jamk.fi

Strategian merkitys tietoturvan johtamisessa

Henri Heinonen

Opinnäytetyö
Toukokuu 2020
Tekniikan ja liikenteen ala
Teknologiaosaamisen johtaminen, Insinööri ylempi AMK

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Heinonen, Henri	Opinnäytetyö, YAMK	05 / 2020
	Sivumäärä 113	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi

Strategian merkitys tietoturvan johtamisessa

Tutkinto-ohjelma

Teknologiaosaamisen johtaminen, Insinööri ylempi AMK

Työn ohjaaja(t)

1. Jari Hautamäki, 2. Päivi Korpivaara

Toimeksiantaja(t)

Aktia Pankki Oyj

Tiivistelmä

Tutkimuksen tavoitteena oli selvittää strategian merkitystä tietoturvan johtamisessa suomalaisessa yritysmaailmassa. Taustana oli tutkimuksen tekijän oma mielenkiinto kyberturvallisuutta kohtaan sekä tarve muodostaa kokonaiskuva tilanteesta tukemaan omien työtehtävien kehittämistä.

Tutkimuksen toteuttamistavaksi valittiin teemahaastattelu. Teemahaastattelu valikoitui toteutustavaksi, koska laadullisella tutkimusmetodilla on mahdollista saavuttaa ennakko-oletuksiin sitoutumatonta tietoa. Teemahaastatteluista saadun laadullisen aineiston pohjalta on mahdollista tehdä jatkopäätelmiä, joiden perusteella voidaan tehdä monipuolisia ja kehittämiseen tähtääviä johtopäätöksiä. Teemahaastattelujen teemat pohjautuivat tutkimuksen aikana kerättyyn teoreettiseen viitekehykseen ja niiden pohjalta pyrittiin selvittämään sekä tietoturvallisuuden strategisen johtamisen ilmentymiä että organisaatioille merkityksellisen strategian osatekijöitä.

Tutkimuksen tulokset osoittivat, että strategian merkitys tietoturvan johtamisessa vaihtelee organisaatioittain. Tuloksista voitiin päätellä, että useimmissa organisaatioissa kuitenkin huomioitiin teoreettisesta viitekehyksestä löytyviä tietoturvallisuuden strategisen johtamisen teemoja ainakin jollakin tasolla. Ei kuitenkaan aina tavoitteellisesti tai tiedostaen.

Yritysten tulisi kiinnittää enemmän huomiota tietoturvallisuuden strategiseen johtamiseen eri viitekehysten antamien suositusten mukaisesti. Yritysten tietoturvan taso liittyy vahvasti myös kansalliseen kyberturvallisuuteen, jolloin organisaatioiden kyky tunnistaa muutoksia sisäisessä ja ulkoisessa toimintaympäristössä sekä kyky reagoida näihin muutoksiin vaikuttaa myös kansallisen kyberturvallisuuden tasoon.

Avainsanat (asiasanat)

kyberturvallisuus, tietoturva, strategia, strategiatyö, strateginen johtaminen

Muut tiedot (Salassa pidettävät liitteet)

jamk.fi

Description

Author(s)	Type of publication	Date
Heinonen, Henri	Bachelor's thesis	05 / 2020
		Language of publication: Finnish
	Number of pages 113	Permission for web publication: x

Title of publication
The role of strategy in information security management

Degree programme
Master's Degree Programme in Technological Competence Management

Supervisor(s)
1. Jari Hautamäki, 2. Päivi Korpivaara

Assigned by
Aktia Pankki Oyj

Abstract

The aim of the study was to discover the importance of strategy in managing cyber security in Finnish corporations. The background was the writer's own interest towards cyber security and the need to comprehend the current over-all picture of the topic to enable personal work development.

Theme interview was chosen as the method of study. Theme interview was chosen because with a qualitative study method it is possible to reach data that is not bound to the pre-assumptions. The qualitative data gathered with the theme interviews enables further analysis that will lead to diverse and development oriented conclusions. The theme interviews were based on theoretical frame work during the study. The aim of the theme interviews was to discover both outlook of cyber security managing and the importance of strategy for the organisation.

The study results indicated that the importance of strategy in managing cyber security differs in organisations. It was possible to conclude from the results that in the most of the organisations some aspects of the theoretical frame work were included at some extent in cyber security strategic managing. Though, not necessarily with spesific aims or with previous comprehension.

Corporations should underline the strategic cyber security managing as it has been recommended in the theoretical frame work. The cyber security level of corporations is closely related to the national cyber security. Therefore, the ability to detect and foresee changes the inner and outer operational environment and the ability to react accordingly to these changes have an impact in the national cyber security as well.

Keywords/tags
cyber security, information security, strategy, strategy work, strategic leadership

Miscellaneous (Confidential information)

Sisältö

Kuviot

Taulukot

1 Johdatus tietoturvallisuuden strategiseen johtamiseen

Tietoturvallisuutta voidaan johtaa monella tasolla aivan kuten muitakin johdettavissa olevia asioita. Tietoturvallisuuden strateginen johtaminen pyrkii varmistamaan, että organisaation tavoitteet ohjaavat tietoturvatyötä ja että tietoturvallisuus pyrkii omalta osaltaan varmistamaan ja tukemaan organisaation keskeisten tavoitteiden saavuttamista. Tietoturvatyön liiketoimintalähtöisyydellä pyritään varmistamaan, että tietoturvaorganisaatio on osannut varautua yrityksen strategiakauden aikaisiin muutoksiin niin yrityksen sisäisessä kuin ulkoisessakin toimintaympäristössä.

1.1 Muuttuva toimintaympäristö luo haasteita tietoturvan johtamiselle ja strategiselle johtamiselle

Maailma muuttuu ympärillämme digitalisaation muovatessa ympäröivää yhteiskuntaa. Tämän tutkimusraportin kirjoittamisen aikaan niin Suomi kuin muukin maailma otti valtavan digitaalisen loikan muutamassa päivässä eikä tämän digitalisaatioaallon takana ollut yksikään CEO, CIO tai CTO vaan COVID-19. Koronavirus teki hetkessä sen mistä organisaatioissa ja yhteiskunnallisissa keskusteluissa oli puhuttu jo vuosia. Nopealla aikataululla työntekijät (niillä toimialoilla missä se vain oli mahdollista) siirtyivät etätöihin ja yritykset joutuivat keksimään lennossa sähköisiä palvelumalleja yhteiskunnan sulkeutuessa sosiaalisen eristäytymisen johdosta viruksen leviämisen hidastamiseksi.

Poikkeusolot saavat kyberrikolliset aktivoitumaan. Heidän tavoitteenaan on hyödyntää ihmisten epätietoisuutta, poikkeustilanteen aiheuttamaa stressiä ja pelkoa. Erilai-

set korona-aiheiset kalastelukampanjat, disinformaation levittäminen, rokotetutkimuksiin liittyvän tiedon saalistaminen ja terveydenhuolto-organisaatioiden hyökkäysten kohteeksi ottaminen alkoivat välittömästi pandemian levitessä maapallolla.

Liiketoiminnan strateginen johtaminen on varsin vakiintunutta toimintaa suuryrityksissä ja kehittyneissä keskisuurissa yrityksissä mutta se ei ole poistanut strategian merkityksen ymmärtämisen haasteita (Kamensky 2014, 14). Strategisessa johtamisessa tehdään tavoitteellisia suunnitelmia noin 3-5 vuoden aikajänteellä mutta ”valmista” strategiaa ei voi jättää pölyyntymään pöytälaatikkoon vaan sitä olisi katselmoitava ja päivitettävä säännöllisesti toimintaympäristössä tapahtuvien muutosten huomioimiseksi. Keväällä 2020 tapahtuneet koronaviruksen aiheuttamat nopeat yhteiskunnalliset muutokset ympäri maapallon olivat selkeä merkki yritysten strategisten suunnitelmien tarkastustarpeesta, mutta aina signaalit eivät ole yhtä vahvoja. Parhaiten menestyvät ne organisaatiot, jotka tunnistavat syntyneet muutostarpeet ja pystyvät reagoimaan muutoksiin nopeimmin, sillä muutoksessa on aina paikka myös uusille liiketoimintamahdollisuuksille.

1.2 Aiheen valinta ja rajaukset

Tämän tutkimuksen aiheen valinta tuli ajankohtaiseksi alkuvuodesta 2019 hieman sen jälkeen, kun olin aloittanut uusissa tehtävissä työnantajallani Aktia Pankilla. Tarvitsin siinä kohtaa työtehtävieni pohjaksi jotain, jonka avulla voisin viedä Aktian tietoturvallisuustyötä kokonaisvaltaisesti nopein ja määrätietoisin askelin eteenpäin. Tarvittavan visionäärisen ja Aktian liiketoimintastrategiaa tukevan näkökulman löytämiseksi katse oli kiinnitettävä operatiivisen ja taktisen johtamisen sijaan strategiseen lähestymistapaan. Operatiivisen johtamisen keskittyessä lyhyen aikavälin tavoitteisiin

(Vuorinen 2013, 15) oli selvää, että tietoturvallisuustyön osalta tavoitteet ja niiden saavuttamisen aikataulu oli asetettava yrityksen liiketoimintastrategian mukaisiksi.

Koin tämän aihealueen mielekkääksi, sillä siinä yhdistyivät kaksi mielenkiintoni kohdetta eli tietoturvallisuus ja johtaminen. Korkean teknologian maana Suomella on erinomaiset mahdollisuudet tulla maailman johtavaksi kyberturvallisuusmaaksi. Kansallinen kyberturvallisuus ja sen kehittäminen on kaikkien yhteiskunnan toimijoiden yhteinen ponnistus ja siinä on oma roolinsa niin valtionhallinnolla, puolustusvoimilla kuin yrityksilläkin. Suomalaisessa yhteiskunnassa suurin osa kriittisestä infrastruktuurista on kaupallisesti tuotetussa yksityisomistuksessa. (Sillanpää, Roivainen & Lehto 2015, 134.)

Tätä taustaa vasten on tärkeää ymmärtää, miten suomalainen yrityskenttä huolehtii omalta osaltaan kyberturvallisuuden toteutumisesta. Tämä ei kosketa pelkästään kriittisen infrastruktuurin toimijoita, vaan jokaisen organisaation tulisi omalta osaltaan varautua uusiin kyberuhkiin ja kyetä tunnistamaan oma roolinsa yhteiskunnallisessa kentässä. Tietoturvallisuuden strateginen johtaminen ei tietenkään yksinään edistä tai huononna yritysten kyvykkyyttä toimia kybermaailmassa mutta se pakottaa organisaatiot tekemään pidemmän aikavälin suunnittelua, analysoimaan niiden omaa toimintaa sekä sitä toimintaympäristöä missä ne toimivat. Näiden analyysien kautta yritykset voivat tunnistaa uusia uhkia, joilla voi olla myös yhteiskunnallista vaikutusta.

Tämän opinnäytetyön lähtökohtana oli tutkia tietoturvallisuuden strategisen johtamisen ilmentymistä Suomessa ja kartuttaa samalla tutkimuksen tekijän tietämystä aiheesta sekä pyrkiä tunnistamaan mahdollisia jatkotutkimuskohteita kansallisen tai

toimialakohtaisen kyberturvallisuusresilienssin parantamiseksi. Tutkimusta edeltäneen valmisteluvaiheen tiedonhankkimisprosessin aikana kävi ilmi, ettei tietoturvallisuuden strategisesta johtamisesta ollut juurikaan tehty aiempaa tutkimusta. Tutkimuksessa ei haluttu lähteä selvittämään tietoturvallisuuden hallintajärjestelmien ja riskienhallinnan viitekehysten merkitystä tietoturvallisuuden johtamisessa, sillä niistä on olemassa olevaa tutkimusta saatavilla runsaasti. Tutkimuksen tarkoituksena oli selvittää teoreettisesta viitekehyksestä löytyvän tietoturvallisuuden strategisen johtamisen ilmentymiä ja käytännön toteutuksia yritysmaailmassa. Tutkimuksen tekeminen ei kohdistunut suoraan toimeksiantajaorganisaatioon vaan se toteutettiin tutkimalla yrityksiä eri toimialoilta. Toimeksi antaneen organisaation osalta tutkimuksesta saavutettu hyöty on tullut tutkijan omien tietojen ja taitojen karttumisesta, joka on välillisesti hyödyttänyt myös tutkijan edustamaa organisaatiota.

1.3 Tutkimustehtävä ja tavoitteet

Tutkimusstrategian valinnassa päädyttiin toteuttamaan tutkimus laadullisen tutkimusotteen avulla, jossa tiedonkeruu toteutettiin teemahaastatteluina. Laadullinen tutkimusote valittiin, koska tutkimuksessa pyrittiin ymmärtämään tutkimuksen kohteena olevaa ilmiötä. Tutkijan rooli tutkimuksessa oli tarkkailla ja tehdä havaintoja eri organisaatioiden nykykäytännöistä, hyvistä toimintatavoista ja mahdollisista puutteista sekä pyrkiä tunnistamaan strategisen johtamisen ilmentymät kerätyn aineiston pohjalta olemassa olevaan teoreettiseen viitekehykseen pohjautuen. Tutkija ei puuttunut kohdeorganisaatioiden toimintaan tutkimuksen aikana. Tutkimuksen tavoitteena oli tutkia tietoturvallisuuden strategista johtamista ilmiönä suomalaisissa suuryrityksissä ja samalla saada selville johdetaanko tietoturvallisuutta strategisen johtamisen teorioiden mukaisesti vai onko tietoturvallisuuden johtaminen pikemminkin

taktisen tai operatiivisen tason johtamista. Lisäksi tutkimuksen avulla haluttiin selvittää, millä tavoin organisaatioiden liiketoimintastrategiat ja niissä määritellyt tavoitteet linjataan tietoturvallisuuden strategioihin tai kehitysohjelmiin sekä tavoitteisiin vai onko organisaatioissa vain yksi strategia (liiketoimintastrategia) ja kuinka tietoturvallisuuden tavoitteet mahdollisesti ilmenevät niissä.

1.4 Tutkimuskysymykset

Edeltävässä kappaleessa 1.3 esitellyt asiat muodostavat yhdessä tutkimuksen tutkimusongelman, joka on strategian merkitys tietoturvallisuuden johtamisessa. Tutkimusongelman pohjalta tutkimuskysymyksiksi valikoituivat seuraavat kysymykset:

1. Johdetaanko tietoturvallisuutta suomalaisissa suuryrityksissä strategisesti?
2. Miten merkityksellinen tietoturvastrategia rakennetaan?
3. Mistä tekijöistä merkityksellinen tietoturvastrategia koostuu?

1.5 Raportin rakenne ja kappalekohtaiset kuvaukset

Tämän tutkimuksen johdannossa määritellään aihevalinta, tutkimusongelma, tutkimuksen tavoitteet ja rajaukset sekä tutkimuskysymykset. Tutkimuksen toisessa luvussa käsitellään laadullisen tutkimusmenetelmän rakennetta ja tutkimusaineiston keräämisessä huomioon otettavia seikkoja. Tutkimuksen kolmas luku keskittyy teoreettisen viitekehyksen rakenteeseen ja tutkimuksen aiheeseen liittyvään olemassa olevaan tutkimukseen. Neljännessä luvussa kuvataan tietoturvallisuuteen keskeisesti liittyvät teoriat ja viitekehykset. Kappaleessa viisi käydään vastaavasti läpi strategiseen johtamiseen liittyvää teoriaa. Kappale kuusi sisältää teoreettisen viitekehyksen tietoturvallisuuden strategiselle johtamiselle. Tutkimuksen seitsemännessä luvussa

kuvataan tutkimuksen toteutus ja aineiston kerääminen sekä esitellään aineiston analysointi. Kahdeksannessa luvussa esitellään tutkimuksen tulokset ja tehdään luotettavuuden arviointi. Viimeisenä olevassa kappaleessa yhdeksän vedetään yhteen tutkimukset johtopäätökset ja tuodaan esiin pohdinnan kautta kehitysehdotuksia sekä jatkotutkimuksen kohteita.

