellä voidaan pyrkiä minimoimaan tutkijan tiedostamaton vaikutus tutkimuksen tuloksiin (Darke ym 1998; Eisenhardt 1989) Myös aiempaa kirjallisuutta voidaan hyödyntää löydösten tukemiseksi ja erojen tunnistamiseksi. Lisäksi haastatteluaineiston analyysissä tulisi huomioida se, että haastattelulla kyetään keräämään vain haastattelijan näkemyksiä liittyen tutkittavaan ilmiöön, ja ne eivät välttämättä perustu organisaation viralliseen linjaan. Tämä tulee ottaa huomioon varsinkin tehdessä yleistyksiä haastatteluiden perusteella.

Empiirisen aineiston analyysissä hyödynnettiin kirjallisuuskatsauksessa kehitettyä viitekehystä. Saatujen tulosten pohjalta ehdotettiin tietoturvastrategialta vaadittavia ominaisuuksia, jotka varmistavat strategian toimivuuden terveydenhuoltosektorilla.

6 TUTKIMUKSEN TULOKSET JA POHDINTA

Tässä luvussa käydään läpi tutkimukseen osallistuneiden organisaatioiden (tapaukset) ja haastateltavien taustatiedot. Lisäksi luvussa esitellään teemahaastattelun tulokset aihe kerrallaan ja pohditaan tutkimuksen tuloksia suhteessa taustakirjallisuuteen ja kirjallisuuskatsauksessa esiteltyyn viitekehykseen.

6.1 Tapausten taustatiedot

Tutkimusaiheella lähestyttiin 12 Suomessa terveydenhuoltoalalla toimivaa julkisen ja yksityisen puolen organisaatioita. Kiinnostusta osallistua tutkimukseen kysyttiin sähköpostin ja puhelimen välityksellä. Lopulliseen tutkimukseen osallistui kolme organisaatiota. Kaikki tutkimukseen osallistuneet tapaukset olivat julkisen terveydenhuollon organisaatioita. Organisaatiot käsittivät oman alueensa sairaanhoitopiirin. Tapauksina toimineiden organisaatioiden yhteenvetoja aineistonkeräystiedot on esitetty taulukossa 1.

Tunniste	Haastateltavan ammattinimike	Henkilöstö	Haastattelun toteutus
ORG1	Tietohallintopäällikkö/ tietoturvavastaava	6000-8000	Skype®
ORG2	Tietohallintojohtaja/ tietoturvavastaava	6000-8000	Skype®
ORG3	Tietoturvapäällikkö	6000-8000	Läsnä

Taulukko 1: Tapausten tiedot

Jokaisesta tutkimuksen kohteena olevasta organisaatiosta haastateltiin asiantuntijoita, jotka osallistuvat organisaation tietoturvan strategiseen suunnitteluun ja toteutukseen. Haastateltavat henkilöt olivat ammattinimikkeeltään tietohallintojohtaja, -päällikkö tai tietoturvapäällikkö. Nämä henkilöt valittiin haastateltaviksi kirjallisuuteen perustuen, jossa näissä työtehtävissä työskentelevät henkilöt on nähty vastuullisiksi tietoturvan strategiseen suunnitteluun (Onibere ym. 2017). Tutkimuskysymyksen kannalta kyseessä olivat oikeat henkilöt, sillä kaikki haastateltavat osallistuvat aktiivisesti organisaation hallinnolliseen tietoturvan suunnitteluun ja toteutukseen. Lisäksi kaikkien haastateltavien erilliseksi vastuualueeksi oli määritetty tietoturva. Kaikki haastateltavat olivat työskennelleet omassa työtehtävässä yli vuoden ajan.

Haastattelut toteutettiin paikan päällä, tai Skype® -puheluna. Yksittäiseen haastatteluun käytetty aika oli noin 30-60 minuuttia. Kaikki haastattelut toteutettiin tammikuun 2018 aikana.

Haastatteluiden lisäksi organisaatioiden nettisivuilta kerättiin tutkimusaiheeseen liittyen avoimesti saatavilla olevaa materiaalia. Tätä materiaalia kyettiin hyödyntämään aineistonanalyysissä ja tukemaan haastatteluista kerättyä aineistoa. Organisaatioiden toimiessa julkisella sektorilla, näiden organisaatioiden toiminnasta oli saatavilla kohtuullinen määrä dokumentaatiota. Kerättyyn aineistoon kuului mm. tietoturvapolitiikat ja -ohjeet, IT- ja liiketoimintastrategia, riskienhallintapolitiikka, organisaation eettiset ohjeet ja hallintosääntö. Tätä aineistoa hyödynnettiin niiden saatavuuden rajoissa, joka vaihteli tapausten välillä, riippuen siitä oliko dokumentit määritetty julkisiksi vai sisäiseen käyttöön.

6.2 Tulokset

Tässä luvussa käydään läpi teemahaastattelun tulokset, jotka auttavat ymmärtämän tietoturvaa terveydenhuollon organisaatioissa. Tapaustutkimuksessa kerätty empiirinen aineisto analysoitiin suhteessa taustakirjallisuuteen ja kirjallisuuskatsauksessa esiteltyyn teoreettiseen malliin. Tulokset on esitetty haastattelun teema kerrallaan.

6.2.1 Tietoturva ja sen merkitys

Haastatteluissa nousi esille tekijöitä kaikkiin yleisiin tietoturvatavoitteisiin, mm. saatavuuteen, luottamuksellisuuteen ja eheyteen liittyen. Tietoturvatavoitteista eniten esille nousivat saatavuuden ja luottamuksellisuuden merkitys.

Varsinkin saatavuudella oli kriittinen merkitys, sillä tietojärjestelmät keskeisessä roolissa organisaatiossa ja niiden sisältävän tiedon tulisi olla käytettävissä tietoon perustuvan päätöksenteon mahdollistamiseksi. On kuitenkin huomattava, että potilaidenhoito ja muut tärkeät prosessit tulisi olla mahdollisia, vaikka tietojärjestelmät eivät olisi saatavilla. Lisäksi luottamuksellisuudella on tärkeä rooli tietosuojan varmistamisessa, joka on terveydenhuolto alalla määrätty laissa. Potilaisiin liittyvän tiedon tulisi pysyä salassa, ja tietoja tulisi käsitellä vain henkilöt, jotka ovat hoitosuhteessa potilaaseen. Esimerkiksi ORG3 kuvaili tietoturvan merkitystä terveydenhuoltoalalla seuraavasti:

> ”Mä ajattelen sitä (tietoturvaa) kokonaisuutena missä on tietosuoja mukana, koska näitä ei voi tässä ajatuksessa tai tässä kokonaisuudessa erottaa, jos ajattelee sitä merkitystä. … Yksi iso asia on se, että meidän asiakkaiden tiedot pysyy salassa tai luottamuksellisena. Niihin pitää pystyä kaikkien meidän asiakkaiden luottamaan, että ne tiedot on turvassa, ne on oikeita ja muuttumattomia sen aikaa kun ne on siellä järjestelmässä. Niihin ei pääse kiinni tai niitä ei käytetä muuten kuin jos on potilassuhde olemassa potilaaseen. ... koko sen elinkaaren ajan niitä käsitellään asianmukaisesti. Tietoturvatoimilla me turvataan tätä ketjua - et se on se meidän ykkösjuttu.”

Tietoturvan nähtiin ORG1 tapauksessa toiminnan menestystekijänä:

> ”Se (tietoturva) on täysin sidoksissa meidän toimintaan ja on äärimmäisen tärkeä, koska täällä sosiaali- ja terveydenhuollossa potilastieto on lähtökohtaisesti salassa pidettävää, ja sitä saa nähdä vain henkilöt, jotka ovat hoitosuhteessa potilaaseen. Sen vuoksi tietoturva ja tietosuoja ovat yksi tärkeimmistä kriittisistä menestystekijöistä tällä toimialalla.”

Tietojärjestelmien kehityksen myötä myös tiedon turvaaminen on muuttunut terveydenhuollon organisaatioissa. ORG2 kuvaili tietoturvan terveydenhuolto puolella tapahtunutta muutosta järjestelmien ja tiedon osalta:

> ”Tiedot on aina ollut luonteeltaan sellaisia, että suurta muutosta ei sinällään järjestelmien osalta tapahtunut. Potilaskertomustiedon käsittely pysynyt samanlaisena 30 vuoden takaa. … toiminnasta on tullut entistä säädellympää, ja järjestelmien merkitys on kasvanut toiminnassa ja sairaalatoiminta on tietojärjestelmien varassa, kun aiemmin se oli käteisdokumentointia. Toiminnasta tullut reaaliaikaista ja ilman tiedonkeräystä toiminta ei ole mahdollista. Lisäksi tiedot sähköisessä muodossa ja toiminnan kriittisyys on kasvanut eri tasolle, eli minkäänlaisia katkoja toiminnassa ei voi tapahtua. Esimerkiksi jos mietitään 90-luvun takaisia tilanteita niin järjestelmät olivat erillisiä, kun nykyisin järjestelmät mahdollistavat Internetin kautta uusia uhkia, jotka tulee ottaa huomioon toiminnassa - haittaohjelmat ovat olleet merkittävä uhkatekijä, ja Internet on tuonut ne uudelle tasolle”

Johdon merkitys tietoturvalle nousi esille kaikissa tapauksissa, mutta kaikissa organisaatioissa ylemmän johdon nähtiin ymmärtävän tietoturvan merkitys toiminnan kannalta ja suhtautuvan tietoturvaan myönteisesti. Kaikissa tapauksissa tietoturvaan nähtiin olevan käytössä riittävät resurssit. Muutamassa haastattelussa nousi esille, että tietoturvaan liittyvien tapahtumien ilmeneminen organisaatiossa ja mediassa, on edesauttavan johdon kiinnostusta tietoturva kohtaan. Esimerkiksi ORG2 nosti esille järjestelmissä tapahtuvat palvelukatkot:

> "Sairaalassa saa aikaiseksi, kun menee ja tapahtuu palvelukatko. Ja pienemmätkin katkokset ovat sellaisia, että saa asioita tapahtumaan, ja saavat aikaan sen, että jotain olisi asialle tehtävä"

Toisaalta ORG3 nosti esille, että tietoturvan merkitystä ei aina ole täysin ymmärretty, tai sen rooli on joissain tapauksissa epäselvä:

> ”Tietoturvallisuuden merkitys, sitä ei ole oikein ymmärretty … Mun omasta mielestä, vieläkään ei (tietoturvaa) täysin olla ymmärretty ja se nähdään enemmän teknisenä. Nähdään vain niitä uhkia mitä TV:stä tai radiosta kuuluu, eli joku virus jossakin jyllää, vaikka virukset ovat talossa tuttuja, niin se ei ole sama asia ... Tiedot pitää pysyä järjestelmässä ja niihin on pääsy vain, jos niihin on tarve päästä ja järjestelmien on oltava aina saatavilla. ... Kaikki terveydenhuollon organisaatiot pitäisi perustaa siihen, että järjestelmien saatavuus on turvattu... Tietoturvan näkökulmasta se on aika haasteellista ja kaikkein vaikein toteuttaa. "

Haastateltava kuitenkin näki, että organisaatiossa on saatu aikaan tietoturvakulttuuriin liittyvää muutosta, jossa johto on alkanut ymmärtämään, että vastuu tietoturvasta on heillä.

Tapauksissa nousi esille vahvasti tietosuojan ja tietoturvan välinen suhde, jossa tietosuoja on osakokonaisuus tietoturvassa. Tietosuojalla on vakiintunut asema ja rooli terveydenhuollossa, ja tietosuojaan liittyviä vaatimuksia on määritetty Suomessa laissa potilastietojen suojaamaseksi ja varmistamiseksi. Tästä johtuen organisaatioissa tietosuojaan ja tietoturvaan oli nimitettynä eri henkilöt, jotka työskentelivät yhteistyössä. Kaikissa tapauksissa tietoturvatoiminnalla varmistettiin henkilötietojen käsittelyn turvallisuus.

Organisaatiot näkivät useita mahdollisia uhkatekijöitä tietoturvaan liittyen. Haastatteluissa nousi esille mahdollisia uhkalähteitä mm. henkilöstöön, lääkinnällisiin laitteisiin ja haittaohjelmiin liittyen. Kaikissa tapauksissa riskienhallinta ja riskiarvio toimi pohjana tietoturvan kehitykselle ja prioriteettien asettamiselle. Kuten kirjallisuudessa riskienhallinta on hyvä keino kerätä ja arvioida liiketoimintaa uhkaavia tekijöitä niin organisaation toimintaympäristöstä kuin organisaation sisältä (Taylor 2015)

Esimerkiksi ORG1 nosti esille henkilöstöön liittyviä riskejä johtuen, muun muassa organisaation koosta:

> ”Yleisesti ottaen ihminenhän se heikoin lenkki näissä asioissa on. Se, että me saadaan 6000 hengen henkilöstö - lääketieteen ja hoitotieteen opiskelijat päälle noudattamaan niitä ohjeita ja määräyksiä mitä organisaatio on antanut.”

Myös ORG3 nosti esille henkilöstöön liittyviä uhkia

> ”Yksi iso uhka on myös, jos muistaa, että aika isoja sairaaloita on Suomessa, niin kun on tuhansia ihmisiä töissä ja kaikki käytännössä sähköpostia lukee. Niin on liian helppoa laittaa haitakkeita (haittaohjelmia) tulemaan liitteenä, ja edelleen on liian helppoa. Useissa sairaaloissa voi viedä laitteita, jotka eivät kuulu sinne ja saastuttavat sitä kautta verkkoa. … aika pitkälle tämä toiminta perustuu luottamukseen, mutta luottamus ei tarkoita sitä, että kaiken pitäisi olla kontrolloimatonta ja avointa, mutta pitäisihän tämän olla hallittua ja ehkä tässä on julkisella sektorilla aika paljon tekemistä.”

Tästä huolimatta kaikki tapaukset näkivät henkilöstön suhtautuvan tietoturvaan tietyllä vakavuudella ja uskoi henkilöstön ymmärtävän tietoturvan merkityksen organisaation toiminnalle. Ongelmallisiksi asiaksi esimerkiksi ORG1 näki kiireisen työn vaikutuksen, josta johtuen henkilöstöllä on omia vaatimuksia, joihin tietohallinnon oli myös kyettävä vastaamaan tietoturvan varmistamiseksi:

> ”… totta kai haluaisivat (henkilöstö), että olisi nopeampaa ja helpompaa, kun järjestelmiä käytetään. … työasemalle kirjautuminen nähdään liian kauan kestäväksi asiaksi, ja tätä kautta tulee naputusta. Tietohallinnon tehtävä on helpottaa myös työtä tässä näkökulmassa - että myös tietoturva toteutuu.”

Tämä voi korostaa entisestään organisaatioiden kykyä muodostaa suotuisa tietoturvakulttuuri organisaatioon. Lisäksi organisaatioiden tulisi varmistaa järjestelmien käytettävyys siten, että henkilöstö ei kehitä omia strategioita työnmahdollistamiseksi ja olemassa olevien tietoturvakontrollien kiertämiseksi. Henkilöstön arvojen huomioiminen tietoturvakontrollien valinnassa on tietoturvakirjallisuudessa ehdotettu keinoksi välttää tietoturvan ja ammatillisten arvojen ristiriita (Hedström ym. 2011).

Kuten jo haastateltaessa tietoturvan merkityksestä myös mahdollisista riskeistä puhuessa nousi esille saatavuuden merkitys, joissa jatkuvuudenhallinnalla ja sen sisältämillä varautumisjärjestelmillä on tärkeä rooli. Esimerkiksi ORG3 korosti riskien minimointia liittyen potilasturvallisuuteen:

> ”Me pyöritään täällä 24/7 ja sairaala on auki kaikki päivät vuodesta. Meillä on jatkuva miehitys talossa ja jatkuvasti asiakkaita sisään. Niin se ykkösasia on toki se potilasturvallisuus. Eli kenenkään henki ei vaarannu tämän takia, että meillä jostakin tietoteknisestä syystä tai toimimattomuudesta johtuen olisi tämmöinen riski.”

ORG3 nosti esille mahdollisia tulevaisuuden uhkia lääkinnällisiin laitteisiin ja ohjelmistoihin liittyen:

> "Lääkintälaitteet on yksi iso asia ja niihin liittyvät haavoittuvuudet. ... lääkintälaite saa CE-merkinnän ennen kuin se voidaan ottaa käyttöön tai myydä, samoin kuin potilastietojärjestelmät tai kliinisentoiminnan järjestelmät. … CE-merkintä sinänsä ei tarkoita yhtään mitään (tietoturvan näkökulmasta): siellä ei ole kyberturvallisuuden vaatimuksia. Silloin kun CE-merkintä tehdään, se haetaan sille kokoonpanolle, joka on sillä hetkellä. Ja lääkintälaitevalmisteet, jotka voivat olla ohjelmistoja, niin ei niillä ole hinkua muuttaa sitä kokoonpanoa ja tehdä niitä päivityksiä, sillä se vaatisi uuden "rumban" siihen CE-merkinnän ylläpitoon tai hakemiseen. Ja tämähän on sellainen asia, että terveydenhuollon kentässä näkee paljon vanhoja järjestelmiä ja sellaisia missä tänäkin päivänä voi pyöriä Windows XP ohjaamassa jotain tiettyä lääkinnällistä laitetta. Ja eihän siihen ole saanut päivityksiä enää niin kuin vuosiin. Ei siihen tule tietoturvapäivityksiä, jos se ei ole ylläpidossa, eli ne täytyy suojata eri tavalla, eli esim. eristämällä verkosta. ”

Samaan asiaan liittyen ORG3 nosti esille teknologian mahdollistamat uhkat ja tarpeen tietoturvavaatimusten sisällyttämiselle CE-merkintään:

> ”… varsinkin digitalisaation kautta, jos niidenkin tulisi alkaa liikennöimään jonnekin pilvipalveluihin ja sitä kautta tänne muualle. Niin silloinhan niidenkin tulisi olla CE-merkinnän tai muun lainsäädännön piirissä, että niitä tulee päivittää. Niillekin tulisi olla kyberturvallisuuden vaatimukset.”

Tapauksista ORG1 oli ainut organisaatio, jossa tietoturvaan liittyviä tavoitteita oli mainittu suoraan liiketoimintastrategiassa. Tietoturva oli ilmaistu ICT:n ja siihen liittyvien palveluiden kehityksen rinnalla, pyrkien varmistamaan näiden järjestelmien saatavuus ja jatkuvuus. Organisaatio pyrki jatkuvaan kehitykseen, jossa käytettävät teknologiat pysyvät tietoturvan vaatimusten mukaisella tasolla.

6.2.2 Tietoturvastrategia ja sen merkitys

Yllättäen tapausorganisaatioissa oli vähemmän kiinnitetty huomiota tietoturvastrategiaan ja sen tarpeellisuuteen, kuin kirjallisuuskatsauksen pohjalta olisi voinut ymmärtää. Tämä voi johtua siitä, että tietoturvastrategian määritelmä voi paikoin olla epäselvä, kuten edellä olleessa kirjallisuuskatsauksessa todettiin. Lisäksi tieteellisestä kirjallisuudesta puuttuu käytännönosoitus kirjatusta tietoturvastrategiasta ja mahdollisista hyödyistä organisaation tietoturvan tehokkuuteen.

Tämän vuoksi organisaatiot voivat epäröidä tämän lähestymistavan kokeilua, sen selvien hyötyjen puuteen vuoksi. Tietoturvastrategian käytännön hyödyt vaativat selkeästi empiiristä lisätutkimusta.

Tietoturvastrategiasta ja tietoturvapolitiikasta löytyy konsepteina paljon yhteneväisyyksiä, joka oli nähtävissä myös haastattelun tuloksissa. Politiikka on tahdon ilmaus tietoturva toteuttamiseksi, mutta se ei varsinaisesti sisällä mitään mitattavissa olevia tekijöitä. Puolestaan tietoturvastrategia voidaan nähdä tavoitetilana, ja siihen pääsemistä pyritään mittaamaan. Kuten politiikka myös strategia pyrkii ohjaamaan toimintaa, politiikasta eroten se voi sisältää suunnitelmalliset menetelmät tähän tavoitteen pääsemiseksi.

Esimerkiksi ORG1, joka oli tapauksista ainut, jolla oli käytössä kirjattu tietoturvastrategia, määritteli tietoturvastrategian ja sen merkityksen omassa toiminnassaan seuraavasti:

> ”Kyllä se siitä lähtee, että meidän tekniset ympäristöt ovat tietoturvallisia ja ajanhermolla ja henkilöstö on koulutettu ja perehdytetty käyttämään järjestelmiä oikein. … Strategiahan aina asettaa suuntaviivat ja antaa edellytykset toimia. … Strategia antaa niin kun valmiudet ja käytönnöntyö tuottaa tulokset.”

ORG1 pyrki hyödyntämään suunnitelmia henkilöstön tietoturvan ja tietosuojan perehdytykseen ja koulutukseen. Lisäksi organisaatiossa oli ICT:n valmiussuunnitelmaa ja osana sitä järjestelmien kriittisyysluokitus. Lisäksi ORG1 näki liiketoiminnalliset tavoitteet tietoturvan strategisen suunnittelun ydinasiaksi, ja salassapidon varmistaminen nähtiin suunnittelun lähtökohdaksi.

ORG3 ja ORG2 hyödynsivät tietoturvapolitiikkaa ylemmän tason dokumenttina, jossa oli muun muassa ORG2 tapauksessa määritetty tieto-organisoinnin periaatteet. ORG3 hyödynsi tietoturvapolitiikkaa strategisena dokumenttina, jossa on otettu huomioon myös liiketoimintastrategia:

> "Meillä on tietoturvapolitiikat ja periaatteet ja ohjeistukset, ja politiikka meidän kielessä tarkoittaa johdon tahdonilmaisua, joka perustuu sairaanhoitopiirin strategiaan ja riskien kartoitukseen. "

Konkreettisemmalla tasolla ORG2 hyödynsi tietoturvasuunnitelmaa, jossa on 2 osaa tietoturvan käytänteet ja tietoturvankehityssuunnitelma. Tietoturvakehityssuunnitelmaa organisaatiossa tarkasteltiin ja päivitettiin vuosittain. Tietoturvakehityssuunnitelma oli heidän organisaatiossaan luettelomainen dokumentti siitä mitä organisaatiossa pitäisi toteuttaa vuoden aikana tietoturvaan liittyen. Dokumenttiin liittyy oleellisena osana toteutettu seuranta:

> ”… toteutuksen seuranta viedään tietoturvaryhmään, josta minä vastaan. Ja siihen osallistuu muita osaprosessien vastuuhenkilöitä, peruskäyttäjäkentästä edustajia. ja siellä käsitellään tietoturvaan liittyviä asioita, mutta tärkein tehtävä on nimenomaan vuosittainen suunnitelman arvio ja valmistella kehittämissuunnitelma seuraavaksi vuodeksi prosessissa.”

Kaikissa tapauksissa tietoturvapolitiikka ja liiketoimintastrategia nähtiin hyödyllisiksi dokumenteiksi toiminnan kannalta. ORG1 nosti esille käytännön toiminnan ja tekemisen merkitystä suhteessa kirjattuihin asioihin:

> ”… tietoturva ja tietoturvapolitiikat on tärkeitä, mutta sellainen käytännöntyö, on se, joka ne tulokset antaa ja määrittää kuinka hyviä ollaan. … hieno mantra ei riitä, siksi ne asiat tulee jalkauttaa käytännössä sinne organisaatioon ja toimitaan sitten niiden politiikkojen mukaisesti.”

Tietoturvastrategian tarpeellisuudesta oli vaihtelevia näkemyksiä, osittain sen hyödyt nähtiin, mutta toisaalta sen tarpeellisuus kyseenalaistettiin, johtuen mm. siitä, että organisaatioilla oli liiketoimintastrategia, johon kaiken toiminnan pitäisi tähdätä. Lisäksi tapauksissa oli mahdollista aktiivisesti käsitellä tietoturvaan liittyviä asioita erilaisissa työryhmissä ja kokouksissa noin 2-4 viikon välein. Tämä nähtiin, jossain tapauksissa tehokkaaksi keinoksi ohjata tietoturvaan liittyvää toimintaa ja varmistaa tietoturvan yhdenmukaisuus liiketoiminnan kanssa. Tietoturvan yhdenmukaisuudella liiketoiminnan kanssa voi olla suuri vaikutus tietoturvan toimivuuteen (Karanja 2017).

ORG3 tapauksessa tietoturvastrategian kirjaamista oli harkittu, samoin kuin IT:n liittyen, mutta sen sijaan ORG3 korosti liiketoimintastrategian merkitystä kaiken toteutuksen suunnittelussa:

> " … kaikkien tulisi tukea sitä organisaation valitsemaa strategiaa, ja tämä pohjautuu siihen, että meille johtoryhmätyöskentely, mikä on joka toinen viikko ja hallitus meillä kokoontuu joka kuukausi. … meidän sairaanhoitopiirin strategiaan kuuluu keskeinen tavoite, joka on se, että sen perustehtävän hoitoon on käytössä joustavat kustannustehokkaat, turvalliset ja jne olevat ohjelmistot ja laitteistot. Niin sehän myöskin auttaa jo siinä itsessään, joka auttaa tiettyä turvallisuutta. Ja siellä sanotaan suoraan, että palveluiden tulee kattaa, ja vastata SHP:n perustehtävän toteuttamisen tarvetta. Niin me emme ole enää sen lisäksi lähteneet rakentamaan erillistä ICT:stä tai tietoturvallisuudesta omaa strategiaa, koska se olisi saman asian toistoa käytännössä, siis visiona,”

Tietoturvan näkökulmasta ORG3 näki tietoturvapolitiikan strategisena dokumenttina:

> ” … meillä se politiikka, se on enemmänkin strateginen tai strategiaa tukeva dokumentti kuin operatiivista toimintaa. … operatiivista toimintaa tukee IT-johdon periaatteet. "

Kysyttäessä ORG3 määritelmää tietoturvastrategialle haastateltava mietti myös tietoturvan hyötyjä:

> "Strategia on pitkän tähtäimen visio tai suunnitelma ... Jos politiikka kuvaa tahtokuvaa niin strategia kuvaa vielä enemmän tahtokuvaa ja suuntaa siitä mihin ollaan menossa. ... Sinänsä kun jos sen näin ajattelee niin ei yhtään huono, että tietoturvastakin olisi kirjattu strategisia suuntaviivoja - se ei ollenkaan olisi huono homma. Olemme tehneet niitä muistakin esim. pilvipalveluista tällaisia strategisialinjauksia. ... Mutta siis pitkänajan suunnitelma ja tahtotilan ilmaisu ... Se olisi enemmän visio pohjainen, mutta visio saattaa olla myös harhanäky. "

ORG3 oli kuitenkin henkilökohtaisesti tyytyväinen siihen, että organisaatiolla ei ollut yksittäisiä pitkän tähtäimen tavoitteilla sillä näki tavoitteeksi ja tärkeäksi asiaksi tietoturvatoiminnan jatkuvan kehityksen ja sen ohjauksen esimerkiksi kuukausitasolla.

6.2.3 Tietoturvan suunnittelu ja kehitys

Kaikissa tapauksissa tietoturvan suunnittelu tapahtui riskienhallinnan ja riskiarvion pohjalta. Lisäksi kaikissa tapauksissa tietoturvaa pyrittiin toteuttamaan proaktiivisesti tunnistaen mahdollisia uhkia toiminnalle. Tietoturvan suunnittelussa hyödynnettiin eri tapauksissa eri keinoja, muun muassa liiketoimintastrategiaa, tietoturvapolitiikkaa, tietoturvastrategiaa ja vuosittain päivitettävää tietoturvan kehityssuunnitelmaa. Myös eri sidosryhmiä otettiin aktiivisesti mukaan tietoturvan suunnitteluun pyrkien varmistamaan muun muassa operatiivinen toiminta ja toiminnan lainmukaisuus.

ORG1 nosti esille tekemisen merkityksen tietoturvaan ja näki politiikat ja strategiat toimivaltuutena toteuttaa sovittua linjaa. ORG1 tietoturvaa toteutettiin jakamalle se kahteen osaan: henkilöturvallisuuden puoleen ja tekniseen tietoturvaan, joka pitää sisällään mm. ICT:n valvontasuunnittelun ja jatkuvuudenhallinnan. ORG1 korosti teknisen tietoturvan lisäksi sitä, että myös henkilöstö tulee olla koulutettu ja ohjeistettu oikein, jotta tietoturvalla tavoitellut hyödyt kyetään saavuttamaan.