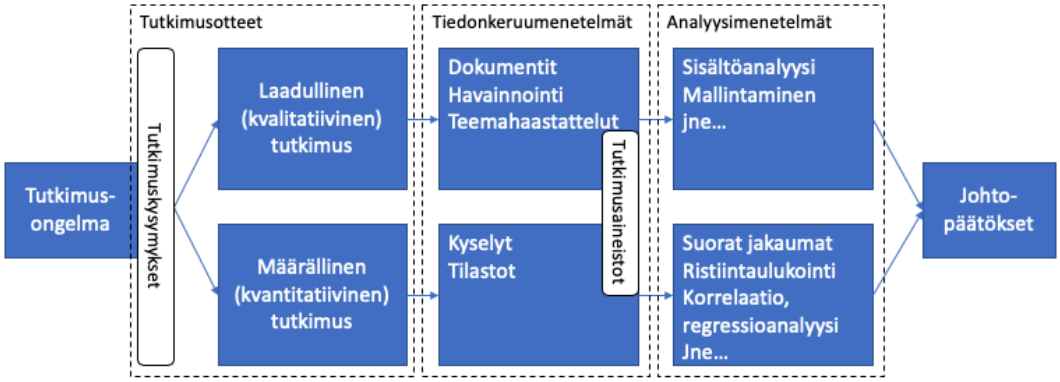
Eri luvut on eroteltu toisistaan luettavuuden ja raportin selkeyden varmistamiseksi. Jokaisen luvun lopussa on yhteenveto luvussa esitetyistä keskeisistä tutkimuksen tekemiseen tai luotettavuuden arviointiin vaikuttavista asioista.

2 Tutkimusaineisto ja käytetyt tutkimusmenetelmät

2.1 Tutkimusmenetelmä

Tutkimuksissa kohteena oleva tutkimusongelma pyritään ratkaisemaan tutkimusmenetelmien avulla. Tutkimusotteet jakautuvat siten, että niiden ääripäissä ovat laadullinen (kvalitatiivinen) tutkimus ja määrällinen (kvantitatiivinen) tutkimus sekä näiden välille sijoittuvat erilaiset tutkimusstrategiat kuten case-, kehittämis- ja toimintatutkimus, joita ei pidetä varsinaisina erillisinä menetelmäkokonaisuuksina. Tutkimusote on laaja ongelmanratkaisun lähestymistapa, johon sisältyy kullekin otteelle ominaiset tiedonkeruun, analysoinnin ja tulkinnan menetelmät. Menetelmät ovat yhteydessä toisiinsa ja tutkimusprosessin alkupää määrittelee tutkimuksen edetessä käytettävissä olevat menetelmät ja työkalut. Tutkimuksen aikana tulee vastaan valintapisteitä, joissa tutkimuksen tekijän on tehtävä päätöksiä käytettävistä tutkimusmenetelmistä. (Kananen 2013, 22-23.)

Määrällinen ja laadullinen tutkimus ilmaistaan usein vastakkainasetteluna, jolloin saattaa muodostua käsitys siitä, että laadullinen tutkimus olisi yksi yhtenäinen kokonaisuus (Tuomi & Sarajärvi 2018, 4). Laadulliselle tutkimukselle löytyy ainakin 34 erilaista tunnusmerkkiä, joten erilaisia tapoja laadullisen tutkimuksen tekemiseen on useita (Tuomi & Sarajärvi 2018, 10).



Kuvio 1. Tutkimusongelman ratkaisu (Kananen 2014, 41).

Kanasen (2013) tekemän tutkimusotteiden vertailun mukaan laadullinen tutkimus lähtee liikkeelle käytännöstä (induktio) ja se pyrkii lisäämään ymmärrystä tutkittavasta ilmiöstä. Tutkimuksessa tutkija on ulkopuolinen osallistuja, joka pyrkii saamaan tutkimusongelmaan ratkaisua hyödyntämällä avoimia kysymyksiä tai teemahaastatteluja. Laadullisessa tutkimuksessa kysymyksiin saatavat vastaukset ovat pääosin kuvailevaa tekstiä. Kanasen mukaan laadullisen tutkimuksen avulla pyritään ymmärtämään ilmiötä, siihen liittyviä tekijöitä sekä näiden välisiä liityntäpintoja. (Kananen 2013, 24.) Syntyneen ymmärryksen lopputuloksena on teoria eli yleistys tutkitusta ilmiöstä. Selityksen tuottamista empiriasta eli käytännöstä kutsutaan induktioksi. (Mts. 26.)

Tuomi ja Sarajärvi (2018) nostavat esiin, että laadullinen analyysi voi olla induktiivista tai deduktiivista mutta lisäävät, että tämän kaltainen jaottelu on ongelmallista siksi, ettei puhtaan induktion mahdollisuutta ole nykytietämyksen mukaan olemassa. Induktiivisen ja deduktiivisen kahtiajaon suurin ongelma on käytännöllinen, sillä silloin jätetään huomioimatta abduktiivinen päättely eli teorianmuodostus silloin, kun havaintojen tekoon liittyy jokin olemassa oleva johtoajatus tai johtolanka. (Tuomi ja Sarajärvi 2018, 80.)

Laadullisessa tutkimuksessa tutkija ei saa vaikuttaa tutkittavaan ilmiöön eli ilmiö ja tutkija on pyrittävä pitämään erillään. Kanasen (2013, 24) mukaan tällä tavoin halutaan varmistaa luotettavan tiedon saaminen aidosta ilmiöstä sille ominaisessa ympäristössä. Laadullisessa tutkimuksessa tulee kuitenkin aina huomioida se mahdollisuus, että tutkija itse saattaa kuitenkin vaikuttaa lopputulokseen tietoisesti tai tiedostamattaan. Laadullisen ja määrällisen tutkimuksen ero on siinä, että ensin mainittu pyrkii ymmärtämään tutkittavaa ilmiötä ja jälkimmäinen tekemään yleistyksiä. Laadullisessa tutkimuksessa ilmiötä ei tunneta täysin tutkimuksen alussa, joten tarkkoja kysymyksiäkään ei voida esittää. Tällöin tutkija voi yrittää ottaa ilmiön haltuun tutkittavan kautta esimerkiksi keskusteluttamalla aiheeseen liittyvistä teemoista haastateltavia. Kyseistä menetelmää kutsutaan teemahaastatteluksi. Laadullisessa tutkimuksen kenttävaiheessa kertyvät aineistot ovat esimerkiksi tekstiä, sanoja, dokumentteja ja kuvia, kun taas määrällisessä tutkimuksessa aineistot ovat pääosin eri kysymysvaihtoehtojen saamia lukuja. (Mts. 26-27.)

Tämän opinnäytetyön tutkimuksen tavoitteena oli ymmärtää tieto- ja kyberturvallisuuden strategista johtamista ilmiönä. Tutkimusotteeksi valittiin laadullinen tutkimus, jossa teemahaastatteluiden avulla kerättiin tietoa tutkittavasta ilmiöstä. Kerätty

aineisto analysoitiin sisältöanalyysin avulla. Näiden tutkimusmenetelmien avulla pyrittiin luomaan ymmärrys ilmiöstä ja selittämään tieto- ja kyberturvallisuuden strategista johtamista Suomessa.

2.2 Aineiston keruu

2.2.1 Teemahaastattelu

Haastattelulla tarkoitetaan henkilökohtaisesti tehtävää haastattelua, jossa haastattelija esittää suullisia kysymyksiä sekä merkitsee tiedonantajan eli informantin vastaukset muistiin. Haastattelun etu on joustavuus, sillä kysymyksiä on mahdollista tarvittaessa toistaa, niihin liittyviä väärinkäsityksiä voidaan oikaista, ilmausten sanamuotoja voidaan selventää ja informantin kanssa voidaan käydä keskusteluja. Kysymykset myös voidaan esittää siinä järjestyksessä kuin haastattelija katsoo tarpeelliseksi. Tärkeintä haastattelussa on saada mahdollisimman paljon tietoa käsiteltävästä aiheesta. Yksi haastattelun eduista on, että haastatteluun voidaan valita ne henkilöt, joilla on kokemusta tutkittavasta ilmiöstä. (Tuomi & Sarajärvi 2018, 63.)

Kanasen (2014, 24) mukaan teemahaastattelussa tutkija keskusteluttaa tutkittavaa valitusta aiheesta ja antaa tämän kertoa siitä mahdollisimman laajasti. Teemahaastattelu on tilaisuus, jossa kaksi ihmistä keskustelee etukäteen valituista aiheista eli teemoista yksi kerrallaan. Teemat ovat yleisluontoisia keskustelun aiheita, jotka tutkittava on saanut tutkittavan ilmiön ennakkonäkemyksestä. (Mts. 70.)

Kuvio 2. Teemojen käyttö ilmiön tutkimisessa (Kananen 2014, 72).

Haastattelun teemojen avulla tutkija pyrkii saamaan ymmärryksen tutkittavasta ilmiöstä. Tutkija käyttää teemoja ja tarkentavia kysymyksiä saadakseen haastateltavalta ilmiöön liittyvää tietoa, joiden pohjalta nousee esiin uusia kysymyksiä. Haastattelujen pohjalta tutkija pyrkii analyysivaiheessa luomaan kokonaisvaltaisen kuvan tutkittavasta ilmiöstä. Haastattelussa esitettävien kysymyksien valintaa ohjaa ratkaistava tutkimusongelma. Teemahaastattelu eroaa strukturoidusta haastattelusta siinä, ettei itse ilmiötä vielä tunneta tarkasti. Strukturoidussa haastattelussa kysymysten lisäksi myös vastausvaihtoehdot ovat valmiina. Dikotomisien kysymysten (kyllä- ja ei-vastaukset) käyttöä tulee varoa, sillä niiden käyttö johtaa suppeaan aineistoon, jota ei voi hyödyntää analyysivaiheessa. (Mts. 72-74.)

Yhdenmukaisuuden vaatimuksen aste vaihtelee tutkimuksesta toiseen ja tutkijan tulee itse päättää esittääkö hän jokaisessa haastattelussa kaikki suunnitellut kysymykset, käykö hän kysymykset aina läpi samassa suunnitellussa järjestyksessä tai käyt-

tääkö hän aina samoja sanamuotoja. Toteutukset voivat siis vaihdella avoimen haastattelun tyyppisistä haastatteluista täysin strukturoidusti eteneviin haastatteluihin. (Tuomi & Sarajärvi 2018, 65.)

Teemahaastattelussa tutkittava saa vapaasti kertoa valitusta aiheesta ja tutkijan tehtävänä on pitää keskustelu valitun aihealueen piirissä sekä tehdä tarvittaessa tarkentavia kysymyksiä. Kerätty aineisto analysoidaan mahdollisimman nopeasti tutkijan ymmärryksen kasvattamiseksi, jolloin saadaan myös esille myös lisäkysymyksiä uusintakierroksia varten. Aloittelevalla tutkijalla haastattelukierrokset saattavat jäädä vain yhteen, mikä johtaa pinnalliseen tietoon tutkittavasta ilmiöstä. Teemahaastattelussa edetään niin, että kunkin teeman osalta lähdetään liikkeelle yleisestä tasosta ja keskustelun edetessä mennään kohti yksityiskohtaisia kysymyksiä. (Kananen 2014, 76-77.)

Teemahaastattelussa on tarkoitus löytää merkityksellisiä vastauksia tutkimuksen tavoitteiden, tutkimusongelman tai tutkimustehtävän mukaisesti. Etukäteen valitut teemat perustuvat tutkimuksen viitekehykseen eli siihen mitä tutkittavasta ilmiöstä jo tiedetään. Haastattelun avoimuudesta riippuu kuinka tiukasti teemoihin liittyvät kysymykset kumpuavat viitekehyksestä ja kuinka paljon sallitaan intuitiivisten ja kokemusperäisten kysymysten esittämistä. (Tuomi & Sarajärvi 2018, 66.)

2.3 Aineiston analyysi

Laadullisen aineiston analyysi ei ole tutkimusprosessin viimeinen vaihe vaan tutkimus on luonteeltaan syklistä ja aineiston analysointi aloitetaan aineiston keräämisen aikana (Seitamaa-Hakkarainen N.d.). Laadullinen tutkimus etenee iteratiivisesti siten,

että tiedon kerääminen ja analyysi vuorottelevat. Syklejä voi olla useita, sillä ennakolta ei voida tietää kuinka paljon tietoa tarvitaan. (Kananen 2014, 99.)

Laadullisen tutkimuksen perinteiden mukainen perusanalyysimenetelmä on sisällönanalyysi. Useimmat eri nimillä kulkevat laadullisen tutkimuksen analyysit perustuvat tavalla tai toisella sisällönanalyysiin. Laadullisen tutkimuksen analyysi voidaan jakaa karkeasti kahteen ryhmään. Toisen ryhmän analyysiä ohjaa tietty teoreettinen asemointi ja toiseen ryhmään kuuluvat ne analyysit, joita ei ohjaa jokin teoria, mutta joihin voidaan soveltaa suhteellisen vapaasti erilaisia teoreettisia lähtökohtia. Sisällön analyysi kuuluu näistä jälkimmäiseen ryhmään. (Tuomi & Sarajärvi 2018, 78.)

Kananen (2014, 99-100) listaa laadullisen tutkimuksen ratkaisun etsimisessä seuraavat vaiheet:

1. Tutkimusongelmaan liittyvän tiedon kerääminen erilaisilla menetelmillä.
2. Kerätyn aineiston yhteismitallistaminen eli litterointi tekstimuotoon.
3. Aineiston koodaaminen eli litteroidun aineiston tarkastelu tutkimusongelman ja -kysymysten avulla ja kokonaisuuksien sisällön kuvaaminen tiivistetysti koodeilla.
4. Aineiston luokittelu, jossa koodien perusteella tunnistetaan mitkä osat muodostavat oman ryhmänsä. Luokat nimetään.
5. Uusi tiedonkeruuvaihe, jossa täydennetään analyysiä tai etsitään vastauksia esiin nousseisiin uusiin kysymyksiin.

Tuomi ja Sarajärvi kuvaavat sisällönanalyysin etenemisen helppotajuisemmin tutkija Timo Laineen rungon pohjalta seuraavasti (Tuomi & Sarajärvi 2018, 78.):

1. Päätä, mikä aineistossa kiinnostaa ja pysy päätöksessä
2. Käy aineisto läpi
    a. Erota ja merkitse ne asiat, jotka sisältyvät kiinnostuksen kohteeseen
    b. Jätä kaikki muu tutkimuksesta pois
    c. Kerää merkityt asiat yhteen ja erilleen muusta aineistosta

3. Luokittele, teemoita tai tyypittele aineisto
4. Kirjoita yhteenveto

Aineistosta voi löytyä paljon kiinnostavia asioita, mutta kaikkea ei voi tutkia yhden tutkimuksen puitteissa. Aineistosta otetaan vain ne osat, jotka liittyvät tarkkaan rajattuun tutkittavaan ilmiöön. Tutkimuksen tavoitteet, tutkimustehtävä tai tutkimusongelma määräävät mistä tutkimuksessa ollaan kiinnostuneita ja sen tulee välittyä raportoidun kiinnostuksen kohteen kanssa. Edellä esitetyn listan kohta kaksi tarkoittaa aineiston litterointia ja koodaamista. Listan kohdalla kolme tarkoitetaan varsinaista analyysiä eikä se ole mahdollinen ilman listan kahden aiemman kohdan toteutumista. (Mts. 78-79.)

Aineistolähtöinen analyysi pyrkii luomaan tutkimusaineistosta teoreettisen kokonaisuuden. Analyysin perusajatus on, että analyysiyksiköitä ei ole etukäteen sovittu tai harkittu. Teorian merkitys analyysin ohjaajana rajoittuu tällöin vain metodologiaan eikä aikaisemmilla tutkittavaan ilmiöön liittyvillä havainnoilla, tiedoilla tai teorioilla ole mitään tekemistä analyysin toteuttamisen tai lopputuloksen kanssa. Teoria koskee vain analyysin toteuttamista. *Teoriaohjaavassa* analyysissä on teoreettisia kytkentöjä ja teoria voi toimia apuna mutta analyysi ei pohjaudu suoraan teoriaan. Analyysiyksiköt valitaan aineistosta, mutta olemassa oleva tieto auttaa ja ohjaa analyysia. Aikaisemman tiedon merkitys ei ole teoriaa testaava vaan uusia ajatuspolkuja avaava. Teoriaohjaavan analyysin päättelyn logiikka on abduktiivinen ja ajatteluprosessissa vaihtelevat aineistolähtöisyys ja valmiit mallit. Tutkija pyrkii yhdistelemään näitä pakolla, puolipakolla tai jopa luovasti samalla mahdollisesti uutta synnyttäen. *Teorialähtöinen* analyysi on perinteinen analyysimalli ja se perustuu johonkin tiettyyn teoriaan. Tutkimuksessa kuvaillaan tämä malli ja sen pohjalta tutkimuksen käsitteet. Tutkittava ilmiö siis määritellään jo jonkun tunnetun mukaisesti. Aineiston analyysiä

ohjaa olemassa oleva teoria, jota testataan tutkimuksessa uudessa kontekstissa. Teorialähtöisen analyysin päättelyn logiikka on deduktiivista. Edellä esitettyjen kolmen analyysimuodon erot liittyvät siihen, kuinka ilmiötä kuvaava teoria ohjaa aineiston hankintaa, analyysiä ja raportointia. Erot on kuvattu Kuviossa 3. (Mts. 81-83.)