Esimerkiksi ORG1 tietoturvan strategiseen suunnitteluun osallistui useiden sidosryhmien edustajia. Tietoturva- ja tietosuojatyöryhmiin, jotka kokoontuivat 1-2 kk välein osallistui muun muassa hallinnon johto, tietoturva- ja tietosuojaasiantuntijat ja turvallisuuspäällikkö. Näiden työryhmien tarkoituksena on tarkastella ajankohtaisia asioita ja linjata toimintaa. Muuten tietoturvan suunnittelu ja kehitys on jatkuvaa ja tiettyjen henkilöiden toimenkuvassa, esimerkiksi tietohallinnossa tietoturvasuunnittelijalla. Useat sidosryhmät voi vaatia hyvää kommunikaatiota eri toimijoiden välillä, jotta kaikki kykenevät puhumaan samasta asiasta.

Myös ORG3 tapauksessa tietoturvan suunnittelu tapahtui tietoturvaryhmässä, joka haastateltavan vastuulla. Ryhmässä oli edustettuina mm. turvallisuuspäällikkö, tietosuojavastaava, potilasturvallisuus koordinaattori, johtajaylilääkäri, hallintopäällikkö ja tietohallintopäällikkö. Ryhmä käsittelee kehityskohteita ja poikkeamia asiantuntijafoorumina, josta voidaan tehdä esityksiä tietoturvajohtoryhmälle, joka on organisaatiossa operatiivinen johtoryhmä, jossa istuu ylimmät johtajat. Tältä johtoryhmältä osa asioista menee eteenpäin hallituksen käsiteltäväksi. ORG3 tapauksessa pienemmät muutokset kyettiin toteuttamaan ilmoitusluontoisesti haastateltavan toimesta, mutta suuremmat muutokset, jotka voivat vaikuttaa työntekijöihin tai työn tekemiseen tuli toteuttaa edellä esitellyn prosessin mukaisesti. Kirjallisuuden näkökulmasta tämä voi auttaa toimintaprosessien huomioimisen tietoturvan toteutuksessa.

ORG2 pyrki aktiivisesti hyödyntämään peruskäyttäjiä tietoturvan suunnittelussa ja ylläpidossa:

> ”tietoturvan suunnitteluryhmässä on mukana perushenkilöstöä eri työntekijätasoilta ja henkilöitä ihan käyttäjätasoltakin on mukana. Käyttäjiä motivoidaan ilmoittamaan tietoturvaloukkauksista, esim. mikäli tietoturvan kannalta on jotain ongelmia. Käytössä on Haipro(-ohjelma) jonka kautta tällaisista (tietoturvauhkista/-tapauksista) voidaan raportoida, vaikka ihan nimettömänä.”

ORG2 tapauksessa prioriteetit tietoturvan toteutukseen oli asetettu tietoturvasuunnitelmassa

> ”Tietoturvasuunnitelmassa on asetettu prioriteetit. Toki kaikki dokumentit on yhtä tärkeitä, mutta kehittämisen osalta suunnitelmassa on määritetty mitkä seikat menevät toisen edelle. Tietoturvaryhmässä luonnokseen määritellään prioriteetit riskiarvion pohjalta. Riskianalyysissä arvioidaan mikä olisivat sellaisia keskeisimpiä riskejä”

Tapaukset hyödynsivät useita erilaisia ohjeistuksia ja viitekehyksiä tietoturvan suunnittelussa. Tärkeimmäksi ohjeistukseksi haastatteluiden perusteella voitiin nähdä VAHTI-ohje, jota kaikki tapaukset hyödynsivät. Esimerkiksi ORG2 kuvaili VAHTI-ohjeistuksen merkitystä tietoturvan suunnittelussa:

> "VAHTI tärkein ohjeistus esim. yleiset vaatimukset johdetaan sieltä, ja niitä käytetään järjestelmän varmistukseen ja osaa ohjeista sovelletaan, mutta osa menee sellaisenaan"

ORG1 nosti esille VAHTI-ohjeistuksen ja teollisuuden yleisten standardien lisäksi tietoturvan ja tietosuojan suunnitteluun osallistuvien henkilöiden henkilökohtaisen osaamisen merkitystä, jota on pyritty kehittämään ja ylläpitämään jatkuvalla koulutuksella.

Muita hyödynnettyjä ohjeita ja viitekehyksiä tapauksissa oli tietoturvaan liittyvät ISO27000-standardit, Katakri, Kanta-palveluhin liittyvät kelan ohjeistukset, lääkinnällisiin laitteisiin liittyvät ohjeistukset ja riskienhallintaan liittyvät ISO31000. Mikään tapauksista ei ollut hakenut ISO standardointia, sillä ne nähtiin sellaisenaan liian raskaaksi implementoida, sen sijaan näitä ohjeistuksia käytettiin hyödyksi toiminnan suunnittelussa. ORG3 tapauksessa Katakri nähtiin hyödylliseksi työkaluksi tietoturvan toteutuksen suunnittelussa.

ORG3 korosti liiketoiminnan ja organisaation todellisen tarkoituksen huomioimista tietoturva suunnittelussa:

> "…varsinainen strategia ohjaa sitä toimintaa … meillä kuitenkin kaikki perustuu siihen tosiasiaan, että se asiakas/potilas tulee hoidettua. … että onpa se sitten käytännössä, on se sitten lainmukaista tai ei, niin se potilas hoidetaan - potilaan kannalta ajateltuna se on erittäin hyvä asia.”

Lisäksi ORG3 korosti toimintaympäristöön soveltuvien tietoturvakontrollien merkitystä

> "siis täällä puhutaan ihmisten kanssa ja ihmiset on se juttu ja niiden hoitaminen on se 1. prioriteetti. Ei se mene niin, että voit laittaa kontrolliksi, että kone pysyy vain yhden minuutin tai puoli minuuttia auki, jos et koneeseen koske. Jonka vuoksi näitä asioita tulee miettiä aivan toiselta kantilta, jos sellaisia asioita ei voikaan tehdä. "

Toiminnan tavoitteista johtuen myös tietoturvakontrollit voivat erota merkittävästi muiden alojen vastaavista. Joka puolestaan vaatii tietoturvan miettimistä strategisesta näkökulmasta, jotta organisaation arvonluotiprosessit ovat mahdollisia.

Myös ORG1 nosti esille toiminnan ja henkilöstön ymmärtämistä tietoturvan toteutuksessa. Kysyttäessä ORG1 mikä tietoturvaan liittyen kaipaisi kehitystä, niin haastateltava nosti esille kommunikaatio kykyä henkilöstön ja tietohallinnon välillä:

> ” … ehkä jos jotain vois toivoa niin ehkä enemmän sellaista vuoropuheluahenkilöstön ja tietohallinnon henkilöstön välillä, niin sanotusti, että ymmärrettäisiin toisiamme vieläkin paremmin … kun IT:stä annetaan ohjeita ja määräyksiä, niin ne ei välttämättä aina kohtaa sen hoitotyön varsinaisten vaatimusten kanssa. Sellaisiinkin olen urani aikana törmännyt, eli sellainen yhdessä tekeminen ja vuoropuhelu olisi tärkeää. Sitä ei voi koskaan tehdä liikaa.”

Sama asia on noussut esille tietoturvakirjallisuudessa, jossa on korostettu tietoturvakontrollien tarpeellisuus huomioida henkilöstön ammatilliset arvot (Hedström ym. 2011).

ORG3 pyrki hyödyntämään aktiivisesti henkilöstöä eri kehitysprosesseissa ja miettimään toteutettuja kontrolleja myös henkilöstön näkökulmasta organisaation varautuessa tulevaisuuden tarpeisiin:

> ” Digitalisaation aiheuttaman muutoksen vuoksi myös tietoturvallisuus ja tietosuojaasioita joudutaan miettimään aivan uudella tavalla ja kuinka pystytään suojaamaan ja pystyykö suojaamaan. Tässä prosessissa henkilöstö suuressa roolissa ja kun mietitään, onko toteutus tekninen vai muu tapa. … meillä on 4000 omaa henkilöstöä ja pelkästään sillä massalla tehdään paljon henkilöstöhallinnon kanssa sellaista yhteistyötä, että miten joku tietty asia vaikuttaa henkilöstön toimintaan. - ilman henkilöstön sitouttamista ja mukaan tuontia niin näillä ei oikein mitään tee.”

6.2.4 Tietoturvan seuranta ja arviointi

Tietoturvaa seurattiin tapauksissa operatiivisella tasolla eri tavoin ja automatisoidut järjestelmät mahdollistivat muun muassa reaaliaikaiset ilmoitukset poikkeamista. Näistä mittareista eniten esille nousi saatavuuden mittari, jota seurattiin organisaatioissa järjestelmien saatavuuden varmistamiksi. Tämä nähtiin tärkeäksi mittariksi, sillä sairaalat toimivat ympäri vuorokauden ja tehokas ja turvallinen hoito vaati tiedon saatavuutta. Esimerkiksi ORG2 tapauksessa tietoturvaa seurattiin aktiivisesti eri mittareiden avulla:

> ”kriittisenä kriteerinä on järjestelmien saatavuus, joka yhtenä mittarina. Mutta tietoturvasuunnitelmassa on määritelty viralliset mittarit ja siellä on mm. käyttökatkojen määrä, järjestelmästä johtuvien virheiden määrä, seurataan järjestelmälokien tarkastuskertoja, eli kuinka monta kertaa tällaisia tarkastuksia on tehty. … Yksi mittari on, kuinka hyvin kehityssuunnitelma on toteutunut ja kuinka siinä määritellyt tavoitteet on saatu valmiiksi. (Lisäksi) koulutusten seuranta eli kuinka paljon tietoturvakoulutuksia tehty vuosien varrella.”

ORG2 tapauksessa mittareita seurattiin pääsääntöisesti vuositasolla, mutta esimerkiksi saatavuutta saatetaan seurata myös tarkemmin kuukausitasolla. Strategisemmalla tasolla mittareita seurattiin ja arvioitiin aktiivisesti tietoturvaryhmässä, josta oli vastuussa haastateltava. Tähän ryhmään osallistui muun muassa

muita osaprosessien vastuuhenkilöitä ja loppukäyttäjien edustajia. Haastateltava kuvaili ryhmän tehtävää tietoturvan toteutuksessa:

> "… käsitellään tietoturvaan liittyviä asioita, mutta tärkein tehtävä on nimenomaan vuosittainen suunnitelman arvio ja valmistella kehittämissuunnitelma seuraavaksi vuodeksi."

Kysyttäessä ORG3 tietoturvan seurannasta ja arvioinnista, haastateltava oli jakautunut näkemys organisaation tietoturvan seurannan tilasta:

> "… aitoa vaatimusta ei ole edelleenkään hirveän hyvin olemassa. … eihän meillä ole mitään, jos meillä ei ole tilannekuvaa ja seurantaa. Tilannekuva on haasteellinen tämmöisessä ja se ei ole meillä kunnossa, eli se tapahtumien arkipäiväinen tapahtumien seuranta on vajaa ja sitä yritetään parantaa, jotta oikeasti nähtäisiin mitä tapahtuu. … Meillä on vuosiraportti, jossa tietoturvallisuuden tilaa on pitänyt viedä johdolle … siten meillä oli puolentoista kuukauden välein tietoturvaryhmä, jonne vietiin tilannekuvaa tiedoksi. Minun mielestä tuossa on sellainen, että vielä se meidän johtoryhmä ei vielä ole sellaisessa kypsyysasteessa tietoturvan osalta, että ne haluaisivat sinne joka kuukausi raportin."

ORG3 kuitenkin näki, että ylemmän johdon kiinnostus tietoturvaa kohtaan on lisääntynyt ja jotta tietoturvan tilaa pystytään käsittelemään organisaatiossa ylemmällä tasolla kiinnostuksen tulisi tulla ylhäältä päin:

> "nyt olemme päässeet siihen tilanteeseen johtaja ylilääkärin kanssa, että kun olemme keskustelleet, niin hän on itse esittänyt kysymyksen, että voisimmeko tehdä tälle asialle jotain, joka on erittäin hyvä, sillä viemällä asiaa alhaalta ylös ja tunkemalla se sinne niin ei se mahdu sinne listalle. Niin sen kiinnostuksen tulee tulla vastuualueiden johtajien kautta ja nyt kun me saamme tallaisen indikaation, että voimmeko tuoda tästä asiaa esille niin on helppo vastata, että kyllä voimme. Niin saadaanhan sinne tehtyä kuukausiraportti tapahtumista, joka on hyvä asia."

Lisäksi ORG3 näki ongelmalliseksi valtakunnallisen vaatimusten puuttumisen, joka voisi auttaa mittariston kehittämisessä:

> " Siinä (tietoturvan arvioinnissa) auttaisi hirveästi, jos olisi valtakunnassa kriteeristö, joiden mukaan tulisi toimia. Sen jälkeen meillä olisi selkeä kompliansivaatimus. Silloin olisi paljon helpompi mennä sitä kohti. Nyt ehkä liikaa pelätään sitä, että sitouduttaisiin johonkin, vaikka Katakrin perustasoon. Sillä eihän siellä ole mitään ihmeellistä, mutta silti pitäisi sitoutua. Jos näin kaikki toimii niin olisi helppo seurata kuinka asiat toimii."

ORG3 nosti kuitenkin esille tarvetta tietoturvavaatimuksille julkiselle puolelle, jossa tietoturvatasot eivät ole pakollisia, ja toivoi kuntapuolelle soveltuvaa kriteeristöä selkeyttämään tietoturvanvaatimuksia ja helpottamaan organisaation tietoturvan arviointia. ORG3 vertasi valtion virastojen tietoturvan tasoa kuntapuoleen, joihin ei liity samanlaista vaatimusta turvallisuustasosta ja niiden vaatimusten hyväksymisestä, joka voi mahdollisesti muodostua ongelmaksi:

> ”Tietoturvavaatimusten puute kuntatasolle vs. valtiontasolla)) tämä on ehkä syistä, miksi sairaalat ovat tilanteessa, jossa tietosuoja on erittäin hyvin toteutettu ja ohjeistettu, mutta tietoturva on laahannut perässä. Koska siihen ei ole ollut kriteeristöä.”

6.2.5 Tietoturvan edellytykset

Kuten kirjallisuudessa myös tapausorganisaatioissa johdontuki nähtiin edellytykseksi tietoturvatoiminnalle. Tärkeimpiä henkilöitä organisaatiossa olivat kaikesta toiminnasta vastaava sairaanhoitopiirin johtajat ja lääkäreistä vastaavat johtajaylilääkärit, joille kuuluu myös tietosuojasta vastaaminen. Näiden henkilöiden asennoituminen tietoturvaan nähtiin hyväksi, ja heidän jopa kasvanut kiinnostus tietoturvaa kohtaan nousi haastatteluissa esille.