	Viitekehys	Aineiston hankinta	Aineiston analyysi	Raportointi
Aineistolähtöinen analyysi	(a) metodologia (b) tutkittavasta ilmiöstä jo tiedetty	metodologia ohjaava vapaa	aineistolähtöinen	aineistolähtöinen
Teoriaohjaava analyysi	(a) metodologia (b) tutkittavasta ilmiöstä jo tiedetty	metodologia ohjaava vapaa	teoriaohjaava, kaksiosainen; aineistolähtöinen johon liitetään teoriaohjaava	teoriaohjaava
Teorialähtöinen analyysi	(a) metodologia (b) tutkittavasta ilmiöstä jo tiedetty	teorialähtöinen	teorialähtöinen	teorialähtöinen

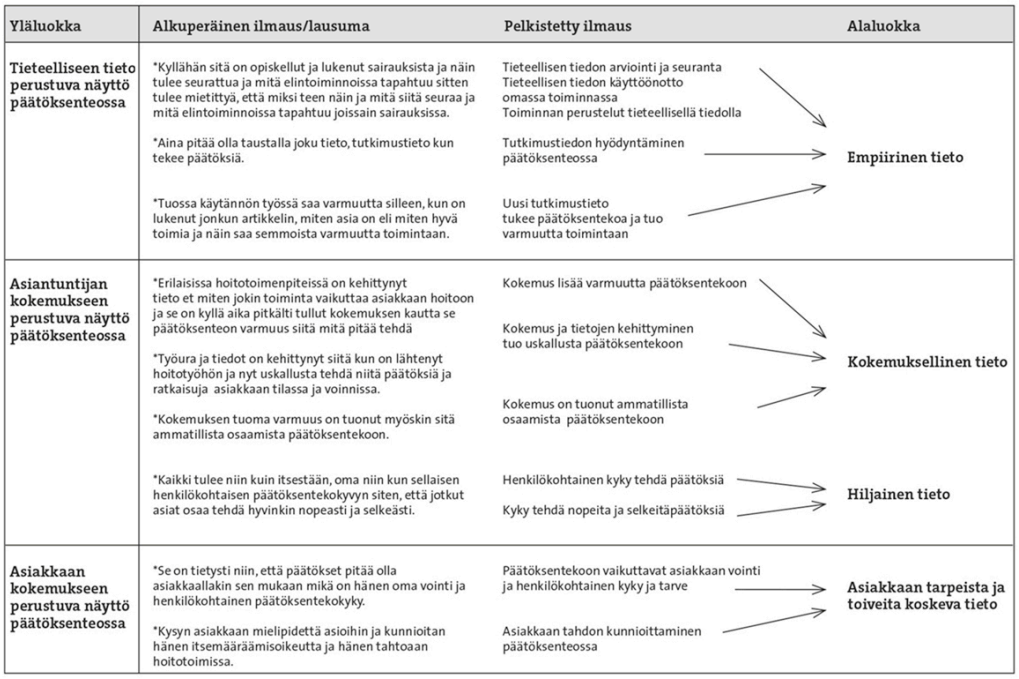
Kuvio 3. Laadullisen tutkimuksen analyysimuodot (Tuomi & Sarajärvi 2018, 83).

Tutkittavaa ilmiötä kuvaa tutkimuksessa kerätty aineisto ja analyysin tarkoituksena on luoda selkeä sanallinen kuvaus siitä. Sisällönanalyysilla muodostetaan tiivis ja selkeä esitys aineistosta kadottamatta sen sisältämää tietoa. Selkeytetyn aineiston avulla pyritään vastaavasti tekemään selkeitä ja luotettavia johtopäätöksiä tutkittavasta ilmiöstä. Käsittely perustuu loogiseen päättelyyn ja tulkintaan, jossa aineiston ensin hajotetaan osatekijöihinsä, käsitteellistetään ja kootaan uudestaan uudella tavalla loogiseksi kokonaisuudeksi. (Mts. 90.)

Kuvio 4. Aineistolähtöisen sisällönanalyysin eteneminen (Tuomi & Sarajärvi 2018, 91).

Teorialähtöisessä sisällönanalyysissä aineiston luokittelu perustuu olemassa olevaan käsitteistöön, joka voi olla teoria, malli, käsitejärjestelmä tms. Sisällönanalyysin ensimmäinen vaihe on analyysirungon muodostaminen. Rungon sisälle muodostetaan aineistosta erilaisia luokituksia tai kategorioita aineistolähtöisen sisällönanalyysin periaatteita noudattaen. Aineistosta poimitaan ne asiat, jotka kuuluvat analyysirunkoon ja lopuista muodostetaan tarvittaessa uusia luokkia samoja aineistolähtöisen analyysin periaatteita noudattaen. Mainittu aineistolähtöinen analyysi on kolmivaiheinen prosessi, jossa aineiston ensin pelkistetään eli redusoidaan. Tämän jälkeen aineisto

ryhmitellään eli klusteroidaan. Viimeisessä vaiheessa aineisto abstrahoidaan eli luodaan teoreettiset käsitteet. Kuviossa 4 esitetään aineistolähtöisen sisällönanalyysin eteneminen. (Mts. 91-95.)



Kuvio 5. Teorialähtöinen sisällönanalyysi (Tuomi & Sarajärvi 2018, 97).

Analyysissa tarvittavan aineiston määrällä on myös merkitystä. Kanasen (2014, 94): mukaan riittävää aineiston määrää pohdittaessa nousee esiin kolme kysymystä

1. Tietojen keräämiseen käytetyt menetelmät
2. Tarvittavan tiedon määrä
3. Montako kohdetta / osallistujaa tarvitaan

Laadullisessa tutkimuksessa ei voida puhua otantateorian mukaisesta otannasta, jolloin tutkimuksessa käytettyjen tutkimuskohteiden tulee täyttää ilmiön kannalta olennaiset tuntomerkit. Koska otantaa ei tehdä, ei myöskään kyseistä termiä tule käyttää tutkimuksen raportoinnissa. Laadulliseen tutkimukseen valitut haastateltavat valitaan harkinnanvaraisesti eikä laadullisessa tutkimuksessa ei ole selvää määräsääntöä. Saturaatiolla tarkoitetaan tilannetta, jossa havaintoyksikköjen lisääntyessä tulkinta ei enää muutu eli uudet tapaukset eivät enää tuo uutta tietoa. (Kananen 2014, 95.)

Analyysia ja aineiston keräämistä jatketaan yleensä siihen asti, kunnes aineistosta ei löydy enää uusia näkökulmia. Sisällön analyysissä voidaan myös yhdistää sekä laadullinen että määrällinen tutkimusote, jolloin nämä täydentävät toisiaan. (Seitamaa-Hakkarainen N.d.) Saturaatio on tilanne, jossa aineisto alkaa toistaa itseään eivätkä tiedonantajat tuota enää uutta tutkimusongelmaan liittyvää tietoa. Perusajatuksena on, että tietty määrä tietoa riittää tuomaan esiin teoreettisen peruskuvion. (Tuomi & Sarajärvi 2018, 74.)

2.3.1 Litterointi

Litteroinnilla tarkoitetaan erilaisten tallenteiden muuttamista kirjalliseen muotoon, jonka jälkeen käsittely manuaalisesti tai ohjelmallisesti eri analyysimenetelmillä on mahdollista. Litterointi on hidas työvaihe, joten tutkijan on valittava mitä kaikkea hän litteroi. Myös litteroinnin taso voidaan valita sanantarkan, yleiskielisen ja propositiotason litteroinnin väliltä. Näistä ensimmäinen on tarkin ja siinä jokainen äännähdyskin kirjataan ylös. Yleiskielisessä litteroinnissa teksti muutetaan kirjakielelle poistamalla murre- ja puhekielen ilmaisut. Propositiotason litteroinnissa kirjataan vain ydinsisältö ylös. (Kananen 2014, 101-102.)

2.3.2 Koodaus

Koodaamisen avulla litteroitu teksti tiivistetään helpommin käsiteltävään muotoon analyysinvaiheen mahdollistamiseksi. Koodauksen avulla aineistoa pyritään selkeyttämään ja tiivistämään, jotta tutkijalla olisi mahdollisuus ”avata” aineisto tai ”nähdä” aineiston sisään. Koodaamalla aineistosta yritetään kaivaa esille olennaisin osa, jonka avulla ilmiöön liittyvä salaisuus pyritään saamaan esille. Koodaamisessa aineiston tietoja yhdistetään siten, että samaa tarkoittavat asiat merkitään samalla koodilla sekä myös sellaiset asiat, joilla on yhteinen elementti tai tekijä. Koodaus itsessään ei ole vielä analyysi vaan välivaihe matkalla analyysiin. Varsinaisessa analyysissä pyritään luodun koodauskehikon avulla löytämään aineistosta rakenteita, säännönmukaisuuksia, teemoja ja malleja. Koodauksen tason valinnassa tulee olla tarkkana, sillä liian ylätasoinen koodaus kadottaa osan aineiston tiedoista ja liian tiivis koodaus tekee tulkinnasta hankalaa. (Kananen 2014, 103-104.)

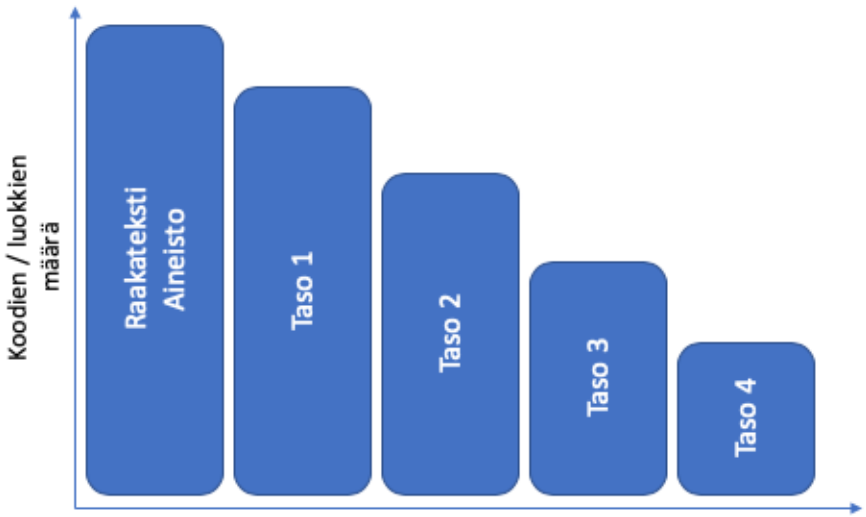
Koodimerkeille ei ole yhtenäistä sovittua merkintätapaa eli jokainen tutkija päättää itse millaisia koodimerkkejä tutkimuksessa käytetään. Tuomi ja Sarajärvi (2018, 79) esittelevät Eskolan & Suorannan (2014) listauksen mukaiset koodimerkkien viisi tehtävää:

1. Koodimerkit toimivat sisäänkirjoitettuina muistiinpanoina
2. Niiden avulla jäsennetään tutkijan näkemystä aineiston sisällöstä
3. Koodimerkit toimivat tekstin kuvailun apuvälineinä
4. Niiden avulla voidaan testata aineiston jäsentelyä
5. Niiden avulla voidaan etsiä ja tarkistaa tekstin eri kohtia eli ne toimivat osoitteina aineistoon

2.3.3 Luokittelu, teemoittelu ja tyypittely

Luokittelu on yksinkertaisin aineiston järjestämisen tapa ja sitä pidetään kvantitatiivisena analyysinä sisällön teemoin. Yksinkertaisimmassa muodossa aineistosta määritellään luokkia, jonka jälkeen lasketaan montako ilmentymää jokaisella luokalla aineistossa on. Luokiteltu aineisto voidaan esittää taulukkona. *Teemoittelu* on luokituksen kaltaista, mutta siinä painotetaan mitä kustakin teemasta on sanottu. Kyse on aineiston pilkkomisesta ja ryhmittelystä aihepiirien mukaan, jolloin on mahdollista vertailla teemojen esiintymistä aineistossa. *Tyypittelyssä* aineisto ryhmitellään tiettyjen tyyppien mukaan. Tyypit tai tyyppiesimerkit ovat tiettyjen teemojen sisältä löydettyjä yhteisiä ominaisuuksia. Tarkoituksena on tiivistää joukko tiettyä teemaa koskevia näkemyksiä yleistykseksi. (Tuomi & Sarajärvi 2018, 79.)

Luokittelussa koodatut tekstisegmentit yhdistetään toisiinsa samaa tarkoittavien asioiden ja käsitteiden avulla. Luokittelun avulla pyritään löytämään loogisia kokonaisuuksia siten, että samaa tarkoittavat käsitteet yhdistetään yhden käsitteen alle. Myös eri käsitteet voidaan yhdistää yhden käsitteen alle. Koodauksen avulla aineistoa pyrittiin tiivistämään ja luokittelun avulla pyritään pääsemään aineiston kanssa teoreettisten käsitteiden tasolle (Kananen 2014, 113.)



Kuvio 6. Koodauksen ja sitä seuraavan luokittelun idea (Kananen 2014, 113).

Sisällön analyysi on laadullisen aineiston analyysimenetelmä, joka korostaa tekstin sisällön ja laadun merkityksiä. Kvantitatiivisen sisällön analyysin luokittelussa voidaan analyysissä käytettävä luokittelu johtaa teoriasta, puhtaasti aineistosta tai aineiston luokitusrunko on näiden yhdistelmä. Kvalitatiivisen sisällön analyysin tavoite on saavuttaa systemaattinen ja kattava kuvaus aineistosta. (Seitamaa-Hakkarainen N.d.)

Käsitteitä tiivistetään tasolta seuraavalle siirryttäessä niin, että luokittelu ja uuden tason koodaus etenevät samanaikaisesti. Esimerkiksi Kuviossa 3 tasolla 4 on enää yksi käsite, joka tiivistää kaikki tason 3 käsiteet sopivalla koodilla. Luokittelemalla saadun ratkaisun tulee pitää sisällään käsitteellisesti käsite tai ilmiö, joka kuvaa koodattua ilmiötä. (Kananen 2014, 113.)

Analyysin aikana luokittelukategoriat kehittyvät ja muuttuvat mahdollisen lisäaineiston keruun myötä. Luokittelukategoriat ovat joustavia välineitä aineiston hahmottamiseen. Uusia analyysiluokkia voi syntyä analyysin edetessä ja analyysi yhdistyy synteesiin. Luokittelun perustana on vertailu ja vastakkainasettelu, joita käytetään koko analyysin ajan aineiston luokittelussa kategorioihin. (Seitamaa-Hakkarainen N.d.)

Analyysin luokitteluvaiheessa tulee päättää, haetaanko aineistosta samanlaisuutta vai erilaisuutta. Aineistosta voidaan myös hakea toiminnan logiikkaa, tyypillistä kertomusta tai kirjoittaa kaikista vastauksista yksi tyypillinen kertomus. (Tuomi & Sarajärvi 2018, 79.)

2.3.4 Tulokset

Kanasen (2014) mukaan Yin (2009) esittää aineistosta haettavaksi tyypillistä kertomusta, toiminnan logiikkaa, samanlaisuutta tai erilaisuutta tai selitystä ilmiölle. Tutkija voi löytää aineistosta erilaisia asioita sen mukaan, mitä näkökulmaa hän aineistoa käsitellessään käyttää. Aineistosta voidaan siis löytää monia tulkintoja. (Kananen 2014, 115.)

2.4 Yhteenveto

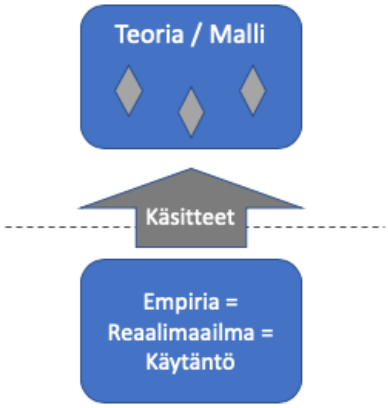
Tutkimuksissa tutkimusongelma ratkaistaan tutkimusmenetelmien avulla. Tutkimusotteet jakautuvat siten, että ääripäissä ovat laadullinen tutkimus ja määrällinen tutkimus ja näiden välille sijoittuvat erilaiset tutkimusstrategiat kuten case-, kehittämis- ja toimintatutkimus. Tutkimusote on laaja ongelmanratkaisun lähestymistapa, johon sisältyy kullekin otteelle ominaiset tiedonkeruun, analysoinnin ja tulkinnan menetel-

mät. Laadullisen tutkimusotteen tiedonkeruumenetelmiä ovat dokumentit, havainnointi ja haastattelut, kuten teemahaastattelut. Haastattelemalla kerätty tutkimusaineisto litteroidaan, jonka jälkeen se voidaan analysoida esimerkiksi sisällönanalyysin avulla. Sisällönanalyysissa aineisto koodataan ja luokitellaan käsitteitä hyväksi käyttäen ja analyysin aikana päätetään, haetaanko aineistosta samanlaisuutta vai erilaisuutta. Tuloksina aineistosta voidaan hakea tyypillistä kertomusta, toiminnan logiikkaa, samankaltaisuutta, erilaisuutta tai muuta selitystä ilmiölle.

3 Teoreettinen viitekehys ja peruskäsitteet

Tutkimuksen tekeminen vaatii tuekseen teoreettista viitekehystä valitusta tutkimusmenetelmästä riippumatta. Teorian eli tietoperustan lisäksi myös tutkimukseen liittyvät keskeiset peruskäsitteet tulee määritellä johdonmukaisesti ja perusteellisesti. Jo tutkimuksen laadukas kysymyksenasettelu edellyttää teoreettisen viitekehyksen tuntemusta. Kanasen (2015, 26) mukaan tutkimukseen liittyvä kysymyksenasettelu pohjautuu tutkittavaan ilmiöön ja siihen, mitä siitä jo tiedetään eli sitä selittäviin teorioihin. Kananen myös esittää, että teoriat selittävät tutkittavaa ilmiötä ja antavat vastaukset peruskysymykseen mikä tai mitkä. (Kananen 2013, 25.)

Tutkimuksen teoria ja viitekehys voivat tarkoittaa samaa asiaa, sillä niin teoria kuin viitekehyskin kuvaavat tutkimuksen keskeisiä käsitteitä ja niiden välisiä merkityssuhteita. Viitekehyksen voi jakaa käsitteellisenä ilmiönä kahteen osaan, jotka ovat tutkimusta ohjaava metodologia ja se, mitä tutkittavasta ilmiöstä jo tiedetään. (Tuomi & Sarajärvi 2018, 18.)



Kuvio 7. Teoria liittyy aina käytäntöön (Kananen 2013, 45).

Teorialla ja reaalimaailmalla on aina yhteys, sillä teoria liittyy aina käytäntöön ja se on yksinkertaistus empiriasta. Käsitteitä käytetään apuna teorian kuvaamisessa ja niiden avulla määritellään ilmiöön vaikuttavat tekijät sekä näiden väliset suhteet. Tieteellisen työn teoriaosuutta eli teoreettista viitekehystä tarvitaan selittämään joko tutkittavaa ilmiötä tai käytettyjä menetelmiä. (Kananen 2013, 45.)

Teoreettisella viitekehyksellä voi olla useita tulokulmia tutkimuksen tekemisessä. Se voi ohjata tieteellisen tutkimuksen etenemistä mutta se voi olla myös tutkimuksen lopputulos. Tieteellisen toiminnan osana on aina myös palautus takaisin teoriamaailmaan. Tutkimuksessa voidaan joko pyrkiä luomaan teoriaa tai testata jo olemassa olevaa teoriaa. Opinnäytetyössä teoreettisen viitekehyksen avulla pyritään myös antamaan työn tekijän perehtyneisyydestä riittävä kuva lukijalle. (Mts. 48-49.)

Kanasen (2013) mukaan laadullisen tutkimuksen osalta teoreettisella viitekehyksellä on oma merkityksensä työn tekemisessä. Laadullisessa tutkimuksessa pyritään usein

pääsemään yksittäisistä tapauksista yleistyksiin. Tällöin kyseessä on induktiivinen päättely, jossa kerätyn havaintoaineiston pohjalta pyritään tekemään yleistyksiä tai luomaan uusia teorioita. (2013, 49.)

Laadullinen tutkimus on tutkimustyypiltään empiiristä ja siinä on kyse havaintoaineiston tarkastelusta ja argumentoinnista empiirisen analyysin tavoilla (Tuomi & Sarajärvi 2018, 20).

3.1 Tietoturvallisuuteen liittyvät tutkimus- ja tieteenalat

Porvari (2012, 39) listaa väitöskirjassaan tietoturvallisuuteen liittyviä tieteenaloja. Keskeisiä hänen tunnistamiaan tieteenaloja ovat taloustieteet, hallintotieteet, käyttäytymistieteet, tilastotiede ja todennäköisyyslaskenta sekä tekniikka ja tietojenkäsittelytiede.

Kuvio 8. Turvallisuuteen liittyviä tieteenaloja (Porvari 2012, 39).

3.2 Aiempi tutkimus aiheesta

Aiemman tutkimuksen etsiminen Doria-, Aaltodoc, Jyx-, Theseus- tai Janet Finna -tietokannoista ei tuota relevantteja osumia tutkimuksen aiheeseen liittyen. Iso osa hakutuloksista käsittelee kansallisia kyberturvallisuusstrategioita. Ne muutamat hakutulokset, jotka palauttavat muita tuloksia ovat joko viittauksia liian vanhoihin julkaisuihin tai ne käsittelevät tietoturvallisuuden teknisiä ratkaisuja.

Haku sanoilla ”Cyber Strategy” Doria-tietokannasta palauttaa Mirva Salmisen artikkelin ”Government of Cyber Security as National Security” vuodelta 2015, joka käsittelee Suomen kansallista kyberturvallisuusstrategiaa. Samaa aihetta käsittelee myös saman haun toisena tuloksena tullut Niklas Nykterin tutkielma ”KNOWING ME, KNOWING YOU - National Cyber Security Situation Understanding Within a Network of actors” vuodelta 2018. Molemmat näistä ovat Maanpuolutuskorkeakoulun julkaisuja eivätkä ne sinänsä käsittele yrityksiin liittyvää tietoturvallisuuden strategista johtamista.

Aaltodoc-tietokannasta löytyy hakusanalla ”Cyber Strategy” Jarno Limnellin ja Martti Lehdon artikkeli vuodelta 2019 ”The importance of strategic leadership in cyber security”, joka niin ikään käsittelee Suomen kansallista kyberturvallisuusstrategiaa. Muita relevantteja hakutuloksia ei tule.

Sekä Doria että Aaltodoc palauttavat samat hakutulokset hakusanoilla ”Information Security Strategy”. Jyx-tietokannasta ei löydy uusia hakutuloksia kummallakaan hakusanalla. Myöskään hakusana ”Cybersecurity strategy” ei palauta relevantteja tuloksia edellä mainituista tietokannoista.

Janet Finna -tietokanta ei palauta relevantteja hakutuloksia millään edellä mainituista hakusanoista. Kuten ei myöskään Theseus.

3.3 Yhteenveto

Teoreettisen viitekehyksen avulla tutkija saa käsityksen tutkittavasta aihealueesta ja siihen liittyvistä keskeisistä käsitteistä. Tutkimukseen liittyvän kysymyksenasettelun tulee pohjautua tutkittavaan ilmiöön liittyvään olemassa olevaan tietoon. Tutkittavaan ilmiöön liittyvien tieteenalojen avulla voidaan yrittää löytää olemassa olevaa aiheeseen liittyvää tutkimusta. Aiempi tutkimus voi johtaa tutkimuksen teoreettiseen viitekehykseen liittyvien lähteiden äärelle tai tutkija voi saada tarkentavia ideoita oman tutkimuksensa tekemiseen. Tutkijan käyttämillä hakutermeillä ei löytynyt relevanttia aiempaa tutkimusta valitusta aiheesta.

4 Tietoturvallisuuden johtaminen on riskienhallintaa ja monimutkaisten kokonaisuuksien hallitsemista

4.1 Uhka

Uhka (*Threat*) on mikä tahansa tapahtuma tai olosuhde, jolla on mahdollinen haitallinen vaikutus organisaatioon tai sen toimintaan tietojärjestelmän tai sen sisältämän tiedon luvattoman käytön, tuhoamisen, paljastamisen, muuttamisen tai palvelun käytön estämisen kautta. Uhkatapahtumia aiheuttavat uhkalähteet (*Threat source*) pyrkivät joko haavoittuvuuden tarkoitukselliseen hyödyntämiseen ja sitä varten luotujen menetelmien käyttöön tai ne hyödyntävät haavoittuvuutta tai siihen liittyvää

menetelmää vahingossa. Tyypillisimpiä uhkalähteitä ovat tarkoitukselliset vihamieliset kyber- tai fyysiset hyökkäykset, henkilöstön tahallisesti tai tahattomasti aiheuttamat poikkeamat, rakenteelliset viat organisaation järjestelmäarkkitehtuurissa tai organisaation hallinnan ulkopuoliset luonnonkatastrofit, onnettomuudet ja viat. (NIST Special Publication 800-30, 8.)

VAHTI-ohjeessa uhka määritellään mahdollisesti tapahtuvaksi haitalliseksi tapahtumaksi tai useammaksi mahdolliseksi häiriöksi, joilla on ei-toivottu vaikutus tiedolle, omaisuudelle tai toiminnalle (Valtionhallinnon tietoturvasanasto 2008, 122).

4.2 Haavoittuvuus

Haavoittuvuus (*Vulnerability*) on tietojärjestelmässä, tietojärjestelmän turvallisuusmenettelyissä, valituissa kontrolleissa tai toteutuksessa oleva heikkous, jota uhkalähteen on mahdollista käyttää hyväkseen. Usein tietojärjestelmien haavoittuvuudet liittyvät joko kokonaan toteuttamattomiin tai huonosti toteutettuihin turvakontrolleihin. Haavoittuvuuksia voi myös ilmaantua ajan myötä, kun organisaatio kehittyy, sisäiset ja ulkoiset toimintaympäristöt muuttuvat, uusia teknologioita otetaan käyttöön ja uusia uhkia tulee esiin. (NIST Special Publication 800-30, 9.)

VAHTI-ohje määrittelee haavoittuvuuden turvatoimien sekä suojausten heikkouden lisäksi niissä olevina puutteina sekä alttiutena turvallisuutta uhkaaville tekijöille (Valtionhallinnon tietoturvasanasto 2008, 30).

4.3 Riski

Riski (*Risk*) mittaa sitä missä laajuudessa mahdollinen olosuhde tai tapahtuma uhkaa kohdetta. Riskiä voidaan kuvata olosuhteista aiheutuvien kielteisten vaikutusten (impakti) ja tapahtuman todennäköisyyden funktiona. Tietoturvariskit johtuvat tietojen tai tietojärjestelmien luottamuksellisuuden, saatavuuden tai eheyden menettämisestä ja niillä on haitallisia vaikutuksia organisaation toimintaan. (NIST Special Publication 800-30, 6.)

Porvarin (2012, 41) mukaan NIST (NIST 1994) määrittelee riskitulon eli vahingon odotusarvon laskettavaksi seuraavasti:

$$R = p * V,$$

missä p on tietyllä haavoittuvuudella oleva uhan toteutumisen todennäköisyys ja V on mahdollisen menetyksen suuruus.

IRAM2 on Information Security Forumin kehittämä tietoturvariskien arviointimenetelmä, joka määrittelee ISO Guide 73:2009 mukaisesti riskin olevan ”epävarmuuden vaikutus tavoitteisiin”. Tämän määritelmän mukaan riskin lopputulema ei aina välttämättä ole negatiivinen vaan myös positiivinen lopputulos on mahdollinen. IRAM2:n mukaisessa riskin määrittelyssä keskiössä on kaksi tekijää, jotka ovat tietyn tapahtuman todennäköisyys (epävarmuus) ja vaikutus, joka edellä mainitulla tapahtumalla voisi olla asetettujen tavoitteiden saavuttamiseen. Todennäköisyys on mahdollisuus sille, että määritelty uhka käynnistää onnistuneen uhkatapahtuman tietyssä ajassa. Vaikutus on organisaatiota kohdanneen vahingon suuruus onnistuneessa uhkatapahtumassa. IRAM2:n määritelmän mukaan tietoturvariski on luottamuksellisuuden,

eheyden tai saatavuuden vaarantumisesta johtuva riski organisaatiota kohtaavasta menetyksestä. IRAM2:n määrittelyn mukainen riskiyhtälö on yhteneväinen aiemmin mainitun NIST:n määrittelyn kanssa (Riski = Todennäköisyys X Vaikutus). (IRAM2 2017, 3.)

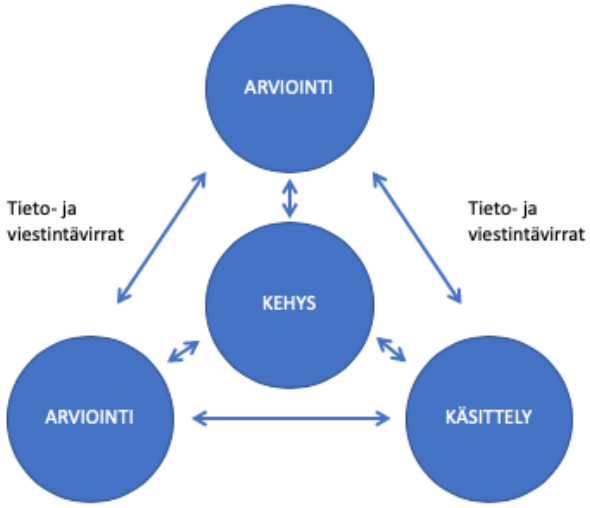
4.4 Riskien arviointi

Riskien arviointi (*Risk assessment*) on prosessi tietoturvariskien tunnistamiseksi, arvioimiseksi ja priorisoimiseksi. Riskien arvioinnissa uhka- ja haavoittuvuustietojen analysoinnin avulla määritetään, missä määrin olosuhteet ja tapahtumat voisivat vaikuttaa vahingollisesti organisaatioon ja millä todennäköisyydellä näin voisi tapahtua. Riskinarviointimenetelmä (*Risk assessment methodology*) koostuu tyypillisesti riskienarviointiprosessista, riskimallista, riskien arviointimenetelmästä ja riskien analyysimenetelmästä. Arviointimenetelmä voi olla kvantitatiivinen, kvalitatiivinen tai puolikvalitatiivinen ja siinä määritellään tunnistettujen riskien mahdolliset arvoalueet riskiarvioinnin aikana ja miten riskitekijöiden yhdistelmät tunnistetaan ja analysoidaan riskin arvioimiseksi. Riskien analyysimenetelmä voi olla esimerkiksi uhkaorientoitunut, vaikutuksiin tai haavoittuvuuksiin keskittyvä tai (tieto)omaisuuteen suuntautuva. Analyysimenetelmän avulla varmistetaan, että ongelma-alueet katetaan riittävän yksityiskohtaisella tasolla. (NIST Special Publication 800-30, 6-7.)

Valittujen turvakontrollien tehokkuudella on taipumus heikentyä ajan myötä organisaation ja toimintaympäristön muuttuessa, joten riskiarviointeja tulee tehdä säännöllisesti järjestelmän kehittämisen ja käytön elinkaaren ajan. (NIST Special Publication 800-30, 9.)

4.5 Riskienhallinta

Riskienhallinta (*Risk Management*) on suunnitelmallista toimintaa riskien rajoittamiseksi siten, että riskien rajoittamisen kustannukset pysyvät hallittuina ja organisaation tavoitteet voidaan saavuttaa. Riskienhallinnan vaiheita oat riksianalyysi, hallintamenetelmän valinta, päätös riskien käsittelystä sekä riskienhallinnan organisointi. (Valtionhallinnon tietoturvasanasto 2008, 81.)



Kuvio 9. Riskienhallintaprosessi (NIST Special Publication 800-39, 8).

Riskienhallinta on kokonaisvaltaista koko organisaation kattavaa toimintaa, jonka osia ovat riskienhallinnan viitekehyksen luominen riskiperusteisen päätöksen teon tueksi, riskien arvioinnit, tunnistettujen riskien käsittely ja riskien jatkuva monito-

rointi. Riskienhallinnan tehtävänä on varmistaa riskiperusteisen päätöksenteon integroiminen osaksi koko organisaation toimintaa. Tunnistettu riski voidaan käsitellä hyväksymällä, välttämällä, vähentämällä, jakamalla tai siirtämällä se. (NIST Special Publication 800-39, 6-7.)

4.6 Kontrollit

Kontrolleilla (*Control*) tarkoitetaan niitä ennaltaehkäiseviä, havaitsevia tai korjaavia toimia, joilla varaudutaan tai suojaudutaan tietoturvaloukkauksia tai haitallisia tapahtumia vastaan. Kontrollit voivat olla esimerkiksi riskienhallinnan tavoitteita tai käytettävissä olevia menetelmiä, suunnitelmallista jatkuvaa toimintaa tai kertaluonteisia tai jatkuvia toimenpiteitä. (Valtionhallinnon tietoturvasanasto 2008, 51.)