Esimerkkinä ORG1 kuvasi johdon asennoitumista tietoturvaan hyväksi:

> ”… kyllä he (ylin johto) suhtautuvat näihin asioihin positiivisesti. Pitävät tärkeänä, ja siitä osoituksena toimii se, että viime vuonna pariin kertaan harjoiteltiin mm. kyberturvallisuutta valmiusharjoituksissa.”

ORG2 tapauksessa johdon sitoutuminen tietoturvaan nähtiin edellytykseksi onnistuneelle tietoturvalle:

> ”… ehkä tärkeimmät edellytykset ovat johdonsitoutuminen siihen asiaan ja siten että myös resursoidaan näihin [tietoturvaan] riittävästi - muuten on aika heikkoa.”

Kaikissa organisaatiossa tietoturvan toteutus oli sidottu IT-budjettiin, mutta suurimmaksi osaksi nykyiset resurssit nähtiin riittäviksi, vaikkakin budjetoidut määrärahat voisivat olla suurempia.

ORG1 nosti esille myös edellytyksenä tietoturvalle henkilökunnan ammattitaidon sekä tekniseen että sosiaaliseen osaamiseen liittyen:

> ”tietoturva on hyvin pitkälle teknistä varautumista ja siihen tarvitaan ICT-alan ammattilaisia. Ja suurin ja isoin juttu on kouluttaa perehdyttää siten, että henkilöstö toimii niiden annettujen ohjeiden ja määräysten mukaan. Silloin se toteutuu parhaiten. Siinä on niin kun 2 ulottuvuutta tekninen ja henkilöstön tietoturvaasiat.”

Tämä näkemys on ollut esillä myös kirjallisuudessa, jossa on todettu organisaation tietoturvakulttuurin vaikuttavan lopulliseen tietoturvan toimivuuteen. (Damenu & Beaumont 2017) Organisaatiot tarvitsevat teknisiä toteutuksia tietojärjestelmien varmistamiseksi, mutta myös työntekijät olisi kyettävä motivoimaan organisaation työntekijät noudattamaan tietoturvapolitiikkaa ja tietoturvaohjeita. Näin organisaatio voi välttää työntekijöiden tahattomat tai tahalliset uhat organisaation tietojärjestelmille sitä kautta arvonluonti prosesseille.

Kysyttäessä ORG3 tapauksessa haastateltavan näkemyksiä kulttuurin merkitykseen, haastateltava näki kulttuurin tärkeäksi osaksi tietoturvan tavoitetta:

> ”Tämähän (tietoturva) on kulttuurikysymys. Tämähän on, jos ajattelee sitä strategiaa ja sille asetetaan se tähtäin sinne kauas, ja se kuvaisi sen meidän vision, mitä sillä tietoturvalla tulisi pyrkiä saavuttamaan - eli sen pitäisi olla sen toiminnan tukena. Oikeastihan tämä on sitä organisaation kulttuurin luomista - on se sitten sitä strategiaa tai politiikkaa niin sen ihmisten kouluttaminen ja mukaan ottaminen. Niin sinähän luot sitä kulttuuria. Niin jos täällä ei ole ollut sitä hyvää kulttuuria sen osalta niin ihmiset toimii silloin valitsemallaan tavalla.”

Lisäksi ORG3 toivoi organisaation yleisen kulttuurin kehittyvän suotuisammaksi myös tietoturvalle ja ymmärtäisi sen merkityksen osaltaan tietosuojan saavuttamisessa:

> " Niin sitä minä toivoisin että sitä kulttuuria kyettäisiin sillä tavoin muuttamaan että se muuttuisi enemmän suotuisammaksi myös tietoturva-asioille. Tietoturva sanana, tällä hetkellä, aiheuttaa sellaisia väristyksiä, että sieltä se showstopper taas tulee. ... Jonka vuoksi olen pyrkinyt menemään tietosuoja-asia edellä, koska se on meidän kaltaisessa duunissa sellainen, että se on pakollista, kun se tulee laista. ... Eihän sitä tietosuojaa voi toteuttaa ilman tietoturvamekanismeja, niin on paljon helpompi sitä kautta mennä sinne sisälle ja unohtaa täysin se tietoturva sanana.”

ORG3 oli kokenut, että tietoturva voidaan joissain tilanteissa kokea tai nähdä toimintaa estävänä toimintana, vaikka haastateltava on pyrkinyt kommunikoimaan organisaatiossa tietoturvaa liiketoiminnan mahdollistajana:

> " Minä olen kaikille yrittänyt sanoa, että en minä tule tänne kauheasti estämään, mutta toki tulen katsomaan, että asiat tehdään lainsäädännön ja näiden (muiden vaatimusten) mukaisesti. Mutta silti sillä on sellainen huono kaiku, se on jossain vaiheessa sössitty, jolloin tietoturvasta on tullut kaiken toiminnan estäjä. Sen vuoksi minä olen sopinut, että mennään sillä tietosuojalla. Yritetään viedä se tietoturvallisuus sinne sellaisena asiana taustalla mukaan. ... Kun on puhuttu tietoturvavaatimuksista, ja on kysytty, että millaisia tietoturvavaatimuksia minulla on. niin olen vastannut, että ei minulla ole varsinaisesti mitään vaatimuksia, mutta liiketoiminnalla on tiettyjä edellytyksiä. Eli jos haluaa jotain liiketoimintaa tehdä niin se edellyttää, että olet asiasi hoitanut näin. ... Meillä on edellytyksiä lainsäädännöstä ja jos haluamme toimia niin meidän tulee tehdä näin. ... Ei tarvitse puhua, että ne olisivat tietoturvavaatimuksia. "

Tämä nostaa mielenkiintoisella tavalla esille tarketta kommunikoida oikein tietoturvan merkitystä ja tarkoitusta, jotta kaikilla työntekijätasoilla tietoturva voidaan ymmärtää ennemmin liiketoiminnan mahdollistajana kuin estäjänä. Näkemys tietoturvan estävästä vaikutuksesta voi johtua historiassa tietoturvan puhtaasti teknisestä toteutuksesta, joissa ei ole otettu huomioon organisaation liiketoimintaprosesseja ja kulttuurisia tekijöitä, samalla suosien estämiseen perustuvia strategioita. Nämä aiemmin paljon suositut ja osin ongelmalliset näkemykset tietoturvan toteutukseen ovat olleet esillä myös tietoturvakirjallisuudessa (Hedström ym. 2011; Baskerville ym. 2014). Tästä syystä organisaatioiden tulisi kiinnittää huomiota siihen, että arvonluontiprosessit on ymmärretty ja ne määrittävät tietoturvakontrollit. Sosiaaliset ja kulttuuriset tekijät ovat keskeisessä roolissa terveydenhuollossa, jossa digitalisaation aiheuttamasta muutoksesta huolimatta

toiminta perustuu vahvasti ihmisten tekemään työhön ihmisiä varten. Organisaation olisi kyettävä kommunikoimaan tietoturvan merkitystä tässä arvonluontiprosessissa, toiminnan varmistamisessa.

ORG3 tapauksessa haastateltava korosti tietoturvan edellytykseksi liiketoiminnan ja strategisten tavoitteiden huomioimisen, varsinkin terveydenhuolto puolella, jossa toiminnalla on vaikutus ihmisten terveyteen:

> "... niin ne tehdään kaikki (strategia, politiikka, periaatteet ja käytännöt) toimintaa ajatellen. Se perustoiminta tulee olla ajateltuna ja semmoisesta minä olen lähtenyt jo pois, tai kuvitelmasta, että mennään tietoturva edellä - ei mennä. Kuten sanoin se potilas hoidetaan ensin. Se hoidetaan, vaikka kone ei olisi kryptattu tai salasana olisi huono - niin potilas hoidetaan. ... Turvallisuus olisi onnistunut, jos se on sellaista jota käyttäjä ei huomaa tai meidän hommat toimii ja kukaan ei sano, että menipä hyvin tai huonosti. Se olisi kaikkiin sisään rakennettua toimintaa … tämän (tietoturvan) tulisi olla mahdollistaja, mutta ei estäjä. Se on hankalaa mutta olen pitänyt siitä kiinni, vaikka se ei ole kovin helppo toteuttaa"

Organisaatioiden tietoturvaohjeissa nostettiin esille sitä, että tietoturva on jokaisen työntekijän vastuulla ja vahva turvallisuustaso muodostuu vain, kun kaikki työntekijät aktiivisesti osallistuvat tietoturvallisuuden toteuttamiseen ja valvontaan.

6.3 Pohdinta

Tutkimuksen tarkoituksena oli ymmärtää tietoturvastrategioita terveydenhuolto kontekstissa. Tutkimuksen löydöksen yleisesti viittaavat, siihen että tietoturvan yleinen merkitys on tiedossa, varsinkin tietosuojan näkökulmasta. Tästä huolimatta tutkimuksen tulokset viittasivat siihen, että tietoturvan roolia tietosuojan varmistuksessa ei täysin aina ymmärretä. Kirjallinen tietoturvastrategia oli käytössä vain yhdessä tämän tapaustutkimukset tapauksista, ja tässäkin tapauksessa korostettiin tekemisen merkitystä politiikkojen ja strategioiden edelle. Tämä voidaan tulkita myös niin, että pelkkä suunnitelma ja tahtotila tietoturvasta ei riitä, vaan tietoturva olisi kyettävä implementoimaan organisaation operatiiviseen toimintaan. Lisäksi kaikissa tapauksissa tietoturvan kehittämistä ohjasi pääasiallisesti organisaation liiketoimintastrategia ja käytännön toiminta. Myös ylimmän johdon tahtotilalla ja näkemyksellä tietoturvan merkitykseen nähtiin olevan vaikutusta tietoturvan toteutukseen, muun muassa asetettujen prioriteettien ja annettujen resurssien kautta.

Kirjattujen tietoturvastrategioiden puute voidaan mahdollisesti perustella niiden selkeiden hyötyjen puutteella, vaikka kirjallisuudessa on esitetty tarvetta tietoturvastrategialle organisaatioiden pyrkiessä kehittämään tietoturva hallintoa ja ylemmän tason lähestymistä tietoturvaan (Carcary ym. 2016; Damenu & Beaumont 2017; Karanja 2017). Tietoturvastrategia voi olla hyödyllinen keino varmistaa tietoturvan ja liiketoiminnan yhdenmukaisuus, pyrkien samalla varmistamaan tietoturvan rooli liiketoiminnan mahdollistajana. Tämä voi olla

kriittinen menestystekijä terveydenhuollon alalla, jonka tavoitteena on edistää väestönterveyttä ja toiminnalla on suora vaikutus ihmisten terveyteen.

Tähän näkemykseen perustuen seuraavissa alaluvussa pohditaan tutkimuksen tuloksia suhteessa taustakirjallisuuteen ja esiteltyyn tietoturvastrategian viitekehykseen, ja ehdotetaan huomioitavia tekijöitä, jotka voivat olla edellytys toimivalle tietoturvastrategialle terveydenhuoltosektorilla.

6.3.1 Riskien huomioiminen

Tapausten liiketoimintastrategioissa tärkeimmäksi tavoitteeksi nostettiin organisaation kyky tarjota hoitamilleen potilaille laadukasta, turvallista ja tehokasta hoitoa. Tämä on ymmärrettävää, sillä organisaatioiden tehtäväksi on alaa koskevassa lainsäädännössä määritetty niiden pyrkimys väestön terveyden edistämiseen. Tästä johtuen organisaatioiden tulisi määrittää myös riskejä tietoturvaan liittyen, jotka voivat vaikuttaa potilaan saamaan hoitoon tai potilaan kokemaan luottamukseen palvelua tarjoavaa organisaatiota kohtaan. Etenkin luottamuksellisuuden rikkoutumisella, voi olla merkittävä vaikutus potilaan taloudelliseen, psykologiseen ja sosiaaliseen tilanteeseen (Romanou 2017). Henkilökunnan näkökulmasta on tärkeää kommunikoida myös tietoturvan merkitystä tietosuojan varmistamisessa, sillä tietosuoja on osa tietoturvaa, eikä käsitä vain henkilökunnan vaitiolovelvollisuutta. Henkilökunnan olisi ymmärrettävä, että myös heidän tekemillään toimilla tietojärjestelmään liittyen voi olla vaikutusta organisaation kokonaistietoturvaan, ja sen kautta potilaan kokemaan luottamukseen palveluntarjoajaa kohtaan.

Yhdessä tapauksista riskienhallintapolitiikassa nostettiin esille kriittisiksi huomioitaviksi uhkiksi ne riskit, jotka voivat johtaa potilaan välittömään hoitoon vaativan toiminnan häiriintymiseen, toiminnan jatkuvuuden vaarantumiseen taloudellisen menetyksen seurauksena ja maineen tai luottamuksen menetykseen. Nämä kaikki riskit voivat toteutua tietoturvan vaarantumisen seurauksena, vaikuttaen mahdollisesti sekä organisaation että potilaaseen. Tämän vuoksi terveydenhuolto alalla tietoturva voidaan nähdä tärkeän strategisen ongelmaksi, jonka hallintaan alan organisaatiot tarvitsevat menetelmiä. Tietoturvaloukkauksella voi kirjallisuuden mukaan olla suuria rahallisia ja maineellisia vaikutuksia organisaation toimintaan, muun muassa kasvaneiden kulujen, vähentyneen tuottavuuden ja menetettyjen tuottojen muodossa (Herath ym. 2010). Terveydenhuollon näkökulmasta vakava tietoturvaloukkaus voi vaikuttaa terveydenhuolto-organisaation kykyyn tarjota hoitoa sitä tarvitseville. Lisäksi tietovuodolla voi olla vakavia seurauksia organisaation maineelle, ja vaikuttaa negatiivisesti myös yhteistyökumppaneihin (Herath ym. 2010).

Järjestelmien monimutkaistuminen ja teknologioiden nopea kehitys on nähty tietoturvakirjallisuudessa ja käytännössä usein haasteeksi tietoturvalle. Kuten myös osassa tapauksia tuotiin esille tietoverkkojen merkityksen kasvu ja esimerkiksi pilviteknologiat tuovat mukanaan uusia haasteita, jotka organisaation olisi kyettävä huomioimaan. Varsinkin verkkoon kytketyt lääkinnälliset laitteet, voivat toimia potentiaalisena hyökkäysvektorina tai tietovuodon lähteenä, mikäli niiden tietoturva ei ole kunnossa. Ongelmalliseksi lääkinnälliset laitteet

tekevät osaltaan niiden hyväksymismenettely (CE-merkintä), joka ei sisällä kyberturvallisuuden vaatimuksia. Kuten ORG3 tapauksessa tuotiin esille, laitevalmistajat ja ohjelmiston tarjoajat voivat olla haluttomia päivittämään lääkinnällisiä laitteita tai ohjelmistoja, sillä nykyinen hyväksymismenettely CE-merkintään liittyen vaatii CE-merkinnän päivityksen esimerkiksi ohjelmistopäivityksen seurauksena. Tästä johtuen lääkinnällisiin laitteisiin voidaan joutua soveltamaan erillisiä tietoturvastrategioita niiden suojaamiseksi, esimerkiksi eristämällä muusta verkosta. Organisaatiot voivat kutenkin tarvita uusia strategioita, mikäli lääkinnällisten laitteiden olisi tarkoitus toimia myös verkon yli.

Riskienhallinta ja riskiarvio toimii tärkeänä lähteenä organisaation uhkatiedolle. Tästä syystä riskienhallinta on historiallisesti toiminut tärkeässä roolissa organisaatioiden kehittäessä tietoturvastrategioita. On kuitenkin huomattava, että kaikkia uhkia ja niiden todennäköisyyksiä ei välttämättä kyetä ennalta tarkasti tunnistamaan tai arvioimaan (Neghime & Scarlat 2013). Tästä johtuen myös terveydenhuolto alan organisaatiot voivat tarvita erillisiä strategioita riskienhallinnan rinnalle (Baskerville ym. 2014). Terveydenhuollon kohtaamat uhkat voivat suurestikin erota muiden alojen uhkista, ja esimerkiksi hyökkääjät voivat olla hyvinkin motivoituneita pyrkiessä rahallisen hyödyn saavuttamiseen anastetuilla terveystiedoilla. Ongelmallista riskienhallinnasta tekee myös se, että mikäli riskit kattavat vain saatavuuteen liittyviä uhkia, voi se johtaa organisaatiota suosimaan ehkäisyyn perustuvia strategioita. Tämä voi olla tärkeää huomioida terveydenhuollon organisaatiossa, joissa tämän tutkimuksen tapausten mukaan saatavuus tietoturva tavoitteena on tärkeässä roolissa. Organisaatioiden olisi kyettävä tasapainottamaan erilaisten tietoturvastrategioiden välillä, kyetäkseen muodostamaan tehokkaan kokonaisvaltaisen puolustuksen riskeihin perustuen (Kayworth & Whitten 2010; Ahmad ym. 2014).

Oman haasteensa, varsinkin julkisen puolen terveydenhuollon organisaatioissa asettaa suuret henkilöstömäärät ja hallintorakenteet. Suuren henkilöstön saaminen sitoutettua organisaation tietoturvapolitiikkaan voi olla haasteellista. Sillä vaikka tiedon luonteen vuoksi voi olla selkeää, että tietoa tulee käsitellä asianmukaisesti, voidaan esim. tietoturvaapolitiikka jättää huomitta, joko huolimattomuuden tai piittaamattomuuden seurauksena. Esimerkiksi ORG2 haastateltava kuvaili kuinka hyvin henkilöstön ymmärrystä tietoturvan merkitystä:

> ”Mielestäni varsin hyvin, selkeää että täällä (terveydenhuoltosektorilla) käsitellään sen luontoista tietoa, että niitä ei pitäisi millään tavalla luvattomasti käsitellä. Tietysti porukassa on aina henkilöitä, jotka eivät pelisääntöjä noudata”

Tämän vuoksi organisaatiot tarvitsevat ymmärrystä uhkiin liittyen organisaation ulkoisen toimintaympäristön lisäksi, myös organisaation sisältä, jotta mahdolliset uhkat kyetään tunnistamaan ja niiden kriittiset vaikutukset liiketoimintaan estämään. Riskejä tulisi tunnistaa muun muassa lainsäädäntöön, teknologiaan, henkilöstöön ja ulkoisiin uhkatekijöihin liittyen, ja hyödyntää tätä tietoa tietoturvastrategioissa.

6.3.2 Tietojärjestelmien huomioiminen kokonaisuutena

Organisaatioiden olisi kyettävä huomioimaan tietojärjestelmät kokonaisuutena, jossa on osatekijöinä ovat teknologiat, ihmiset ja prosessit. Samaan tapaan organisaation olisi kyettävä rakentamaan organisaation tietoturva huomioimalla nämä kaikki tietojärjestelmän osatekijät. Jonkin osa-alueen huomiotta jättäminen voi johtaa haavoittuvaisuuteen tietojärjestelmässä. Kaikissa tapausorganisaatioissa tietoturvaa oli pyritty rakentamaan teknisestä näkökulmasta, samaan aikaan hyödyntäen henkilöstön perehdytystä ja koulutusta tietoturvaan ja tietosuojaan liittyen. Tämä on tärkeää, sosiaalisen kontekstin huomioimiseksi tekniset kontrollit tarvitsevat ei-teknisiä ratkaisuja, kuten tietoturvapolitiikkaa ja tietoturvakoulutusta kokonaistietoturvan varmistamisessa (Damenu & Beaumont 2017). Kustannustehokkaan tietoturvan aikaansaamisessa voi kuitenkin olla tarvetta ymmärtää eri tietoturvakontrollien välisiä vuorovaikutussuhteita, jotta kyetään välttämään tarpeettomia tietoturvakontrolleja olemassa olevien kontrollien rinnalle (Sveen ym. 2009). Tietojärjestelmien sosioteknisen luonteen huomioiminen voi korostua entisestää kohdennettujen hyökkäysmenetelmien kehittyessä.

Tietoturvakirjallisuudessa on tunnistettu, että lisääntynyt kohdennettujen hyökkäysten kehittyneisyys ja monimutkaisuus siirtää organisaatioiden puolustusta estävistä strategioista enemmän reagoivien strategioiden suuntaan, joissa organisaatiot pyrkivät reagoimaan tilannekuvaan perustuen mahdollisiin uhkiin (Baskerville ym. 2014). Nämä strategiat voivat mahdollistaa organisaatioiden reaktiokykyä tunnistamattomiin uhkiin, mutta nostaa kustannuksia tietoturvaan liittyen, muun muassa SOC-toiminnan ylläpidosta johtuen.

Tietoturvan toteutus voi olla jokseenkin haastavaa terveydenhuoltosektorilla, jossa toimintaa on ympärivuorokauden. Lisäksi järjestelmien tulisi olla aina saatavilla toiminnan mahdollistamiseksi, ja tehokkaan ja turvallisen hoidon tarjoamiseksi. Tiloissa liikkuu paljon ihmisiä ja henkilöstö on tiiviissä vuorovaikutuksessa ihmisten kanssa, jonka vuoksi tietoturvaan toiminta tulisi olla tarkkaan mietittyä, mutta kaikkiin tilanteisiin on mahdotonta varautua rajallisilla resursseilla. Tietoturvan vaatimuksista ja järjestelmien saatavuudesta huolimatta, organisaation olisi kyettävä auttamaan välitöntä hoitoa tarvitsevia potilaita. Tietojärjestelmillä ja tiedolla on kuitenkin keskeinen rooli alan organisaatioissa digitalisaation lisätessä tietojärjestelmien merkitystä operatiivisessa toiminnassa. Tietoturvastrategia voi toimia keinona varmistaa tietoturvan yhdenmukaisuus niin teknologisen kehityksen, että liiketoiminnan kanssa.

Kuten osassa tapauksissa tuli esille tietoturva olisi kyettävä rakentamaan järjestelmiin siten, että se olisi huomaamatonta, mutta toimivaa. Terveydenhuollon tietojärjestelmiin ei voida määrittää tietoturvakontrolleja ja -prosesseja ottamatta huomioon toiminnan tarpeita, sillä varsinkin terveydenhuollossa, jossa henkilöstö omaa vahvat ammatilliset arvot, voivat arvoristiriidasta johtuen pyrkiä kiertämään olemassa olevia kontrolleja (Hedström ym. 2012). Loppujen lopuksi työntekijät pyrkivät tekemään oman työnsä, ja terveydenhuollossa auttamaan potilasta ja edistämään tämän terveyttä.

Esimerkiksi ORG3 tapauksessa haastateltava jopa pyrki välttämään tietoturvasta ja tietoturvavaatimuksista puhumista, ja pyrki ennemmin kommunikoimaan tietosuojaa ja liiketoiminnan edellytyksiä tietoturvan edistämiseksi,

alalla vielä puuttuessa yleiset tietoturvaan liittyvät vaatimukset. Organisaatiossa olisi kyettävä kaikilla tasoilla ymmärtämään tietoturvan rooli suhteessa tietosuojaan, jotta myös tietoturva tulee huomioiduksi, vaikka tietoturvalle ei olemassa yhtä selkeitä vaatimuksia laissa kuten tietosuojalle.

6.3.3 Kulttuurin merkitys

Tapausten perusteella ylin johto ja henkilöstö ymmärtävät tietoturvan merkityksen ja suhtautuvat siihen positiivisesti. Tapauksissa kulttuuria tietoturvaan liittyen oli pyritty huomioimaan ottamalla työntekijöitä mukaan tietoturvan kehitykseen ja kouluttamalle henkilöstöä tietoturvaan liittyen. Tietoturvakulttuurin kehittäminen on tärkeää, sillä kaikki henkilöstöön kohdistuva ohjeistus ja koulutus pyrkii vaikuttamaan organisaation sisäiseen kulttuuriin. Strategisesta näkökulmasta on tärkeää huomata, että kuinka sosiaalista muutosta pyritään kommunikoimaan.

Ongelmat liittyen ihmisten suhtautumiseen tietoturvaa voidaan osin selittää henkilöstön ja tietoturvan poikkeavista tavoitteista (Hedström ym. 2011). Tämän vuoksi tietoturvaa suunnittelevien olisi ymmärrettävä sekä henkilöstön tekemää työtä, että heidän omaamia arvoja. ORG2 tapauksessa nostettiin esille vuorovaikutuksen tärkeyttä ja tarvetta kehittää sitä eri toimijaryhmien ymmärtämiseksi.

Terveydenhuollossa työntekijät pyrkivät pääasiallisesti hoitamaan potilaita. Tätä tavoitetta tukee henkilöstön ammatilliset arvot, jotka muovautuvat organisaation sisäisen kulttuurin, eettisten ohjeiden ja henkilökohtaisten arvojen vaikutuksesta. Tietoturvakirjallisuudessa on havainnut organisaation kulttuurin aiheuttaman haasteen tietoturvan toteutukselle (Da Veiga & Eloff 2007; Kayworth & Whitten 2012). Tästä johtuen tietoturvan toteutuksessa tulisi pyrkiä varmistamaan tietoturvaprosessien yhdenmukaisuus organisaation kulttuurin kanssa. Strategisesta näkökulmasta henkilöstön ottaminen mukaan tietoturvan suunnitteluun voi olla tehokas keino varmistaa kulttuurin ja arvojen huomioiminen tietoturvan suunnittelussa ja toteutuksessa. Tätä keinoa oli pyritty myös hyödyntämään kaikissa tapauksissa.

Tapausten perusteella työntekijät pääsääntöisesti motivoituneita tietoturvan toteutukseen, mikäli he ymmärtävät suojeltavan tiedon (mm. potilastieto) merkityksen ja mahdollisen tietovuodon vaikutukset hoidettavaan potilaaseen. Toisaalta kirjallisuus on tunnistanut, että työntekijät aikomus noudattaa tietoturvapolitiikka voi erota varsinaisesta toiminnasta. Toimintaan voi vaikuttaa esim. kiire, muistamattomuus ja välinpitämättömyys. Suotuisan tietoturvakulttuurin ylläpitäminen vaatii kommunikaatiota tietoturvan ja suojattavan tiedon merkityksestä. Tietoturvastrategia ja sen määrittämät mittarit voivat auttaa tietoturvan kommunikoinnissa ja jalkauttamisessa operatiiviseen toimintaan. Esim. hyödyntämällä tietoturvan osa-alueita mittaavia tekijöitä, joihin myös työntekijät voivat toiminnallaan vaikuttaa.

Linjaamalla varsinainen tietoturvastrategia suhteessa organisaatioiden varsinaiseen tarkoitukseen edistää väestön terveyttä voi organisaatio hyötyä alalla työskentelevien ihmisten luontaisesta pyrkimyksestä auttaa ihmisiä - myös

organisaatioiden strategian tärkeimmäksi tavoitteeksi oli määritetty potilaiden turvallinen hoito. Ymmärtämällä tietoturvan merkityksen tähän tavoitteeseen pääsemiseksi organisaatio voi kyetä luontaisesti motivoimaan työntekijöitä ja kehittämään organisaation tietoturvakulttuuria.

Kommunikaatio tietoturvan merkityksestä on tärkeää, sillä työntekijät voivat ymmärtää tietosuojan merkityksen, mutta eivät välttämättä osaa yhdistää tietoturvan edellytystä tietosuojan saavuttamiseksi, ilman kommunikaatiota asiasta. Esimerkiksi työntekijöille voi olla selvää, että potilastietoja ei tule tarkastella ilman hoitosuhdetta, mutta eivät välttämättä ymmärrä kuinka henkilökohtaisten laitteiden kytkeminen organisaation verkkoon voi toimia uhkalähteenä potilastietojen tietosuojalle. Kirjallinen tietoturvastrategia voi auttaa tietoturvan merkityksen kommunikoinnissa suhteessa organisaation tavoitteisiin ja näin auttaa tietoturvakulttuurin rakentamisessa.

Ylemmän johdon näkemyksellä ja tuella voi olla suuri vaikutus työntekijöiden ajatuksiin tietoturvasta, sillä ylemmän johdon ottaessa esille tärkeitä tietoturvaan liittyviä ongelmia, voi se motivoida myös henkilöstöä kehittää omaa toimintaa tietoturvan ongelmiin liittyen. Tapausten tietoturvapolitiikassa ja ohjeistuksessa nostettiin esille sitä, että tietoturva on jokaisen työntekijän vastuulla ja vahva turvallisuustaso muodostuu vain, kun kaikki työntekijät aktiivisesti osallistuvat tietoturvallisuuden toteuttamiseen ja valvontaan. Henkilöstön olisi myös ymmärrettävä mitä tämä käytännössä tarkoittaa.