Tietoturvakontrollien avulla suojataan tietojärjestelmiä ja organisaatiota sekä pyritään varmistamaan näiden sisältämien, käsittelemien ja välittämien tietojen luottamuksellisuus, eheys ja saatavuus. Kontrollien avulla pyritään myös toteuttamaan määritellyt turvallisuusvaatimukset. (NIST Special Publication 800-53, 1.)

Tietoturvallisuuden standardit kuten ISO/IEC 27002 ja NIST SP 800-53 listaavat valmiita kontrolleja, joita organisaatiot voivat hyödyntää oman riskienhallinnan viitekehyksensä mukaisesti. Tietoturvakontrollit ovat luonteeltaan ja toteutuksiltaan erilaisia ja niitä voidaan toteuttaa esimerkiksi politiikkojen, valvontakeinojen, manuaalisten prosessien, yksittäisten toimenpiteiden tai automaattisten toimintojen avulla. (NIST Special Publication 800-53, 9.) Eri standardit ja viitekehykset ryhmittelevät kontrollit niihin liittyvien aihealueiden mukaan. NIST SP-800-53 ja ISF:n The standard of Good Practice listaavat molemmat 18 kontrolliryhmää, kun taas ISO/IEC 27002 listaa 14 pääluokkaa.

4.7 Hallinnollisen tietoturvallisuuden standardit ja -viitekehykset

Alla on listattuna yleisiä tunnettuja tietoturvallisuuden standardeja ja viitekehyksiä. Listasta on jätetty tarkoituksella pois toimialakohtaiset viitekehykset ja standardit.

ISO/IEC 27001

ISO/IEC 27001 on laajalti tunnettu ja kansainvälinen ISO/IEC 27000 standardiperheeseen kuuluva tietoturvastandardi, jonka ovat julkaisseet International Organization for Standardization (ISO) yhdessä International Electro-technical Commission (IEC) kanssa. ISO/IEC 27001 määrittelee tietoturvallisuuden hallintajärjestelmän (*information security management system*) rakentamiseen, ylläpitämiseen ja kehittämiseen liittyvät vaatimukset. Standardi sisältää myös vaatimukset tietoturvariskien arvioinnista ja käsittelystä. Standardin avulla organisaatio pystyy valitsemaan liiketoiminnan laajuuteen suhteutetut tietoturvakontrollit suojattavien kohteiden turvaamiseksi. ISO/IEC 27001 standardia tukee ISO/IEC 27002 standardi, joka antaa menettely- ja toteutusohjeet ISO/IEC 27001 mukaisen tietoturvallisuuden hallintajärjestelmän käyttöönottoon. Organisaation on mahdollista hakea virallista sertifiointia ISO/IEC 27001 standardin asettamia vaatimuksia vasten. (Dekker, Karsberg, Lakka & Liveri 2013, 3-4.)

VAHTI-ohjeisto

Valtiovarainministeriön asettaman Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) tehtävänä on julkishallinnon ja valtionhallinnon tietoturvallisuuden ohjaaminen ja kehittäminen. Vahti pyrkii toiminnallaan edistämään valtionhallinnon toimintojen tietoturvallisuutta sekä käsittelemään tietoturvallisuuden linjaukset. VAHTI-ohjeisto on edellä mainitun digitaalisen johtoryhmän ohjesivusto, joka sisältää laajan kokoelman ohjeita digitaalisen turvallisuuden kehittämiseen ja varmistamiseen. VAHTI-ohjeen 2/2010 Liite 5 kappale 1 asettaa vaatimukset tietoturvallisuuden hallinnalle. (Valtionhallinnon tietoturvallisuuden johtoryhmä 2010, 10.)

NIST Cybersecurity Framework

NIST Cybersecurity Framework on yleiskäyttöinen tieto- ja kyberturvallisuuden viitekehys, jonka avulla eri kokoiset organisaatiot toimialasta riippumatta voivat vahvistaa tietoturvallisuutensa tasoa. Cybersecurity Framework -viitekehys perustuu viisiportaisen prosessiin, jonka avulla hallitaan tietoturvariskejä sekä ylläpidetään turvallisia järjestelmiä. Viitekehyksestä on pyritty tekemään helposti lähestyttävä, jolloin myös matalammalla kypsyystasolla olevien organisaatioiden on helppo lähteä kehittämään toimintaansa sen avulla. (Dawson 2019.)

NIST SP 800-53

NIST Special Publication 800-53 on yhdysvaltalaisen kauppaministeriön alaisen viraston National Institute of Standards and Technologyn tekemä julkaisu, joka sisältää tietoturva- ja tietosuojakontrolleja Yhdysvaltain liittovaltion tietojärjestelmien suojaamiseen. (NIST Special Publication 800-53 Rev. 4 2013, xv.)

The Standard of Good Practice for Information Security

Information Security Forumin julkaisema The Standard of Good Parctice for Information security on liiketoimintalähtöinen ja laaja-alainen ohjeistus tietoturvakontrollien

toteuttamiseksi ja tietoturvariskien hallitsemiseksi tunnettujen hyvien käytäntöjen avulla. Julkaisun kontrollit ja suositukset toteuttamalla voi samalla kattaa myös seuraavien viitekehysten asettamat vaatimukset: ISO/IEC 27002, NIST Cybersecurity Framework, CIS Top 20, PCI DSS ja COBIT 5 for Information Security. (Information Security Forum 2018).

COBIT 5 for Information Security

COBIT (Control Objectives for Information and related Technology) on ISACAN alun perin vuonna 1996 julkaisema liiketoimintalähtöiseen IT-hallintoon suunnattu viitekehys. Viitekehyksen viimeisin versio COBIT 5 julkaistiin vuonna 2012. COBIT on korkean tason viitekehys, joka toimii yhteen muiden tarkempien standardien, viitekehysten ja hyvien käytäntöjen, kuten COSO, TOGAF, ITIL ja ISO 27000-sarjan standardit kanssa. ISACA on julkaissut viitekehykseen tietoturvaan liittyvän laajennoksen ”COBIT 5 for Information Security”, joka toimii myös ylätason viitekehyksenä ja jonka avulla organisaatiot voivat kehittää tietoturvallisuuteen liittyvää toimintaansa COBIT-mallin mukaisesti. Tämä laajennos on yhteensopiva muun muassa ISO/IEC 27000 standardiperheen sekä ISF:n ja NIST:n viitekehysten kanssa. (Dekker ym. 2013, 6.)

4.8 Tietoturvallisuuden osa-alueet

Tietoturvallisuuteen kuuluvien osa-alueilla ei ole vakiintunutta määrittelyä, jolloin määrittely vaihtelee viitekehyksittäin. Erot eivät ole suuria ja keskeiset tunnetut viitekehykset pyrkivät huomioimaan varsin kattavasti tietoturvallisuuden keskeiset osa-alueet. Eroja syntyy osa-alueiden sisällön painotuksissa, ryhmittelyssä sekä erilaisissa tavoissa lähestyä kokonaisuutta. Alla olevassa taulukossa on listattuna neljän eri viitekehysten tietoturvallisuuden osa-alueiden määritelmiä. Taulukossa ei ole huomioitu erilaisia lähestymistapoja, joten esim. NIST Cybersecurity Frameworkin osalta siinä toistuvat osa-alueet on kirjattu taulukkoon vain kertaalleen.

Taulukko 1. Tietoturvallisuuden osa-alueet eri viitekehyksissä

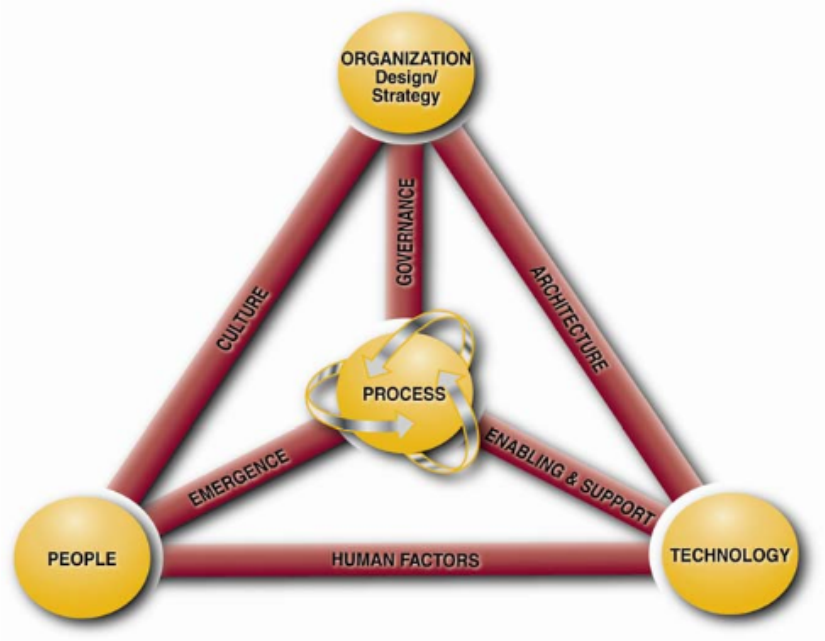
Viitekehys	**The Standard of Good Practice for Information Security 2018**	**NIST Cybersecurity Framework**	**ISO/IEC 27002**	**NIST SP 800-53**
Lähde	The Standard of Good Practice for Information Security 2018, 4-6	Framework for Improving Critical Infrastructure Cybersecurity 2018, 23	SFS-EN ISO/IEC 27002:2017, 89-90	NIST Special Publication 800-53 Rev. 4. 2013, 9
1	Security Governance	Asset Management	Information Security Policies	Access Control
2	Information Risk Assessment	Business Environment	Organization of Information Security	Awareness and Training
3	Security Management	Governance	Human Resource Security	Audit and Accountability
4	People Management	Risk Assessment	Asset Management	Security Assessment and Authorization
5	Information Management	Risk Management Strategy	Access Control	Configuration Management
6	Physical Asset Management	Supply Chain Risk Management	Cryptography	Contingency Planning
7	System Development	Identity Management and Access Control	Physical and Environmental Security	Identification and Authentication
8	Business Application Management	Awareness and Training	Operations Security	Incident Response
9	System Access	Data Security	Communications Security	Maintenance

10	System Management	Information Protection Processes and Procedures	System Acquisition, Development and Maintenance	Media Protection
11	Networks and Communications	Maintenance	Supplier Relationships	Physical and Environmental Protection
12	Supply Chain Management	Protective Technology	Information Security Incident Management	Planning
13	Technical Security Management	Anomalies and Events	Information Security Aspects of Business Continuity Management	Personnel Security
14	Threat and Incident Management	Security Continuous Monitoring	Compliance	Risk Assessment
15	Local Encironment Management	Detection Process		System and Services Acquisition
16	Business Continuity	Reponse Planning		System and Communications Protection
17	Security Monitoring and Improvement	Communications		System and Information Integrity
18		Analysis		Program Management
19		Mitigation		
20		Improvements		
21		Recovery Planning		

4.9 Tietoturvallisuuden rakenne

Perinteisesti tietoturvallisuutta on tutkittu ja kuvattu kaksiulotteisen mallin kautta, jossa keskeiset ja ainoat komponentit ovat olleet ihmiset (*people*), prosessit (*process*) ja teknologia (*technology*). The Institute for Critical Information Infrastructure Protection (ICIIP) on kehittänyt käsitteellisen viitekehyksen laajentamaan näitä kolmea elementtiä siten, että kyseinen kehys lisää uusiksi elementeiksi sen, miten ihmiset, prosessit, tekniikka ja organisaation järjestäytyminen ovat kaikki monimutkaisessa vuorovaikutuksessa keskenään. Yhdessä nämä muodostavat kokonaisvaltaisen tietoturvallisuuden rakenteen.

ICIIP:n Systematic Security Management -mallissa (*SSM)* edellä mainittujen kolmen elementin rinnalle on tuotu neljäntenä elementtinä organisaation strategia ja rakenne sekä lisäksi myös eri elementtien väliset yhteydet ja niiden keskinäinen vuorovaikutus toisiinsa. ICIIP:n laajennettu malli voi vaikuttaa monimutkaiselta ja saada tietoturvallisuuden rakenteen vaikuttamaan vaikealta lähestyä mutta se pakottaa ottamaan huomioon keskeisen tekijän eli elementtien välisen dynamiikan ja auttaa täten tunnistamaan kokonaisturvallisuuteen vaikuttavat tekijät aiempaa paremmin.



Kuvio 10. ICIIP SSM -malli (Kiely & Benzel 2006, 3)

ICIIP SSM -malli kuvataan kolmiulotteisena pyramidina, jonka solmujen välisiä yhteyksiä kuvataan termillä jännite johtuen niiden dynaamisista ja usein kilpailevista sekä ristiriitaisista suhteista toisiinsa. Kokonaisturvallisuuden edistämiseksi kaikkia

näitä elementtejä sekä niiden välisiä vuorovaikutuksia eli jännitteitä on pystyttävä arvioimaan ja mittaamaan sekä pyrittävä ymmärtämään paremmin. (Kiely & Benzel 2006, 2-3).

4.10 Tietoriski ja tietoturvariski

Valtionhallinnon tietoturvasanasto erottelee toisistaan tietoriskin ja tietoturvariskin. Tietoriskillä (*Information Risk*) tarkoitetaan joko tietoon kohdistuvaa tai itse tiedosta aiheutuvaa riskiä (Valtionhallinnon tietoturvasanasto 2008, 104), kun taas tietoturvariski (*Information Security Risk*) kattaa tiedon lisäksi tietoliikenteeseen tai tietojärjestelmään kohdistuvan vahingon uhan (Valtionhallinnon tietoturvasanasto 2008, 111).

Tietoturvariskit ovat riskejä, jotka johtuvat tietojen tai tietojärjestelmien luottamuksellisuuden, eheyden tai saatavuuden menettämisestä ja jotka voivat vaikuttaa organisaation toimintaan, varoihin (ml. tietovarannot), työntekijöihin tai yhteistyötahoihin haitallisesti (NIST Special Publication 800-30 2012, 6).

4.11 Suojattava kohde

Suojattava tai turvattava kohde (*asset*) on organisaatiolle arvokas kohde, kuten eri muodoissa olevat tiedot, tietojärjestelmät, resurssit, toiminnot, palvelut, fyysinen ympäristö, ihmiset ja osaaminen, käyttöympäristö ja tietojenkäsittelytilat, ulkoiset palvelut sekä edellä listattuja palvelevat prosessit. (Valtionhallinnon tietoturvasanasto 2008, 121.)

4.12 Tietoturvapolitiikka

Tietoturvapolitiikka (security policy) on ennalta määritelty joukko sääntöjä ja käytäntöjä, joiden avulla organisaatio pyrkii varmistamaan suojattavien tietojen sekä kriittisten järjestelmäresurssien suojaamisen. (RFC 2828 2000, 154.)

ISO/IEC 27003 mukaan tietoturvapolitiikka on koko henkilöstön ja tarvittavien sidosryhmien saatavilla oleva dokumentti, jonka on tarkoitus ohjata organisaation tietoturvatyötä organisaation strategisten tavoitteiden mukaisesti. Politiikan avulla tuodaan esiin, mitä tietoturvallisuuden tarpeita organisaatiolla on toimintaympäristössään ja sen tulisi sisältää ylätasoiset kuvaukset tietoturvallisuuden tavoitteista sekä kehittämisen suunnasta. Tietoturvapolitiikan on oltava suhteutettu organisaation liiketoiminnan laajuuteen ja sen tulisi olla organisaation yrityskulttuurin mukainen, helppolukuinen ja ylimmän johdon tukema. (SFS-ISO/IEC 27003:2017, 14.)

4.13 Tietoturva-auditointi

Tietoturva-auditointi (*security audit*) tarkoittaa järjestelmän sisältämien tietojen ja toimintojen suunniteltua riippumaton tarkastelua ja tutkintaa sen varmistamiseksi, ovatko tutkittavan järjestelmän tietoturvallisuuteen liittyvät toiminnot ja kontrollit riittäviä, noudatetaanko sovittuja tietoturvapolitiikkoja ja -menettelyjä ja onko tutkinnan kohteessa havaittavia turvallisuusrikkomuksia. Tietoturva-auditoinnin lopputuloksena on suositukset tarvittavista toimenpiteistä järjestelmän turvallisuustason parantamiseksi. (RFC 2828 2000, 150.)

4.14 Kyberturvallisuus ja tietoturvallisuus

Termien tietoturvallisuus ja kyberturvallisuus käytölle ei ole täysin vakiintunutta tapaa arkikielessä. Termejä saatetaan käyttää hyvinkin vapaasti toistensa synonyymeina, mutta niille löytyy kirjallisuudesta myös omat määritelmänsä.

Tietoturvallisuudella (*information security*) pyritään varmistamaan organisaation tietojen luottamuksellisuus eli suojaamaan tietojen paljastuminen oikeudettomille käyttäjille (*confidentiality*). Tietoturvallisuuden avulla suojataan myös tiedon eheyttä (*integrity*) estämällä tietoon kohdistuvat väärät muokkaukset. Lisäksi tietoturvallisuuden avulla varmistetaan tiedon saatavuus (availability) tai tarvittaessa rajoitetaan sitä. Kyberturvallisuus (*cybersecurity*) taas pyrkii suojaamaan turvattavaa tieto-omaisuutta torjumalla uhkia verkkopohjaisten tietojärjestelmien käsittelemää, tallentamaa tai siirtämää tietoa vastaan. (ISACA Glossary N.d.)

Tietoturvallisuuden ja kyberturvallisuuden erot ovat pääasiassa niiden erilaisessa lähestymistavassa. Tietoturvallisuus keskittyy tiedon luottamuksellisuuden, eheyden ja saatavuuden varmistamiseen tiedon muodosta riippumatta, oli se sitten sähköisessä, paperisessa tai jossain muussa muodossa. Kyberturvallisuus keskittyy huolehtimaan tietojärjestelmien saatavuudesta ja oikeasta toiminnasta sekä siitä, että niiden käsittelemään ja säilyttämään tietoon voi luottaa. (Akpeninor 2013, 126-127.)

4.15 Tietoturvallisuuden hallintajärjestelmä

Tietoturvallisuuden hallintajärjestelmä (*Information Security Management System*) pyrkii suojaamaan tiedon luottamuksellisuutta, eheyttä ja saatavuutta riskienhallinta-

prosessin avulla. Tietoturvallisuuden hallintajärjestelmän on tärkeää olla osa organisaation olemassa olevia prosesseja ja johtamisjärjestelmää. Hallintajärjestelmän käyttöönotto on organisaation strateginen päätös, jolloin sen toteutuksen on oltava organisaation tarpeiden ja tavoitteiden mukainen. Tietoturvallisuuden hallintajärjestelmän avulla voidaan pyrkiä vahvistamaan keskeisten sidosryhmien luottamusta siihen, että tietoturvariskejä hallitaan organisaatiossa asianmukaisesti liiketoiminnan laajuus huomioon ottaen. (ISO/IEC 27001:2017, 5.)

4.16 Kyberresilienssi

Resilienssi on järjestelmän tai verkon kyky vastustaa virhetilannetta tai toipua häiriöstä mahdollisimman nopeasti (ISACA Glossary N.d.) Valtionhallinnon VAHTI-ohjeistus määrittelee resilienssin sekä vastustuskykyisyytenä eli toimintakyvyn eri tilanteissa säilyttävänä että vikasietoisuutena eli toimintakykynsä vioista huolimatta ainakin osittain säilyttävänä. (Valtionhallinnon tietoturvasanasto 2008, 130-136.)

Kyberresilienssi on kyvykkyyttä ennakoida, kestää, palautua ja mukautua sellaisiin haitallisiin olosuhteisiin, häiriötilanteisiin, hyökkäyksiin ja järjestelmien tai niiden sisältämien tietojen vaarantumiseen, jotka kohdistuvat sähköisiin tai verkkopohjaisiin järjestelmiin tai niiden käsittelemään tietoon. Kyberresilienssiä voidaan tavoitella ja kehittää usealla tasolla järjestelmien komponenttitasosta organisaatioiden, johtamisjärjestelmien ja jopa valtiollisen yhteistyön tasolle. Kyberresilienssiä toteuttavissa järjestelmissä turvallisuuselementit ovat sisäänrakennettu osa järjestelmän arkkitehtuuria ja suunnittelua. Tämänkaltaiset järjestelmät kestävät hyvin kyberhyökkäyksiä, ovat vikasietoisia ja ne pystyvät toimimaan heikentyneessä toimintaympäristössä.

Riskienhallinnallisesta näkökulmasta kyberresilienssi vähentää sähköisiin ja verkottuneisiin järjestelmiin kohdistuvia operatiivisia, liiketoiminnallisia, organisatorisia ja toimialakohtaisia riskejä. (NIST Special Publication 800-160 2019, 1-2.)

4.17 Yhteenveto

Tietoturvallisuuteen liittyvien keskeisten käsitteiden ja aihealueiden kirjo on laaja. Tietoturvallisuuden hallintajärjestelmillä, viitekehyksillä ja hyvillä käytännöillä pyritään varmistamaan kaikkien tietoturvallisuuteen kuuluvien osa-alueiden huomioiminen tietoturvatyössä. Tietoturvallisuuden johtamisessa riskien hallinnalla ja siihen liittyvillä toimenpiteillä on suuri merkitys kokonaiskuvassa. Erilaisia malleja, standardeja ja viitekehyksiä on tarjolla runsaasti eri kokoisten ja eri toimialalla toimivien organisaatioiden käyttöön.

5 Strateginen johtaminen on tulevaisuuden muokkaamista

Yksi maailman vanhimmista organisaatioiden johtamisen käsitteistä on strategia, sillä strategiaa on sovellettu oppina sodan voittamisesta jo vuosituhansia sitten (Kamensky 2014, 13). Strategia-sanan alkuperä liittyy tähän sotaisaan historiaan, sillä kreikankielinen sana ”strategos” tarkoittaa sodan johtamisen taitoa (mts. 16).

Vuorinen (2013) kertoo, että strategia on pyrkimystä tehdä sellaisia päätöksiä, joiden avulla organisaatio voi saavuttaa menestystä tulevaisuudessa. Sen avulla pyritään valitsemaan tietoisesti tavoitteellisesti organisaation suunta muuttuva toimintaympäristö huomioiden. Hyvän strategian avulla organisaatio saa suunnan ja merkityksen

samalla, kun organisaation identiteetti vahvistuu ja työntekijöiden toiminta johdonmukaistuu. (Vuorinen 2013, 15.) Laaja-alaisena ja monitahoisena käsitteenä strategia muodostaa monipuolisen kehyksen organisaation, liiketoiminnan ja henkilöstön johtamiseen ja kehittämiseen (Kamensky 2014, 13).

Mckeownin (2015) mukaan strategialla pyritään muokkaamaan tulevaisuutta. Strategian avulla toivotut lopputulokset pyritään saavuttamaan käytettävissä olevilla keinoilla. Lisäksi Mckeowin mukaan strategiaa on pelkistetysti katsoen historian saatossa lähestytty kahdesta suunnasta: ihmiskeskeisesti (ns. luova lähestyminen) sekä analyyttisesti. Strategisesti ajatteleva henkilö joutuu tasapainottelemaan tarpeen mukaan näiden kahden lähestymistavan välillä. (Mckeown 2015, What is Strategy.)

Hyvän strategian tunnusmerkki on yksinkertaisuus ja joka määrittelee muutaman selkeän kehittämisen kohteen. Selkeän strategian aikaansaaminen edellyttää organisaation nykytilan selvittämistä ja toimintaympäristön määrittämistä. Strategian määrittelyn onnistuminen edellyttää lähtötilanteen selkeää täsmentämistä. (Lindroos & Lohivesi 2004, 44.)

5.1 Tarkoitus

Tarkoituksen avulla organisaatio viestii siitä, mitä hyvää se tekee ja mikä on sen toiminnan tarkoitus. Tarkoituksen avulla yritys viestii erityisesti 1990-luvun jälkeen syntyneille tarkoitussukupolven edustajille, joille pelkkä rahan ansaitseminen ei ole kaikki kaikessa, että heidän työnsä on merkityksellistä. Vain aito ja uskottava tarkoitus motivoi henkilöstöä halutulla tavalla. Tarkoituksen määrittelyllä vaikuttaa tutkimusten mukaan olevan vaikutusta kannattavuuteen sekä brändin luotettavuuteen. (Mitronen & Raikaslehto 2019, 131.)

5.2 Missio

Perustehtävä (eli missio tai toiminta-ajatus) täsmentää organisaation keskeisen olemassaolon oikeutuksen. Mission avulla organisaatio voi kohdistaa toimintaansa ja luoda tarvittavia toimintaedellytyksiä tavoitteidensa saavuttamiseksi. (Lindroos & Lohivesi 2004, 20-21.)

Hyvä toiminta-ajatus on kaiken toiminnan perusta ja niin vahva, että se pystyy ohjaamaan organisaation toimintaa. Toiminta-ajatuksen määrittelyssä tulee ottaa huomioon sen laajuus tai rajaukset, valittu näkökulma, keskeiset sidosryhmät sekä tunteen tuominen järjen rinnalle. Organisaation koko henkilöstön tulee tuntea, ymmärtää ja sisäistää organisaation missio. (Kamensky 2014, 69-71.)

5.3 Visio

Visio on kurkistus tulevaisuuteen, sillä se tarjoaa näkemyksen organisaation tulevaisuudesta (Lindroos & Lohivesi 2004, 26). Vision on toivottava tulevaisuudenkuva ja se voi ohjata löytämään mahdollisia reittejä haluttuun tulevaisuuteen. Samalla visio voi kertoa yrityksen omasta tahtotilasta eli siitä mitä se haluaisi tulevaisuudessa olla. (Mitronen & Raikaslehto 2019, 132).

Visiolla siis tarkoittaa organisaation julkilausuttua ajatusta siitä, millaiseksi se haluaa tietyn ajanjakson aikana kehittyä. Hyvä visio innostaa organisaation omaa henkilöstöä, on asiakkaille toimiva ja se on mitattavissa uskottavasti. Visiota luodessa tulee varoa tekemästä siitä sisällöltään latteata ja tyhjää, sillä silloin visio ei innosta ketään. Tehokkaan vision on yleensä syytä olla nykytilasta poikkeava ja sen tarkoituksena on saada aikaiseksi innostusta organisaation tulevaisuudesta. Hyvä vision toimii kuin

haastava tavoite, joka on koko henkilökuntaa yhdistävä tekijä. (Lindroos & Lohivesi 2004, 26-27.)

Hyvä visio selkeyttää ja rajaa laajan valintojen joukon yhdeksi yhteiseksi tavoitteeksi. Se saa ihmiset liikkeelle ja motivoitumaan samalla, kun se ohjaa toimintaa yhteiseen suuntaan siten, ettei jokaisesta pienestä asiasta tarvitse keskustella ja päättää erikseen. (Vuorinen 2013, 141.)

5.4 Arvot

Arvot ovat organisaation toimintaa ohjaavia periaatteita. Arvot pyritään määrittelemään niin, että ovat riippumattomia ajasta ja paikasta. Julkilausuttujen arvojen avulla organisaatio pyrkii ilmaisemaan tai ohjaamaan omaa yrityskulttuuriaan. Koko organisaation tulee omaksua ja sisäistää arvot ja kyetä soveltamaan niitä myös omassa päivittäisessä työssään. (Kamensky 2014, 76-77.)

Arvot ovat organisaation eettinen perusta ja niillä on ihmisten toimintaa ohjaava ja yhtenäistävä merkitys (Viitala & Jylhä 2019, 65).

5.5 Strateginen johtaminen

Visiossa täsmentyneet organisaation päämäärät voidaan pyrkiä saavuttamaan strategian ja strategianprosessin avulla. Strategia siis antaa keinot vision toteuttamiseksi. Strategiaan sisältyvät pohdinnat, johtopäätökset, valinnat ja toimenpiteet eli pohjimmiltaan strategiassa on kyse organisaation toimintaan liittyvien innovaatioiden tekemisestä. Strategian avulla organisaatio pyrkii löytämään uusia toimintamalleja ja ide-

oita asiakkaiden tai sidosryhmien tarpeiden tyydyttämiseksi eli lisäarvon tuottamiseksi organisaation oman perustehtävän mukaisesti. Organisaatiossa ei ole välttämättä vain yhtä strategiaa vaan sitä voidaan tehdä useilla eri tasoilla. Strategia kertoo omalle organisaatiolle, miten sen tulee toimia, jolloin strategia ei voi olla sisällöltään salainen. Oman organisaation lisäksi myös keskeisten sidosryhmien tulisi olla selvillä siitä mitä strategia heiltä edellyttää. (Lindroos & Lohivesi 2004, 27-29.)

Strategia kertoo miten kohti visiota tai tavoitteita päästään (Mitronen & Raikaslehto 2019, 130). Visio ja strategia ovat johtamisen työkaluja ja niiden avulla pyritään saamaan aikaa näkemyksiä, linjauksia, päätöksiä ja toimenpiteitä (Lindroos & Lohivesi 2004, 30).

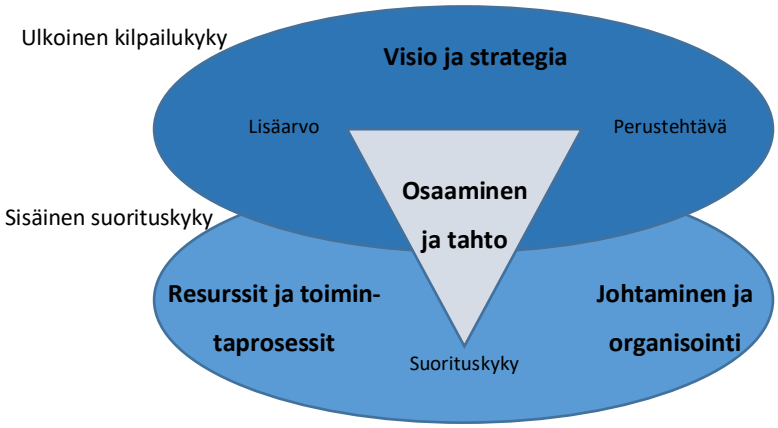
Vuorinen (2013) määrittelee strategisen johtamisen toiminnaksi, jonka tarkoituksena on pitkän aikavälin menestyksen mahdollistaminen. Hän tekee eron operatiivisen johtamisen ja strategisen johtamisen välille juuri tarkastelujakson avulla. Operatiivinen johtaminen tarkastelee asioita lyhyellä aikavälillä (tämä päivä, huominen, ensi viikko) kun taas strateginen johtaminen tarkastelee asioita seuraavien kuukausien, vuosien tai jopa vuosikymmenten tasolla. (Vuorinen 2013, 15).

Kuvio 11. Tarkoitus, visio, toiminta-ajatus, strategia ja arvot - keinoja toiminnan suuntaamiseen (Mitronen & Raikaslehto 2019, 130)

Vuorisen määrittelemää pitkän aikavälin menestystä voi lähteä etsimään Mckeown (2015) esittämien kysymysten kautta, joiden avulla haarukoidaan strategian tavoitteita. Näistä kysymyksistä kaksi ensimmäistä ovat analyyttisiä (Mitä organisaatio tekee tällä hetkellä? Miten organisaatio asemoituu kilpailijoihin nähden?) ja kaksi jälkimmäistä ovat luovuutta ruokkivia (Mitä organisaatio haluaa saavuttaa? Kuinka voidaan luoda jotain, mitä asiakkaat haluavat?). (Mckeown 2015, What is Strategy.)

Organisaation strategisessa päätöksenteossa on laitettava aina ulkoinen kilpailukyky ja sisäinen suorituskyky kaikkien muiden asioiden edelle. Ulkoinen kilpailukyky määrittelee, miten organisaatio asemoituu ympäröivään yhteiskuntaan. Tähän asemointiin vaikuttaa organisaation kyky tuottaa ulkopuolisille sidosryhmille hyötyä sekä se, miten organisaatio vastaa sille asetettuihin yhteiskunnallisiin perustehtävän mukaisiin haasteisiin. Tuottaakseen tehokkaasti hyötyä sidosryhmilleen, organisaation on

oltava sisäisesti suorituskykyinen eli kyettävä tuottamaan palveluita ja tuotteita edullisemmin kuin mitä esimerkiksi asiakkaat ovat niistä valmiit maksamaan. Yritysten tulee olla niin suorituskykyisiä, että ne pystyvät tuottamaan ylijäämää eli tekemän voittoa. Yrityksen johto on epäonnistunut, ellei yritys tuota taloudellista tulosta ja ellei se pysty myymään tuotteitaan tai palveluitaan asiakkaiden maksuvalmiuden kanssa kohtaavaan hintaan. (Lindroos & Lohivesi 2004, 20-21.)



Kuvio 12. Yrityksen ydinhaasteet ja keinot haasteisiin vastaamiseksi (mukaillen Lindroos & Lohivesi 2004, 25).