Organisaatioiden olisi kyettävä kommunikoimaan myös sitä, että tietoturva ei ole vain tekninen ongelma, johon myös organisaation yleisellä kulttuurilla on vaikutus. Aiempi tekninen lähestyminen tietoturvaan yhdistettynä estämiseen perustuviin strategioihin, on voinut saada aikaan tilanteen, jossa tietoturva nähdään toiminnan estäjänä.

6.3.4 Tietoturvavaatimukset

Terveydenhuolto ala on tarkkaan säädelty, ja alaan liittyy paljon lakeja ja säädöksiä, jotka organisaatioiden tulisi huomioida omassa toiminnassaan. Nämä lait pyrkivät varmistamaan yksilön oikeudet ja turvallisuuden hoitoon ja luottamukselliseen tietoon liittyen.
Tietoturvakirjallisuudessa määräysten ja lainsäädännön mukaisuus voi motivoida organisaatioita implementoimaan tietoturvastrategian organisaation käyttöön. (Horne ym. 2015) Lisäksi organisaatioiden pyrkimys standardin ja parhaisiin käytöntöihin voi toimia tällaisena alustavana tekijänä tietoturvastrategialle. Tämän tutkimuksen tapaukset eivät olleet hakeutuneet täyteen standardin mukaisuuteen (esim. ISO27001), sen sijaan näitä parhaita käytäntöjä ja standardeja käytettiin työkaluina tietoturvan kehityksessä. Tämä voi osaltaan selittää miksi tapauksissa ei ollut käytössä tietoturvastrategioita, vaikkakin ORG3 tapauksessa haastateltava toivoi yhtenäisiä tietoturvan vaatimuksia niin julkiselle sektorille kuin terveydenhuoltoon operatiivisen ja strategisen työn helpottamiseksi. ORG3 näki ylimmän johdon asennoitumisen tietoturvaan suotuisaksi, mutta toivoi yhtenäisiä vaatimuksia työn helpottamiseksi:

> "mielestäni kaikki alkaa pikkuhiljaa ymmärtämään tämän kokonaisuuden, mutta se mikä on vielä, mun mielestä, kehittämisen paikka, ja en puhu vain meidän talosta, mutta sitä vaatimusta ei vielä oikein ole vielä olemassa julkisella puolella … ylin johto tukee ja ovat sitoutuneita - se on oikeasti hyvä asia. "

Esitetty tarve julkisenpuolen tietoturvavaatimuksille, johti ajatuksesta, että niistä kyettäisiin johtamaan julkista terveydenhuoltoa koskevia arviointiperusteita tietoturvan arviointiin ja seurantaan. Terveydenhuolto-alalla tietosuoja on hyvin ymmärretty ja sen rooli on tarkkaan määritelty ja ohjeistettu. Vaikka tietosuoja on osa tietoturvaa, tästä huolimatta tietoturva ei ole välttämättä saanut niin vakiintunutta roolia tämän alan organisaatioissa, jonka vuoksi tietoturva voidaan yhä nähdä joissain tilanteissa teknisenä ongelmana. Tapauksissa tätä ongelmaa on pyritty ratkaisemaan ohjeistamalla ja perehdyttämällä henkilöstöä tietoturvaan liittyvissä asioissa.

Tapauksissa tietoturvan toteutus ja prosessit erosivat odotetusti toisistaan, vaikka kaikki tapaukset olivat noin saman suuruisia julkisen puolen toimijoita. Tämä voi olla selitettävissä yhtenäisen ohjeistuksen puuttumisesta terveydenhuoltosektorilla. Tärkeitä tietolähteitä tapauksissa olivat, VAHTI-ohjeiden lisäksi, muun muassa tietoturvastandardit (mm. ISO 27000), Kanta-ohjeet, julkisen terveydenhuollonlainsäädäntö, mm. tietoturvaan, tietosuojaan ja lääkinnällisiin laitteisiin liittyen, ja riskienhallinnan standardit.

6.3.5 Liiketoiminnalliset tarpeet

Tietoturvan ja mahdollisen tietoturvastrategian tulisi olla linjassa liiketoiminta- ja IT-strategian kanssa. Tapauksissa nousi esille, kuinka tietoturvassa pyritään kohti liiketoiminanallisia tavoitteita. Organisaatioiden toiminta perustuu pyrkimykseen edistää väestön terveyttä. Varsinkin yksityisyyden rikkoutumisella voi olla merkittäviä vaikutuksia potilaan henkiseen ja taloudelliseen hyvinvointiin. Lisäksi tietoturvaprosessit olisi suunniteltava siten, että ne aiheuttavat mahdollisimman vähän estettä toimintaprosesseille ja soveltuisivat organisaation kulttuuriin. Järjestelmien saatavuudesta riippumatta organisaatioiden olisi kyettävä välittömän hoidon tarjoamiseen, joka edellyttää tietojärjestelmistä riippumattomien varautumisjärjestelmien ylläpidon. Tämä voi osaltaan asettaa haasteen toiminnan suunnittelulle ja edellyttää strategista lähestymistapaa tämän toiminnan varmistamisessa rajallisilla resursseilla. On kuitenkin odotettavissa, että tietojärjestelmien ja niiden sisältämän tiedon rooli ja merkitys tulee kasvamaan digitalisaation vaikutuksesta. Digitalisoituminen auttaa organisaatioita tarjoamaan tehokkaampaa ja turvallisempaa hoitoa, mm. hyödyntämällä organisaation käytössä olevaa tietoa järjestelmien avulla. Tietoturvalla on keskeinen rooli tämän toiminnan mahdollistamisessa.

Esimerkiksi ORG2 tapauksessa tietoturvapolitiikasta nousi esille riskienhallinnan merkitys tietoturvan toteutukselle. Riskienhallintapolitiikassa löytyi selkeä linkitys liiketoiminnallisten tavoitteiden, esimerkiksi potilaan hoidon laadun ja turvallisuuden varmistaminen ja riskienhallinnan välillä. Näiden liiketoiminnallisten tavoitteiden merkitys noussut yhtä selvästi noussut esille tietoturvapolitiikassa.

Tapausten liiketoimintastrategioissa nousi esille etenkin potilaan asema ja hoidon merkitys. Strategioissa ei suoraan esiintynyt viittausta tietoturvan tai tietosuojan merkitykseen. Strategioissa nousi esille kyky ja tarve tiedolla johtamiseen, jonka varmistamisessa tietoturvalla on tärkeä merkitys. Strategioissa nousi esille myös organisaatioiden kyky tarjota yhä enemmän sähköisiä palveluita, ja tämä voi puolestaan tulevaisuudessa kasvattaa tietoturvan merkitystä: viestintäteknologioiden kasvattaessa potentiaalista hyökkäyspinta-alaa. Tapausten tietoturvapolitiikoissa ja tietoturvaohjeissa nostettiin esille yleiset tietoturvatavoitteet luottamuksellisuuden, eheyden ja saatavuuden merkitystä.

Posthumus & von Solms (2004) mukaisesti tietoturva tulisi kuulua ylimmän johdon prioriteetteihin ja integroida tietoturva osaksi yrityksen hallintoa. Tapauksissa tietoturvaan liittyviä asioita käsiteltiin ylimmässä johdossa, mutta ORG3 tapauksessa johto nähtiin olevan vielä siinä kypsyysasteessa, että tietoturvaan liittyvistä tapahtumista ei haluttu tilannetietoa kuukausitasolla. Tietoturvaa käsiteltiin vähintään vuosittaisessa tilannekatsauksessa.

Johdontuen merkitys tietoturvalle nousi esille kaikissa tapauksissa, ja ylin johto nähtiin suhtautuvan tietoturvaan myönteisesti ja sen merkitys ymmärrettiin. Kaikki haastateltavat näkivät, että tietoturvaan on riittävät resurssit sen toimivuuden varmistamiseksi. Johdon kiinnostusta tietoturvaan nähtiin edesauttavan tietoturvan esiintyminen mediassa. Toisaalta riittävien resurssien varmistaminen tietoturvaan ja sen jatkuva kehitys voi vaatia pitkäaikaista sitoutumista tietoturvaan, jotta toiminta on proaktiivisempaa, joka voi johtaa usein parempiin tuloksiin tietoturvan osalta (Kwon & Johnson 2013). Kirjallinen tietoturvastrategia voi olla keino varmistaa johdontuki ja resurssit, muun muassa ymmärtämällä tietoturvan pitkäaikaiset tavoitteet ja merkitys toiminnalle.

Tietoturvastrategia voi toimia menetelmänä tietoturva organisaation voimavarojen rakentaja ja arvonluontiprosessien mahdollistajana, jolloin tietoturva ei nähdä vain pakollisena kuluna liiketoiminnassa. Kuten tapauksissa, ajoittain tapahtuvat tietoturvatapahtumat voivat auttaa tietoturvan nostamista ajankohtaiseksi asiaksi, mutta se ei välttämättä riitä tehokkaan tietoturvan saavuttamiseen. Ylemmän johdon olisi kyettävä jatkuvaan tietoturvan tukemiseen riittävien resurssien varmistamiseksi, vaikka uhkat eivät ilmenisikään organisaatiossa. Tämä voi auttaa välttämään ad-hoc tyylisten tietoturvainvestointeja, jotka eivät ole välttämättä linjassa organisaation liiketoiminnan ja pitkäaikaisten tavoitteiden kanssa (Ahmad ym. 2014). Turhat tai tarpeettomat tietoturvainvestoinnit voivat näin hukata organisaation käytössä olevia resursseja.

Tapauksista nousi esille tietoturvan strategiseen seurantaan soveltuvien mittareiden puute. Näitä mittareita oltiin tapauksissa kehittämässä tai johto ei ollut halukas sitoutumaan vaatimuksiin. Tietoturvakirjallisuudessa tällaiset mittarit on nähty hyödyllisiksi, sillä ilman seurantaa organisaation ei voi tietää missä se voi kehittyä. Varsinkin tietoturvan kulttuurin arviointiin soveltuvien mittareiden puute voi hankaloittaa tietoturva kulttuurin arviointia ja ollaanko mahdollisista investoinneista esim. tietoturvakoulutukseen saatu haluttua hyötyä.

Lisäksi strategisista mittareista johdetut operatiiviset mittarit, joihin myös työntekijät kykenevät osaltaan vaikuttamaan voivat toimia tehokkaana motivaatiotekijänä henkilöstön tietoturvaan sitoutumisessa ja hyödyntämisessä

tietoturvan toteutuksessa (Harath ym. 2010). Varsinkin terveydenhuollossa, jossa tietoturvakulttuurin luonti voi olla haasteellista mahdollisesta tietoturvan arvojen ja ammatillisten arvojen konfliktista.

Tapauksissa nähtiin, että tietosuoja on henkilöstön osalta hyvin ymmärretty, ja se toisaalta on ymmärrettävää, sillä terveydenhuollon tietosuojan perusta on esitetty jo Hippokrateen valassa:

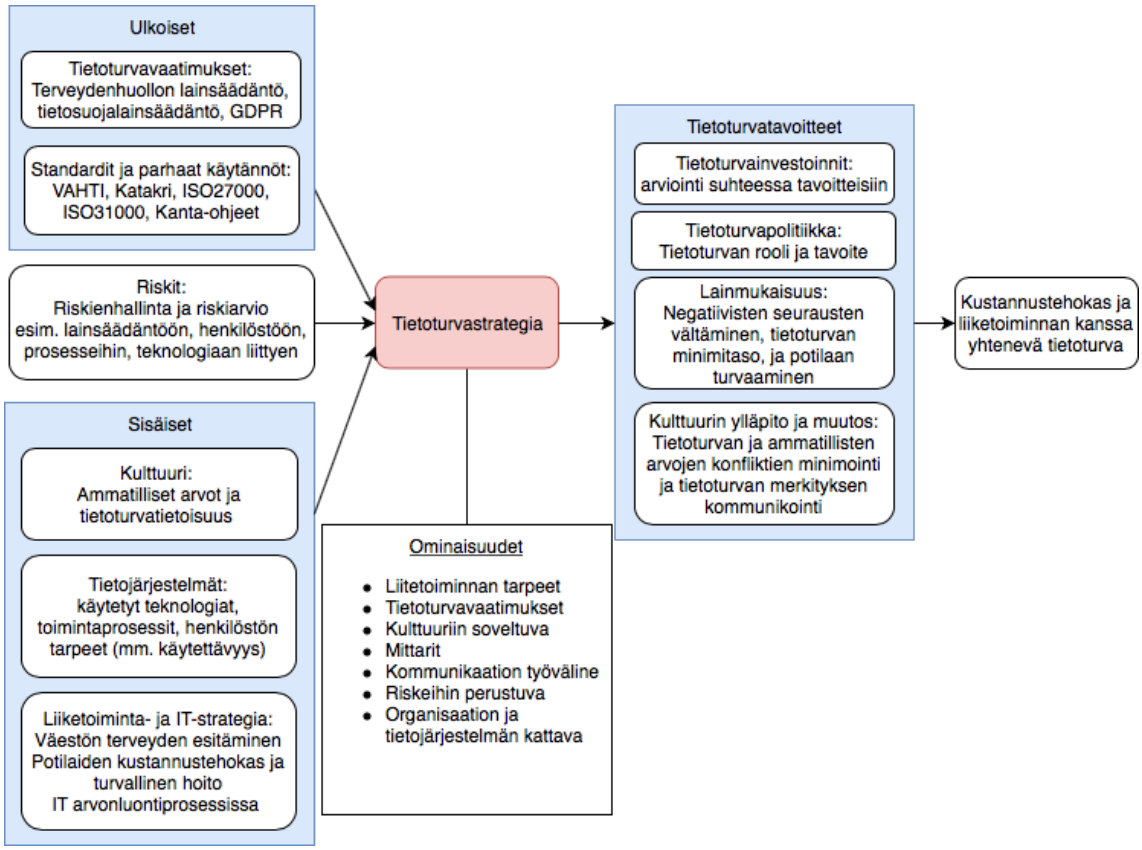
> ”Mikäli parannustyössäni tai sen ulkopuolella ihmisten parissa näen tai kuulen sellaista, mitä ei pidä levitettämän, vaikenen ja pidän sen salaisuutena.”

Ymmärrys tietosuojasta voi toimia tehokkaana lähtöasetelmana, organisaatioiden pyrkiessä kommunikoimaan tietoturvan roolia tietosuojan turvaamisessa, ja tiedon luottamuksellisuuden varmistaminen vaatii enemmän kuin henkilöstön vaitiolovelvollisuutta.