Kuviossa 9 on kuvattua yrityksen ulkoiseen kilpailukykyyn (lisäarvo, ja perustehtävä) ja sisäiseen suorituskykyyn (tehokas ja kannattava eli suorituskykyinen toiminta) liittyvät ydinhaasteet sekä mahdolliset keinot näiden haasteiden ratkaisemiseksi.

Ulkoisen kilpailukyvyn näkökulmasta visio ja strategia tulee kiteyttää niin, että ne vastaavat asiakaslisäarvon ja yhteiskunnallisen perustehtävän haasteisiin. Sisäisen

suorituskyvyn osalta kyse on vision mukaisen strategian käytännön toteutuksesta. Tällä tarkoitetaan johtamista ja organisoitumista sekä olemassa olevien resurssien ja prosessien hyödyntämistä. Osaamista ja tahtoa tarvitaan sekä ulkoiseen kilpailukykyyn että sisäiseen suorituskykyyn liittyviin haasteisiin vastattaessa. (Lindroos & Lohivesi 2004, 24-25.)

5.6 Strategiaprosessi

Strategiatyön tueksi on olemassa joukko työkaluja ja prosesseja mutta Mckeown (2015) korostaa strategin roolia strategiatyön onnistumisessa. Strategin tehtävänä on saada ihmiset välittämään siitä mitä ollaan tekemässä ja miksi. Strategi laittaa liikkeelle tarvittavan tapahtumaketjun tulevaisuuden muokkaamiseksi. (Mckeown 2015, osa 1.)

Kamensky (2014) varoittaa kiinnittämästä liikaa huomiota pelkästään strategian sisältöön ja hän korostaa strategiaprosessin olevan yhtä tärkeä sisällön kanssa. Hänen mukaansa prosessi vaikuttaa ratkaisevasti strategia sisällön laatuun, strategiatyöskentelyn tuottavuuteen, strategien toteutumiseen ja strategian uudistamiseen. (Kamensky 2014, 15.)

Strategiaprosessin avulla pyritään löytämään vastaukset pysyvien ydinhaasteiden ratkaisuun. Strategiaprosessin vaiheita ovat vastausten etsiminen, suunnittelu, päätöksenteko ja toimeenpano. Osana strategiaprosessia tulee pystyä tekemään valintoja ja päätöksiä esimerkiksi (Lindroos & Lohivesi 2004, 24):

1) visioista ja strategiasta (eli toimintalinjoista)
2) johtamisesta ja organisoinnista (eli ohjauksesta ja puitteista)
3) resursseista ja toimintaprosesseista (eli edellytyksistä)

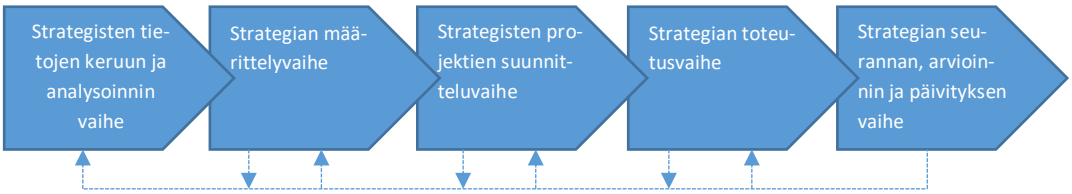
4) osaamisesta ja tahdosta (eli taidoista ja haluista)

Strategiaprosessi voidaan nähdä joko perinteisenä lineaarisena prosessina, jossa eri vaiheet seuraavat toisiaan tai nykyaikaisena jatkuvana prosessina, jossa on tietyt määritellyt vaiheet mutta ne eivät seuraa toisiaan missään kronologisessa järjestyksessä (Vuorinen 2013, 41-42).

Mitrosen ja Raikaslehdon mukaan Henry Mintzberg on määritellyt neljä organisaation toimintatapaan sidottua strategiaprosessia (Mitronen & Raikaslehto 2019, 121-122):

1) Strateginen suunnittelu, jossa vakaassa ja muuttumattomassa toimintaympäristössä tehdään systemaattista suunnittelua ja tulevaisuuden ennakointi koetaan mahdolliseksi
2) Strateginen visiointi, jossa tehdään systemaattista suunnittelua muuttuvassa ympäristössä siten, että strategia on sidottu ennemmin visioon kuin ennakoitavaan tulevaisuuteen
3) Strategiset hankkeet, jossa strategisen suunnan määrittely on joustavaa ja perustoimintaympäristön oletetaan pysyvän suhteellisen muuttumattomana
4) Strateginen oppiminen, jossa tehdään kokeiluja dynaamisessa toimintaympäristössä uusien liiketoiminnan löytämiseksi

Lindroos ja Lohivesi (2004) määrittelevät strategiaprosessille viisi selkeää vaihetta, joiden avulla strategia luodaan. Prosessin ensimmäisessä vaiheessa tehdään arvio siitä mihin suuntaan liiketoimintaympäristö kehittyy, jonka jälkeen luodaan visio tulevan toiminnan päämääristä. Tämän jälkeen täsmennetään millä keinoilla asetetut päämäärät voidaan yrittää saavuttaa. Toteutusvaiheessa valitaan tarvittavat resurssit ja kehityshankkeet strategian toteutuksen tueksi. (Lindroos & Lohivesi 2004, 32.)



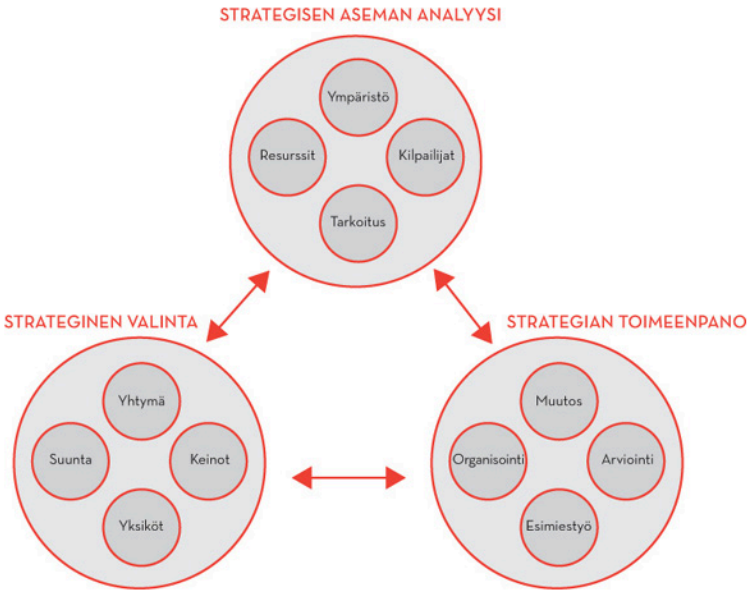
Kuvio 13. Strategiaprosessin viisi keskeistä työvaihetta (Lindroos & Lohivesi 2004, 31).

Kuviossa 4 on näkyvissä Lindroosin ja Lohiveden esittelemän prosessin vaiheet. Yleensä vaiheet käydään läpi kuvion mukaisessa järjestyksessä mutta prosessia voi noudattaa myös iteratiivisen mallin mukaisesti, jolloin myöhemmissä vaiheissa on mahdollista palata tekemään tarkennuksia aiempiin vaiheisiin. (Lindroos & Lohivesi 2004, 32.)

Vuorinen (2013, 40) esittelee myös kuviossa 4 esitetyn lineaarisen prosessin ja toteaa sen kattavan kaikki strategiatyön olennaiset aihealueet. Hän mainitsee prosessin lähteenä Näsin & Aunolan (2002). (Vuorinen 2013, 41.)

Lineaarisen prosessin vastakohtana voidaan pitää jatkuvaa strategisen johtamisen prosessia, josta voidaan tunnistaa kolme keskeistä vaihetta (Vuorinen 2013, 42-43):

- Strategisen aseman analyysi
  - Analyysejä organisaation olemassaolon tarkoituksesta, tahtotilasta, toimintaympäristöstä, kilpailijoista ja omista resursseista
- Strateginen valinta
  - Eri vaihtoehtojen tunnistaminen, arviointi ja valinta
- Strategian toimeenpano
  - Valittujen asioiden toteuttaminen käytännössä



Kuvio 14. Jatkuva strategiaprosessi (Vuorinen 2013, 44)

Mckeown (2015) painottaa strategiatyön alkuvaiheessa tapahtuvaa puntarointia analyyttisen ja luovan lähestymistavan välillä. Valinnan tulisi olla tietoinen ja linjassa organisaation muun toiminnan kanssa. (Mckeown 2015, What is Strategy).

Mckeown (2015) puhuu myös tulevaisuuden muokkaamisesta ja että sen saavuttaminen vaatii ajattelua, suunnittelua ja reagointia. Hän esittää neljä keskeistä kysymystä strategiatyön alkuunsaamiseksi (Mckeown 2015, Osa 1):

- Mitä organisaatio haluaa tehdä?
- Minkä kuvittelemme olevan mahdollista?
- Mitä tulee tehdä tavoitteiden saavuttamiseksi?

- Milloin tulee reagoida uusiin mahdollisuuksiin ja muokata suunnitelmia?

”Strategiaprosessin onnistumisen tärkeimpiä seikkoja on, että kyetään luomaan yhteinen näkemys ja tahto siitä, millaiseksi halutaan tulla” (Lindroos & Lohivesi 2004, 43).

Seuraavissa kappaleissa lähestytään strategiaprosessia aiemmin esitetyn viisiosaisen lineaarisen prosessin näkökulmasta, sillä se kattaa kaikki strategiatyön olennaiset aihealueet ja jotka ovat myös sovellettavissa jatkuvan strategisen prosessin johtamisessa.

5.7 Strategisten tietojen keruun ja analysoinnin vaihe

Strategisten tietojen keruun ja analysoinnin vaiheeseen kuuluvat analyysit toimintaympäristöstä, markkinoista ja kilpailijoista, sidosryhmistä sekä oman organisaation toiminnasta. Näillä analyyseillä pyritään kasvattamaan ymmärrystä liiketoimintaympäristön muutoksista, sidosryhmien odotuksista, organisaation sisäisen toiminnan tilasta ja markkinoiden kehittymisestä. (Lindroos & Lohivesi 2004, 32-42.)

Tietojen keruun ja analysointivaiheen aikana voidaan hyödyntää useita analysointimenetelmiä, joista muutamia on esiteltynä liitteenä (Liite 1).

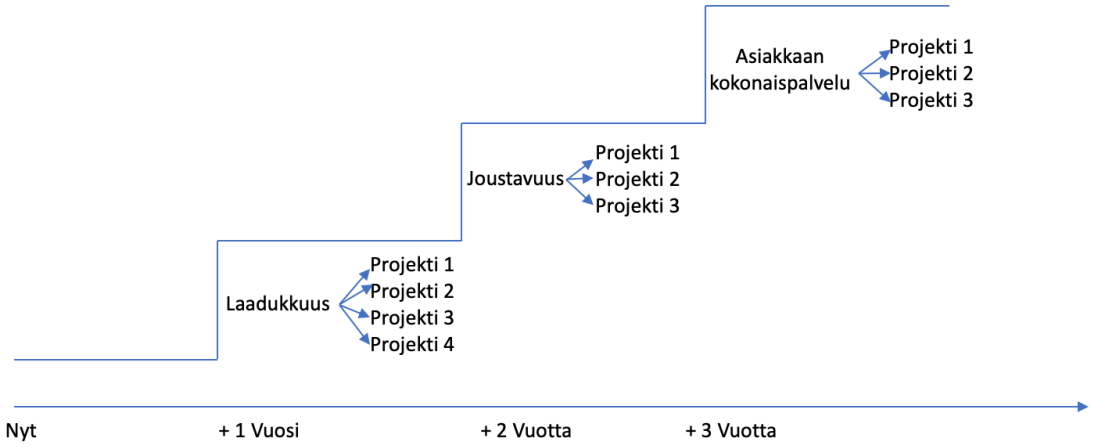
5.8 Strategian määrittelyvaihe

Analysointivaiheen lopputuloksena muodostuu kokonaisnäkemys toimintaympäristöstä, johon strategiaa ollaan tekemässä ja jonka jälkeen tehdään päätökset siitä, millaisia päämääriä organisaation toiminnalle asetetaan strategian toteutusjakson ajaksi. Määrittelyvaiheen alussa on tärkeää määritellä organisaation mission pohjalta realistinen mutta haastava visio strategiatyön pohjaksi. Missio ja visio toimivat perustana, jonka päälle linjaukset eli strategia voidaan rakentaa. Vision pohjalta määritellään konkreettiset ja riittävän haastavat tavoitteet, jotka halutaan saavuttaa strategiajakson aikana. Ylätason tavoitteiden lisäksi tulee asettaa mitattavissa olevia osatavoitteita, joilla varmistetaan ideoiden jalostuminen toteutukseksi. Strategian dokumentaatiossa tulee ottaa kantaa siihen, mitä tulee tehdä, jotta vision mukainen tahtotila voidaan käytännössä saavuttaa. Strategiatyön tarkoitus on miettiä vaihtoehtoja siitä, mitä voitaisiin tehdä ja tehdä päätöksiä siitä, mitä lopulta tehdään ja mitä ei tehdä. Lopuksi päätetään myös miten asetetut päämäärät ja tavoitteet tullaan saavuttamaan. Strategian määrittelyvaiheen tuloksena on dokumentaatio, josta käy ilmi päätökset vision avulla asetetuista päämääristä sekä valitut keinot päämäärien toteuttamiseksi. (Lindroos & Lohivesi 2004, 43-44.)

5.9 Strategisten projektien suunnitteluvaihe

Strategiaprosessin toteutusvaihe voi alkaa, kun strategian toteuttamisessa käytettävät keskeiset kehitysprojektit on määritelty ja kirjattu. Näitä kehitysprojekteja tehdään koko strategiakauden ajan ja niistä ensimmäisten on syytä käynnistyä mahdollisimman aikaisessa vaiheessa. Osa kehitysprojekteista voi olla niin pitkiä, että ne voivat jatkua myös tulevien strategiajaksojen aikana. Kehitysprojektien riippuvuutta toi-

siinsa voidaan kuvata kehitysportaiden avulla. Tällöin projektien keskinäinen toteutusjärjestys on paremmin hahmotettavissa ja voidaan helpommin hahmottaa, miten kokonaisuus rakentuu aiempien projektien varaan. Kehitysportaat voi teemoittaa esim. vuosittain, jolla edelleen selkeytetään mikä teema on kyseisenä vuonna erityisesti kehittämisen kohteena (Lindroos & Lohivesi 2004, 46.)



Kuvio 15. Esimerkki strategisista kehitysportaista (Lindroos & Lohivesi 2004, 47)

5.10 Strategian toteutusvaihe

Toteutusvaihe on jatkuva ja läpi koko strategiajakson käynnissä oleva prosessi, jonka aikana strategia toteutetaan vuosittaisia toimintasuunnitelmia hyödyntäen. Toimintasuunnitelma on tarkka kuvaus kulloisenkin vuoden tavoitteista ja keinoista asetettujen tavoitteiden saavuttamiseksi. Analyysi- ja suunnitteluvaiheisiin verrattuna toteutusvaihe on resurssi-intensiivisempi. Organisaation johto on merkittävässä ase-

massa strategian toteutusvaiheessa, sillä strategiaa toteutetaan jokapäiväisen toiminnan kautta ja toteutuksen onnistuminen vaatii johdolta strategian mukaista johtamista. Strategian johtaminen on toiminnan johtamista, jolloin epäonnistuminen strategian toteuttamisessa on johtamiseen liittyvä ongelma. (Lindroos & Lohivesi 2004, 47-48.)

5.11 Strategian seurannan, arvioinnin ja päivityksen vaihe

Toimintaympäristössä tapahtuu strategiajakson aikana myös muutoksia, joihin ei ole voitu strategiassa ennakolta varautua. Tästä johtuen on säännöllisesti arvioitava ovatko aiemmin tehdyt linjaukset vielä voimassa ja voidaanko niiden mukaisesti vielä jatkaa. Tarvittaessa aiemmin tehtyihin linjauksiin on tehtävä muutoksia. Menestyvä organisaatio ei ole muita parempi ennustamaan tulevaisuutta, vaan se pystyy reagoimaan muutoksiin muita organisaatioita nopeammin ja täsmällisemmin. (Lindroos & Lohivesi 2004, 48.)

Strategiatyön lopputuloksen dokumentoinnilla on suuri merkitys strategian jalkautuksessa ja toteutuksessa. Pelkkään strategiadokumentaation laatuun keskittyminen ei riitä, vaan myös henkilöstö- ja sidosryhmäviestinnän suunnitteluun ja laatuun tulee paneutua huolella. Jos henkilöstö ei tunne strategian keskeisiä kohtia, ei se myöskään voi toimia henkilöstön toiminnan ohjausvälineenä. (Mts. 53.)