Tapauksissa oli tyypillistä, että tietoturvaa tarkasteltiin ja suunniteltiin strategisella tasolla noin 1 vuoden välein, ja varsinainen tietoturva todettiin toteutuvan käytännön toiminnan kautta. Organisaatiot pyrkivät ohjaamaan tietoturvan toteutusta 2-4 viikon välein, muun muassa erilaisissa työryhmissä ja kokouksissa. Tietoturvakirjallisuuden näkökulmasta tämä voi johtaa reaktiiviseen tietoturvaan, joka ei aseta pitkäaikaisia tavoitteita tietoturvan toteutukseen esimerkiksi 3-5 vuoden aikavälille, ottaen samalla huomioon myös liiketoiminnalliset tavoitteet. Varsinkin tietoturvakulttuurin muutos voi vaatia organisaatiolta pidempiaikaista sitoutumista halutun muutoksen aikaansaamiseksi. Toisaalta teknologian ja tietoturvan nopea kehitys voi vaatia nopeita muutoksia, tietoturvan ylläpitämiseksi, jonka vuoksi myös tietoturvastrategia tulisi olla riittävän dynaaminen, jotta oleellisiin muutoksiin kyetään reagoimaan.

6.3.6 Terveydenhuolto-organisaation tietoturvastrategia

Tulosten perusteella tietoturvastrategiaa ei nähty kriittiseksi dokumentiksi organisaation toiminnan kannalta, sillä sen hyödyt verrattuna esimerkiksi varsinaiseen liiketoimintastrategiaan ja tietoturvapolitiikkaan eivät olleet selvät. Organisaatioiden halukkuuteen ottaa käyttöön voi vaikuttaa myös konseptin vaihtelevat määritelmät tieteellisessä kirjallisuudessa. Tietoturvastrategialle ei ole olemassa selkeäitä ohjeita esimerkiksi siitä mitä sen tulisi sisältää ja kuinka sellainen voitaisiin kehittää. Organisaatiot voivat olla haluttomia sitoutumaan strategisiin tietoturvatavoitteisiin, ilman että on selkeää näyttöä siitä, että se tuottaa tavoiteltua hyötyä. Muiden strategioiden kehittäminen ja hyödyntäminen tyypillisesti pyrkii toiminnan kehittämiseen, joka pyrkii loppukädessä joko säästöihin tai tehokkuuden paranemiseen. Tietoturvanosalta implementoitu strategia ei välttämättä johda rahallisiin hyötyihin sillä tietoturvan arvo on sen kyvyssä estää jotain tapahtumasta, jolloin organisaatio ei voi tietää johtuuko haittatapahtumien poissaolo toimivasta tietoturvastrategiasta vai uhkien poissa olosta tietyllä ajanhetkellä. Kuvio 3 esittää tapausten ja kirjallisuuskatsauksen perusteella tunnistetut huomioitavat tekijät, jotka auttavat varmistamaan tietoturvastrategian toimivuuden terveydenhuoltosektorilla ja linjaamaan tietoturvaa kohti määritettyjä tietoturvatavoitteita.



Kuvio 3: Tietoturvastrategia terveydenhuollon organisaatiossa

Tietoturva voi saada vähemmän huomiota organisaatiossa ennen kuin jotain odottamatonta tapahtuu ja tietoturvatapahtumalla on vaikutuksia organisaatioon operatiiviseen toimintaan. Tietoturvastrategialla voidaan varmistaa tietoturvan huomioiminen toiminnassa ja pyrkiä tietoturvan jatkuvaan kehitykseen ja arviointiin perustuen strategiassa määritettyihin pitkän aikavälin tavoitteisiin. Varsinkin terveydenhuolto sektorilla, jossa kulttuurin muutos voi vaatia pitkäaikaista sitoutumista ja resursseja. Lisäksi tietoturvastrategia voi toimia kommunikoinnin työvälineenä ylemmän johdon, operatiivisen toiminnan ja henkilöstön välillä ja ohjata tietoturvainvestointeja pohjautuen organisaation liiketoiminnallisiin tavoitteisiin. Tietoturvainvestointien hyötyjen arviointi voi usein olla haastavaa, sillä ne eivät aina johda suoraan rahallisiin hyötyihin, kuten tehokkuuden parantamiseen tai kustannussäästöihin. Tästä syystä tietoturvastrategia voi auttaa varmistaa investoinnit tietoturvaan suhteessa IT-investointeihin, joiden hyödyt voivat olla helpompia mitata.

7 YHTEENVETO

Tietoturvastrategia terminä on paljon käytetty tietoturvakirjallisuudessa, mutta tästä huolimatta se on saanut suhteellisen vähän huomiota tietoturvakirjallisuudessa. Aiempi kirjallisuus on tunnistanut useita erilaisia tietoturvastrategioita organisaatioiden tietoturvan toteutukseen ja todennut näiden erilaisten strategioiden yhdistämisen, johtavan tehokkaampaan tietoturvaan kuin hyödyntämällä vain yhdentyyppistä strategiaa. Kokonaisvaltaisia, koko organisaation kattavia tietoturvastrategioita, jotka pyrkivät yhdistämään kaikki organisaation tietoturvatoiminnan yhtenäiseksi kokonaisuudeksi, on tutkittu vähän (Karanja 2017). Tämä tutkimus selvitti millainen tällainen kokonaisvaltainen tieturvastrategia olisi terveydenhuolto-organisaatiossa, ja mitkä ovat huomioitavia tekijöitä sen toimivuuden varmistamisessa. Kirjallisuuskatsauksen pohjalta tunnistettiin tietoturvastrategian edellyttävän organisaatioon liittyvien riskien, lainsäädännön, tietoturvaohjeiden, kulttuurin, tietojärjestelmien ja liiketoiminnallisten tarpeiden huomioimista.

Tutkimus valaisi mielenkiintoisella tavalla tietoturvaa terveydenhuollon organisaatioissa. Näiden organisaatioiden tietoturvan toteutukseen sovelletut strategiat voivat erota suurestikin muiden alojen vastaavista, muun muassa näiden organisaatioiden poikkeavista toiminnallisista tavoitteista, kulttuurista ja tiedon merkityksestä. Prosessit ja tavoitteet pyrkivät potilaiden hoitoon ja väestön terveyden edistämiseen, vaikka järjestelmät eivät olisi saatavilla tai toiminta rikkoisi hetkellisesti esimerkiksi tietoturvaan liittyvää ohjeistusta. Organisaatioiden tunnistamalla nämä tavoitteet, kykenee ne rakentamaan strategisesti tietoturvaprosessit siten, että hoitoa vaativien potilaiden auttaminen on mahdollista aiheuttamatta tarpeetonta riskiä organisaation jatkuvuudelle.

Terveydenhuoltoalalla tietoturvalla on kriittinen merkitys alan organisaatioiden toiminnassa. Organisaatioiden olisi kyettävä tarjoamaan tietoon perustuvaa hoitoa potilaille, samalla pyrkien varmistamaan potilaaseen liittyvän tiedon tietosuoja. Tietosuojalla on pitkä historia terveydenhuoltosektorilla ja se on tarkkaan määritelty laissa. Historiallisesti tietosuoja on pyritty varmistamaan ehkäisemällä tietojen luvatonta levitystä, muun muassa vaitiolovelvollisuudella. Uuden kehittyneet kohdennetut hyökkäykset voivat kuitenkin luoda tulevaisuuden haasteen terveydenhuollon organisaatioiden tietoturvantoteutukselle, arkaluontoisen terveystiedon toimiessa houkuttelevana kohteena rahallista hyötyä tavoittelevalle hyökkääjälle. Oman haasteensa asettaa teknologian merkityksen kasvu (esim. pilvipalvelut) ja teknologiat, joiden tietoturvassa saattaa olla puutteita (esim. lääkinnälliset laitteet). Tutkimuksessa nousi esille, kuinka linkittämällä tietosuoja tietoturvaan ja kommunikoimalla tietoturvan merkitystä tietosuojan varmistamisessa, alan organisaatiot voivat mahdollisesti hyödyntää alalla työskentelevien henkilöiden ymmärrystä tietosuojasta tietoturvakulttuurin kehittämisessä. Organisaation olisi kyettävä kommunikoimaan tietoturvan roolia myös muuna kuin teknisenä ja toimintaa estävänä toimintana, jolloin henkilöstö ja ylempi johto kykenee ymmärtämään tietoturvaa toiminnan mahdollistajana. Tämä kuitenkin vaatii liiketoiminnan huomioimisen tietoturvassa.

Tapauksiin perustuen liiketoimintastrategialla, riskiarviolla, tietoturvapolitiikalla, lainsäädännöllä ja operatiivisella toiminnalla on tärkeä rooli terveydenhuollon organisaatioiden tietoturvaprosesseissa. Tapaukset hyödynsivät erilaisia keinoja tietoturvansuunnittelussa ja kehittämisessä, ja toimintaa ohjattiin aktiivisesti erilaisilla tietoturvan ohjaus ja suunnitteluryhmillä. Varsinkin tietoturvapolitiikkaa hyödynnettiin strategisena dokumenttina, määrittäen tietoturvan tahtotilan ja ylemmän johdon sitoutumisen.

Tietoturvastrategia voi täydentää organisaation tietoturvapolitiikkaa määrittelemällä konkreettisemmat pitkän aikavälin tavoitteet, joita voidaan tarvita suuremman muutoksen aikaansaamiseksi. Tietoturvastrategia voi myös ohjata tietoturvapolitiikan kehitystä ja varmistaa liiketoiminnallisten tarpeiden huomioiminen tietoturvassa (Baskerville & Dhillon 2008). Strategia yleensä määrittää nykytilan, tavoitetilan ja menetelmät tavoitteeseen pääsemiseksi. Jotta strategian toimivuutta voidaan seurata, tarvitaan mittareita, jotta edistystä tietoturvaan liittyen kyetään seuraamaan. Lisäksi tietoturvastrategia voi auttaa määrittämään prioriteetit tietoturvassa liiketoiminnan kannalta. Tieturvastrategiaa voidaan hyödyntää tietoturvan kommunikoinnissa sekä omalle henkilökunnalle että yhteistyö kumppaneille. Etenkin terveydenhuolto alalla, jossa tietoturvaloukkauksilla voi olla vaikutuksia sekä organisaation että sen hoitamiin potilaisiin. Tästä johtuen tietoturva olisi kyettävä kehittämään osaksi organisaation joka päiväistä toimintaa.

Tapauksista kerätyn aineiston pohjalta esiteltiin tekijöitä, jotka organisaation olisi kyettävä huomioimaan tietoturvastrategiassa ja linjaamaan ne tietoturvan tavoitteisiin (Kuvio 3). Tietoturvastrategian tulisi perustua organisaation toimintaympäristöön, ottaen huomioon tekijöitä sekä organisaation sisältä ja sen toimintaympäristöstä. Tämän avulla tietoturvastrategialla voidaan muodostaa yhtenäinen, koko organisaation kattava ja tavoitteisiin pyrkivä tietoturvan ylläpito ja kehittäminen, joka voi auttaa sekä tietoturvapolitiikan määrittämisessä että tietoturvainvestointien valinnassa. Tietoturvan toteutus on usein tasapainoilua käytettävyyden ja tietoturvan välillä, jolloin tietoturvastrategia voi olla keino varmistaa henkilöstön huomioiminen tietoturvaprosesseissa ja kulttuurisen konfliktin välttämiseksi.

Organisaatioiden tietoturvan kehittyessä ja tietoturvateknologian parantuessa, myös hyökkääjät pyrkivät hyödyntämään yhä kehittyneempiä hyökkäysmenetelmä ja -strategioita omien tavoitteiden saavuttamiseksi, tämän vuoksi voi olla tarpeellista, että organisaatiot miettivät tietoturvaa enemmin strategisena kuin vain teknisenä ongelmana (Posthumus & von Solms 2004). Tässä uudessa lähestymistavassa tietoturvastrategia voi auttaa organisaatioita siirtymään proaktiivisempaan tietoturvan toteutukseen. Tietoturvastrategia tarvitsee kuitenkin lisää tutkimusta, jotta sen tarpeellisuutta ja käytännön hyödyt kyetään täysin ymmärtämään.

Tietoturvapolitiikka strategisena dokumenttina ei välttämättä riitä tietoturvan toteutuksessa, sillä jokainen päätös tietoturvainvestoinnista olisi hyödyllistä linjatta liiketoimintastrategiaan. Kirjattu tietoturvastrategia voi auttaa tässä päätöksenteko prosessissa valitsemaan tietoturvakontrollit suhteessa määritettyihin tavoitteisiin. Mahdollistaen samalla muutoksen seurannan, mikäli

siinä on määritetty mittareita muutoksen seurantaan. Huomioimalla liiketoiminnalliset tarpeet tietoturvassa voi se toimia osaltaan liiketoiminnan mahdollistajana, vähentäen organisaation arvonluontiprosessiin liittyviä riskejä.

7.1 Tutkimuksen rajoitteet

Kuten kaikkiin tutkimuksiin myös tämän tutkimuksen tuloksiin ja hyödynnettävyyteen liittyy rajoitteita. Sovellettaessa tämän tutkimuksen tuloksia käytäntöön tulee huomioida, muun muassa tapaustutkimuksesta ja aineistonkeräysmenetelmästä johtuvat rajoitteet. Tutkimukseen kysyttyjen organisaatioiden alustavasta kiinnostuksesta huolimatta, lopullinen osallistumisprosentti jäi suhteellisen pieneksi (25% kaikista tutkimukseen kysytyistä organisaatiosta). Tutkimukseen ei osallistunut yhtään yksityisen puolen organisaatiota. Nämä voivat rajoittaa tutkimuksen tulosten yleistettävyyttä yksityisen puolen terveydenhuollon organisaatioihin. Lisäksi tuloksiin voi liittyä maantieteellisiä rajoitteita. On kuitenkin huomattava, että vaikka tutkimuksessa onnistuttiin hyödyntämään vain kolmea tapausta, näiden organisaatioiden tulokset olivat samankaltaisia. Tämä puolestaan lisää tutkimuksen tulosten soveltuvuutta samankokoisten julkisensektorin terveydenhuollon organisaatioihin.

Myös haastattelujen hyödyntäminen ensisijaisena aineistonkeräysmenetelmänä voi vaikuttaa tulosten sovellettavuuteen. Haastattelut aineistonkeräysmenetelmänä tyypillisesti kerää haastateltavan näkemyksiä aiheeseen liittyen, jotka voivat vaihdella haastateltavasta ja haastattelun ajankohdasta riippuen.

Lisäksi tulkitessa tutkimuksen tuloksia tulee ottaa huomioon, että tutkimuksessa ei ensisijaisesti selvitetty tietoturvastrategiasta saatavia hyötyjä, vaan tutkimuksessa keskityttiin selvittämään näiden strategioiden ominaisuuksia terveydenhuollon organisaatioissa, joka voi rajoittaa tulosten hyödynnettävyyttä muiden alojen organisaatioissa. Myös kirjallisten tietoturvastrategioiden puute tapausorganisaatioissa saattoi vaikuttaa tutkimuksen tuloksiin ja niiden hyödynnettävyyteen. Tutkimuksessa esitetty viitekehys ei välttämättä esitä kaikkia tarpeellisia tietoturvastrategiassa huomioitavia tekijöitä, johtuen esimerkiksi kirjallisuuskatsauksen aineistohaun tuloksesta, joka voi vaihdella hakutermeistä riippuen.

7.2 Tulosten hyödyntäminen ja jatkotutkimus

Tutkimuksella voidaan nähdä olla sekä käytännöllisiä että teoreettisia hyötyjä. Tutkimuksen tuloksia voidaan hyödyntää terveydenhuollon organisaatioissa kehittäessä ja arvioitaessa tietoturvastrategioita organisaation käyttöön. Tutkimuksessa esitettiin teoreettinen viitekehys, joka osoitti huomioitavia tekijöitä toimivalle tietoturvastrategialle. Tämä viitekehys voi auttaa myös muiden alojen toi-

mijoita arvioimaan tietoturvastrategiaa oman organisaation käyttöön, pyrittäessä varmistamaan muun muassa liiketoiminnalliset tarpeet ja organisaation kulttuuri organisaation tietoturvassa.

Tieteellinen tutkimus voi hyödyntää tämän tutkimukset tuloksia pyrkiessään ymmärtämään tietoturvastrategian terveydenhuoltolan kontekstissa. Tutkimuksen teoreettista viitekehystä voidaan käyttää hyödyksi tulevaisuuden tutkimuksessa pyrittäessä paremmin ymmärtämään tietoturvastrategioita ja esimerkiksi niiden käytännön hyötyjä suhteessa tietoturvapolitiikkaan.

Jatkotutkimukselle on nähtävissä kolme selkeää tutkimussuuntaa. Ensimmäinen tutkimussuunta voi pyrkiä tutkimaan viitekehyksen toimivuutta toisella sektorilla, kuten esimerkiksi pankkialalla, joka on terveydenhuoltoalan tavoin tarkkaan säädelty ala. Tarkkasäätely voi vaikuttaa toteutettuun tietoturvastrategiaan ja voi näin valaista näiden alojen eroja.

Toinen tutkimussuunta voisi pyrkiä testaamaan tämän tutkimuksen tuloksia keskittymällä yksittäiseen tapaukseen ja osallistumalla syvällisesti tietoturvastrategian kehitykseen mallin avulla. Keskittyminen yksittäiseen tapaukseen voi mahdollistaa syvällisemmän ymmärryksen organisaation liiketoiminta- ja tietoturvaprosesseista.

Kolmas tutkimussuunta voisi tarkastella tarkemmin terveydenhuolto-organisaatioiden hyödyntämiä strategioita varmistaa potilaiden tietosuoja erilaisten tietoturvamenetelmien avulla. Kuten tässä tutkimuksessa nousi esille, tietosuoja terveydenhuollon organisaatioissa voi olla hyvin pitkälle kehittynyttä, mutta tietoturvan merkitystä tässä prosessissa ei aina täysin ymmärretä. Varsinkin erilaisten pilvipalveluiden yleistyessä, myös potilaisiin liittyvää terveystietoa voi päätyä ulkopuolisten saataville, varsinkin mikäli tähän teknologiaan liittyvä tietoturva ei ole kunnossa. Tämä tutkimus voisi tuoda esille uusia menetelmiä, joiden avulla terveydenhuollon organisaatiot kykenisivät vahvistamaan potilaiden tietosuojaa tietoturvakontrollien avulla.

LÄHTEET

Ahmad, A., Maynard, S.B. & Park, S. (2014). Information security strategies: towards an organizational multi-strategy perspective. *Journal of intelligent manufacturing*, 25(2), 357-370.

Allianz (2017). Allianz Risk Barometer: Top business risks 2017. Lainattu 16.10.2016, saatavilla: http://www.agcs.allianz.com/insights/white-papers-and-case-studies/allianz-risk-barometer-2017/

Anderson, E.E. & Choobineh, J. (2008). Enterprise information security strategies. *Computers & security*, 27(1-2), 22-29.

Appari, A. & Johnson, M. (2010). Information security and privacy in healthcare: Current state of research. *International Journal of Internet and Enterprise Management*, 6(4), 279-314.

Badr, Y., Biennier, F.& Tata, S. (2011). The Integration of Corporate Security Strategies in Collaborative Business Processes. *IEEE transactions on services computing*, 4(3), 243-254.

Bai, X., Gopal, R., Nunez, M., Zhdanov, D. (2014) A decision methodology for managing operational efficiency and information disclosure risk in healthcare processes. *Decision support systems*, 57, 406-416.

Barton, K.A., Tejay, G., Lane, M. & Terrell, S. (2016) Information system security commitment: A study of external influences on senior management. *Computers & Security*, 59, 9-25.

Baskerville, R., Spagnoletti, P. & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information & management*, 51(1), 138-151.

Beebe, N. L., & Rao, V. S. (2010). Improving organizational information security strategy via meso-level application of situational crime prevention to the risk management process. Communications of the Association for Information Systems, 26(1), 17.

Benbasat, I., Goldstein D. & Mead M. (1987). The Case Research Strategy in Studies of Information Systems. *MIS Quarterly*, 11(3), 369-386.

Carcary, M., Renaud, K., McLaughlin, S., & O'Brien, C. (2016). A Framework for Information Security Governance and Management. IT Professional, 18(2), 22-30.

Collmann, J. & Cooper, T. (2007). Breaching the security of the Kaiser Permanente Internet patient portal: the organizational foundations of information security. *Journal of the american medical informatics association*, 14(2), 239-243.

Damenu, T. K., & Beaumont, C. (2017). Analysing information security in a bank using soft systems methodology. Information & Computer Security, 25(3), 240-258.

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

Doherty, N. F., & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. Computers & Security, 25(1), 55-63.

Eisenhardt, K. (1989) Building Theories from Case Study Research. *The Academy of Management Review*, 14(4), 532-550.

Eisenhart, K. & Graebner, M. (2007). Theory Building from Cases: Opportunities and Challenges. *Academy of Management Journal*, 50(1), 25–32.

Eisenhart, K. & Graebner, M. (2007). Theory Building from Cases: Oppor- tunities and Challenges. *Academy of Management Journal*, 50(1), 25–32.

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) (2011) Euroopan unionin virallinen lehti. L 119/1.

Fernandez-Aleman, J.L., Sanchez-Henarejos, A., Toval, A., Sanchez-Garcia, A.B., Hernandez-Hernandez, I. & Fernandez-Luque, L. (2015). Analysis of health professional security behaviors in a real clinical setting: An empirical study. *International journal of medical informatics*, 84(6), 454-467.

Flores, W. R., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security,* 43, 90-110.

Furnell, S. & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & security*, 31(8), 983-988.

Gaunt, N. (2000). Practical approaches to creating a security culture. *International journal of medical informatics*, 60(2), 151-157.

Ghaeb, J.A., Smadi, M.A. & Chebil, J. (2011). A high performance data integrity assurance based on the determinant technique. *Future generation computer systems-the international journal of escience*, 27(5), 614-619.

Hall, J. H. (2011). Impacts of organizational capabilities in information security. *Information Management & Computer Security*, 19(3), pp. 155-176.

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

Herath, T., Herath, H., & Bremser, W. G. (2010). Balanced scorecard implementation of security strategies: a framework for IT security performance management. *Information Systems Management*, 27(1), 72-81.

Horne, C. A., Ahmad, A., & Maynard, S. B. (2016). Information Security Strategy in Organisations: Review, Discussion and Future Research Directions. arXiv preprint arXiv:1606.03528.

Huang, C.D., Behara, R.S. & Goo, J. (2014). Optimal information security investment in a Healthcare Information Exchange: An economic analysis. *Decision support systems*, 61, 1-11.

Karanja, E. (2017). The role of the chief information security officer in the management of IT security. *Information and computer security*, 25(3), 300-329.

Kayworth, T. & Whitten, D. (2010). Effective information security requires a balance of social and technology factors. *MIS Quarterly Executive*, 9(3), 163-175.

Kennedy, S.E. (2016). The pathway to security - mitigating user negligence. *Information and computer security*, 24(3), 255-264.

Kwon, J. & Johnson, M.E. (2013). Health-Care Security Strategies for Data Protection and Regulatory Compliance. *Journal of management information systems*, 30(2), 41-65.

Kwon, J. & Johnson, M.E. (2014). Proactive versus reactive security investments in the healthcare sector. *MIS Quarterly*, 38(2), 451-+.

Mansfield-Devine, S. (2017). Leaks and ransoms – the key threats to healthcare organisations. *Network Security*, 2017(6), 14-19.

Martin, G. (2017). Cybersecurity and healthcare: How safe are we? *BMJ*, 358.

McFadzean, E., Ezingeard, J-N. & Birchall, D. (2007). Perception of risk and the strategic impact of existing IT on information security strategy at board level. *Online information review*, 31(5), 622-660.

Mithas, S. (2016). How information technology strategy and investments influence firm performance conjecture and empirical evidence. *MIS Quarterly*, 40(1), pp. 223-245.

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

Neghina, D. & Scarlat, E. (2013). Managing Information Technology Security in the Context of Cyber Crime Trends. *International journal of computers communications & control*, 8(1), 97-104.

Oshri, I., Kotlarsky, J., & Hirsch, C. (2007). An information security strategy for networkable devices. IEEE Security & Privacy, 5(5).

Park, E.H., Kim, J. & Park, Y.S. (2017). The role of information security learning and individual factors in disclosing patients' health information. *Computers & Security*, 65, 64-76.

Park, S. & Ruighaver, T. (2008). Strategic Approach to Information Security in Organizations. *Information Science and Security, 2008. ICISS. International Conference on,* 26-31.

Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. Computers & Security, 23(8), 638-646.

Raggad, B. G. (2010). Information security management: Concepts and practice. Boca Raton, Florida ; London, [England] ; New York: CRC Press.

Romanou, A. (2017). The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise. *Computer Law & Security Review: The International Journal of Technology Law and Practice*.

Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. Computers & Security, 26(1), 56-62.

Siponen, M., Mahmood, M.A. & Pahnila, S. (2014) Employees' adherence to information security policies: An exploratory field study. *Information & Management*, 51, 217–224.

Sonnenreich, W., Albanese, J. & Stout, B. (2006). Return on security investment (ROSI) - A practical quantitative model. *Journal of research and practice in information technology*, 38(1), 45-56.

Stahl, B.C., Doherty, N.F. & Shaw, M. (2012). Information security policies in the UK healthcare sector: a critical evaluation. *Information systems journal*, 22(1), 77-94.

Sveen, F.O., Torres, J.M., Sarriegi, J.M. (2009). Blind information security strategy. *International journal of critical infrastructure protection*, 2(3), 95-109.

Taylor, R. (2014). The Roles Of Positive And Negative Exemplars In Information Security Strategy. *Academy of Information and Management Sciences Journal*, 17(2), pp. 57-79.

Taylor, R.G. (2015). Potential Problems with Information Security Risk Assessments. *Information security journal*, 24(4-6), 177-184.

Tutton, J. (2010). Incident response and compliance: A case study of the recent attacks. *Information Security Technical Report*, 15(4), pp. 145-149.

van Deursen, N., Buchanan, W.J. & Duff, A. (2013) Monitoring information security risks within health care. *Computers & security*, 37, 31-45.

Veiga, A. D., & Eloff, J. H. (2007). An information security governance framework. Information Systems Management, 24(4), 361-372.

Webb, J., Ahmad, A., Maynard, S.B. & Shanks, G. (2014). A situation awareness model for information security risk management. *Computers & security*, 44, 1-15.

Williams, S. P., Hardy, C. A., & Holgate, J. A. (2013). Information security governance practices in critical infrastructure organizations: A socio-technical and institutional logic perspective. Electronic Markets, 23(4), 341-354.

Yoon, Y.B., Oh, J., Lee, B.G. (2013). The Establishment of Security Strategies for Introducing Cloud Computing. *Ksii transactions on internet and information systems*, 7(4), 860-877.

Young, R. (2010a). Empirical Evaluation of Information Security Planning and Integration. *Communications of the Association for Information Systems*, 26, 40.

Young, R. (2010b). Evaluating the Perceived Impact of Collaborative Exchange and Formalization on Information Security. *Journal of International Technology and Information Management*, 19(3), 19-37.

Zerlang, J. (2017). GDPR: A milestone in convergence for cyber-security and compliance. *Network Security*, 6, 8-11.

LIITE 1 TEEMAHAASTATTELUN RUNKO

Haastateltavan tausta

- Nimi
- Rooli ja tehtävät organisaatiossa

Tietoturva

- Voitteko kuvailla tietoturvan merkitystä organisaatiossanne?
- Tietoturvan näkökulmasta, mitkä näette olevan suurimpia uhkia/riskejä/haasteita terveydenhuollolle - nyt tai tulevaisuudessa?
- Onko organisaatiollanne tietoturvastrategia tai muu strateginen suunnitelma tietoturvan toteuttamiseksi?

Tietoturvastrategia

- Kuinka omin sanoin määrittelette tietoturvastrategian?
- Mitä tietoturvastrategia merkitsee teille ja organisaatiollenne?
- Voitteko kuvailla tietoturvan strategista kehitysprosessia ja ketkä osallistuvat tähän prosessiin?
- Hyödyntääkö organisaationne viitekehyksiä/ohjeistuksia tietoturvan strategisessa suunnittelussa? Mitä?
- Kuinka mahdolliset prioriteetit tietoturvalle asetetaan strategian suunnittelussa? - Voitteko kuvailla tietoturvastrategian keskeisen sisällön?
- Seurataanko/arvioidaanko organisaatiossanne tietoturvan toimivuutta? Miten?
- Mikä ovat mielestänne edellytykset onnistuneelle tietoturvastrategialle?

Haastateltavan kommentit

- Muuta lisättävää tietoturvaan tai tietoturvastrategioihin liittyen?