Toimintaympäristössä tapahtuvat muutokset eivät ole vain uhkia, vaan ne ovat myös mahdollisuuksia organisaatiolle, sillä muutos tarkoittaa vallalla olevan toimintatavan päättymistä ja samalla myös uuden tavan alkua. Strategian laadinnassa olisi siksi syytä varautua sekä pieniin muutoksiin että suuriin murroksiin. (Mts. 56.)

5.12 Yhteenveto

Strategiseen johtamiseen ja strategiaprosessiin liittyvää tutkimusta ja kirjallisuutta on tarjolla runsaasti. Strategiaprosessia voidaan tarkastella lineaarisena prosessina tai se voidaan nähdä uudemman tutkimuksen mukaisesti jatkuvana prosessina. Keskeisiä teemoja strategian luomisessa ovat nykytilan ja toimintaympäristöjen (sisäinen ja ulkoinen) analysointi, keskeisten sidosryhmien tunnistaminen, tavoite- ja tahtotilan määrittäminen, organisaation olemassa olon perustelun kiteyttäminen, tavoitteiden asettaminen, toteutusprojektien suunnittelu, aikataulutus ja resursointi sekä toteutuksen aikainen seuranta ja muutostarpeiden tunnistaminen. Strategisella johtamisella pyritään vastaamaan noin 3-5 vuoden aikajänteellä tapahtuvaan muutokseen.

6 Tietoturvallisuutta tulee johtaa myös strategisella tasolla

Tässä luvussa tarkastellaan tietoturvallisuuden strategisen johtamisen teoreettista viitekehystä aiemmin kappaleessa 5.6 esitetyn viisiosaisen strategiaprosessin mukaisesti.

Tietoturvallisuuden johtamista ohjaavista viitekehyksistä on löydettävissä tarve tietoturvallisuuden strategiselle johtamiselle. ISO/IEC 27003 ohjeistaa ISO/IEC 27001-standardin mukaisen tietoturvallisuuden hallintajärjestelmän toteuttamista. Ohjeistuksen kappale 5 käsittelee johtajuutta ja johdon sitoutumista tietoturvallisuuden hallintajärjestelmää kohtaan. Ohjeistuksen mukaan johtajuutta tulee osoittaa varmis-

tamalla, että organisaatiolle luodaan tietoturvapolitiikka ja tietoturvallisuuden tavoitteet määritellään ja että ne ovat linjassa organisaation strategian kanssa. (ISO/IEC 27003:2017, 12.)

Information Security Forumin julkaisema The Standard of Good Practice listaa yhtenä tietoturvallisuuden hallintamallin peruskomponenttina tietoturvastrategian. Sen mukaan tietoturvastrategian tulisi olla todistettavasti integroitu organisaation strategisiin tavoitteisiin. Lisäksi se asettaa tietoturvastrategian tavoitteeksi sen varmistamisen, että tietoturvan kehitysohjelmat ja -projektit edistävät organisaation menestymistä. (Information Security Forum 2018, 22). The Standard of Good Practice listaa yhteensä 11 suoraa vaatimusta tietoturvastrategian toteuttamiselle (Information Security Forum 2018, 22-24).

VAHTI-ohjeen 2/2010 liitteessä 5 määritellään tietoturvallisuuden johtamiselle asetettuja vaatimuksia ja vaatimuksissa katetaan myös tietoturvallisuuden johtamisen strateginen taso. Perustason vaatimuksiksi ohje esittelee lainsäädännön kautta tulevien vaatimusten tunnistamisen, organisaation ydintoimintojen ja -prosessien tunnistamisen ja tietoturvapolitiikan luomisen. Korotetulla tasolla ohjeen mukaan tulee olla kirjallinen strategiatason suunnitelma tietoturvatyön vastuuttamiseksi ja organisoimiseksi ydintavoitteiden saavuttamiseksi. Korkean tason lisävaatimuksina ohje määrittelee vuosittaiset tietoturvallisuuden kehittämissuunnitelmat ja tietoturvallisuuden huomioimisen tulosohjauksessa. (Valtionhallinnon tietoturvallisuuden johtoryhmä 2010, 96.)

Tietoturvallisuus voi olla myös tuotuna mukaan yrityksen liiketoimintastrategiaan. Paavo Porvari kuvaa väitöskirjansa johdannossa (2012) yrityksen liiketoimintaan kytkettyjen tietovoimavarojen ja tuotantotekijöiden turvaamisen merkitystä. Porvarin

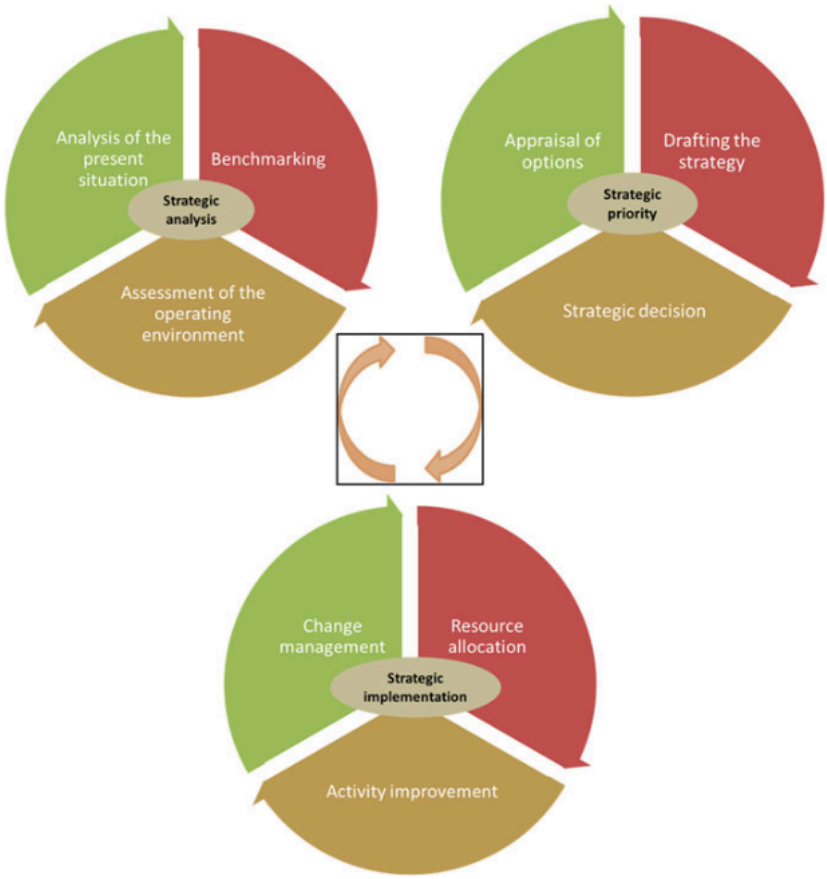
mukaan Saarenpää ja muut (1997) painottavat tiedon merkitystä yhteiskunnan ja sen osatekijöiden strategisena voimavarana. Lisäksi Porvarin mukaan Wood (1990) ehdottaa korkean tietoturvallisuuden tason ottamista yhdeksi yrityksen strategiseksi tulokulmaksi. (Porvari 2012, 3.)

Porvarin (2012) mukaan Johnston ja Hale (2009) ovat tutkineet tietoturvallisuuden huomioimista organisaation strategisessa suunnittelussa ja sen vaikutusta tietoturvallisuusohjelmien laatuun. Yrityksen periaatteet ja menettelytavat sisältyvät todennäköisemmin päämääriin ja tavoitteisiin, kun tietoturvallisuus liitetään osaksi strategista suunnittelua. (Mts. 76.)

Porvarin (2012) mukaan White (2009) on määritellyt tietoturvallisuuden hallintamallissa strategisen johtamisen siten, että se vastaa kysymykseen miksi yrityksellä on tietoturvallisuusongelmia? Kysymykseen vastaaminen johtaa tietoturvapolitiikan määrittelemiseen ja siinä tulisi ottaa huomioon sekä ulkoiset että sisäiset sidosryhmät että näihin liittyvät riskiarvioinnit. Strategisen johtamisen fokus tulisi olla toiminnallisuudessa sekä merkittävissä kaikkia sidosryhmiä koskevissa aihealueissa. Sisäisten ja ulkoisten sidosryhmien lisäksi tulisi tarkastella sisäistä ja ulkoista toimintaympäristöä, kuten lakeja, sääntelyä, eettisiä periaatteita ja yhteiskunnallisia tarpeita. Myös pehmeisiin arvoihin, kuten viestintään, ihmisten väliseen kanssakäymiseen ja henkilöstön johtamiseen tulee kiinnittää huomiota. Strategisella johtamisella voidaan saada aikaan kilpailuetua, parempi ymmärrys yrityksen hallitustasolla tietoturvallisuuteen liittyvistä huolista ja riskeistä sekä luottamusta liikekumppaneiden sekä asiakkaiden keskuudessa. (Mts. 79.)

Sillanpää ja muut esittelevät artikkelissaan ”Finnish Cyber Security Strategy and Implementation” geneerisen kyberstrategiaprosessin. Vaikka kyseinen prosessi on luotu

kansallisen kyberstrategian kehittämisen näkökulmasta, on siinä esitellyt komponentit yleiskäyttöisiä ja siten myös organisaatioiden hyödynnettävissä. Heidän esittämässään mallissa strategiaprosessi on jatkuva prosessi, joka on jaettu kolmeen alaprosessiin: strategiseen analyysiin, strategiseen painopisteeseen ja strategian toteutukseen. Nämä kolme päätasoa jakaantuvat kukin vielä kolmeen aliprosessiin kuvion 16 mukaisesti. Kyseiset aliprosessit seuraavat aiemmin esiteltyjä strategiaprosessin vaiheita ja ne kattavat kaikki keskeiset strategiaprosessin osa-alueet toimintaympäristöjen analyysistä strategian toteutuksen seurantaan ja jatkuvaan parantamiseen. (Sillanpää ja muut 2015, 140.)



Kuvio 16. The cyber strategy process (Sillanpää ym. 2015, 140)

Seuraavissa kappaleissa käsitellään tarkemmin keskeisten tietoturvallisuuden viitekehysten strategiaprosessin eri vaiheisiin liittyviä linjauksia ja suosituksia.

6.1 Tietoturvastrategian tietojen keräämisen ja analysoinnin vaihe

ISO/IEC 27003 ohjeistus korostaa tietoturvallisuuden hallintajärjestelmän toteuttamisessa seuraavien vaiheiden merkitystä (ISO/IEC 27003:2017, 5):

- Organisaation tarpeiden ymmärtäminen sekä tietoturvapolitiikan ja tietoturvatavoitteiden laatimisen välttämättömyyden ymmärtäminen
- Tietoturvaan liittyvien riskien arviointi
- Tietoturvaprosessien ja -hallintakeinojen sekä muiden riskinhallintakeinojen toteutus ja käyttö
- Tietoturvallisuuden hallintajärjestelmän seuranta ja sen suorituskyvyn ja vaikuttavuuden katselmointi
- Jatkuva parantaminen

Näistä organisaation ja sen toimintaympäristön ymmärtämisen voi nähdä kuuluvan strategisen tietojen keräämisen ja analysoinnin vaiheeseen. ISO/IEC 27003 ohjeistaa organisaatiota määrittämään sellaiset sisäiset ja ulkoiset seikat, joilla voi olla vaikutusta organisaation toimintaan tai tietoturvallisuuden hallintajärjestelmältä odotettuihin tuloksiin. Ohjeistus määrittelee hallintajärjestelmän toimintona, jonka avulla organisaatio analysoi koko ajan itseään ja toimintaympäristöään. Näiden sisäisten ja ulkoisten asioiden analyysien tulisi olla jatkuvia ja niiden avulla on tarkoitus ymmärtää toimintaympäristöä, tunnistaa riskejä sekä mahdollisuuksia ja pyrkiä reagoimaan sisäisen sekä ulkoisen ympäristön muutoksiin. Ulkoisiksi asioiksi luetaan sellaiset

asiat, joita organisaatio ei voi itse hallita ja joista seuraa vaikutuksia tietoturvallisuuden toteuttamiseen sekä siihen, miten tietoturvallisuutta voidaan hallita. Ulkoisen ympäristön analysointiin kuuluu muun muassa seuraavat osa-alueet (ISO/IEC 27003:2017, 7-8):

- Yhteiskunnalliset ja kulttuuriset osa-alueet
- Poliittiset, oikeudelliset, normatiiviset ja säännellyt osa-alueet
- Taloudelliset ja makroekonomiset osa-alueet
- Teknologiset osa-alueet
- Luontoon liittyvät osa-alueet
- Kilpailulliset osa-alueet

ISO/IEC 27003 mukaan organisaation tietoturvallisuuteen tai sen hallintaan vaikuttavia ulkoiset tai sisäiset tekijät riippuvat organisaation omasta tilanteesta, toimintaympäristöstä ja prioriteeteista. Tällaisia ulkoisia tekijöitä voivat olla mm. luonnon katastrofit, salaustekniikoiden kehittyminen ja organisaation tarjoamien palveluiden kysyntä. Sisäisiä tekijöitä voivat olla mm. organisaation kulttuuri, hallintotapa, organisaatiorakenne, roolit ja vastuut sekä toimintaperiaatteet, tavoitteet ja niiden saavuttamisessa tarvittavat liiketoimintastrategiat. ISO/IEC 27003 ohjeistaa katselmoimaan sekä organisaation ulkoisen ympäristön olennaisten ulkoisten tekijöiden tunnistamiseksi että myös sisäiset osa-alueet olennaisten sisäisten tekijöiden tunnistamiseksi. Ohjeistus pyrkii näin varmistamaan organisaation tarkoituksen (toiminta-ajatus tai liiketoimintasuunnitelman) ymmärtämisen ja huomioon ottamisen. Ohjeistus kehottaa pohtimaan miten ulkoisen ympäristön osa-alueet ja niistä seuraavat tekijät voivat vaikuttaa tietoturvatavoitteisiin. (SFS-ISO/IEC 27003:2017, 8.)

The cyber strategy process -mallin mukaisessa strategisen analyysin vaiheessa tulee tunnistaa nykytila ja organisaation toimintaympäristö. Nykytila-arvio ottaa muun muassa kantaa siihen, miten organisaatio on sijoittunut toimintaympäristöönsä. Kyberkontekstissa analyysivaiheessa on tärkeää pyrkiä havainnoimaan uhkamaisemaa, tunnistamaan ympärillä olevia haavoittuvuuksia ja arvioimaan näistä seurauksena olevia riskejä. Toimintaympäristön analyysilla pyritään identifioimaan kybertoimintaympäristön ilmiöitä, keräämään pohjatietoa strategiaa varten ja arvioimaan jo olemassa olevia projekteja ja suunnitelmia. Analyysivaiheessa voidaan käyttää benchmarking-menetelmää muissa organisaatioissa käytössä olevien parhaiden käytäntöjen tunnistamiseksi. (Sillanpää ym. 2015, 141.)

ISO/IEC 27003 ohjeistaa tunnistamaan tietoturvallisuuden hallintajärjestelmän kannalta olennaiset sidosryhmät ja niiden tarpeet sekä odotukset. Sidosryhmä on henkilö tai organisaatio, joka ”voi vaikuttaa johonkin päätökseen tai toimintoon tai johon jokin päätös tai toiminto voi vaikuttaa tai joka kokee olevansa jonkin päätöksen tai toiminnon vaikutuksen kohteena”. Sidosryhmät voivat olla sisäisiä tai ulkoisia ja niillä voi olla tietoturvaan liittyviä tarpeita, odotuksia tai vaatimuksia. Ulkoisia sidosryhmiä ovat esimerkiksi sääntelyviranomaiset, lainsäätäjät, osakkeenomistajat, toimittajat (alihankkijat, konsultit ja ulkoistuskumppanit), toimialajärjestöt, kilpailijat jne. Sisäisiä sidosryhmiä voivat olla esimerkiksi päätöksentekijät (mm. ylin johto), järjestelmien omistajat, tukitoiminnot, työntekijät, käyttäjät jne. Ohjeistuksen mukaan sisäiset ja ulkoiset sidosryhmät tulee tunnistaa samoin kuin näiden vaatimukset tietoturvatyöhön liittyen. Sidosryhmäanalyysit on ohjeistuksen mukaan säännöllisesti uusittava sidosryhmien tarpeiden, odotusten ja vaatimusten muuttuessa ajan kuluessa. (SFS-ISO/IEC 27003:2017, 9-10.)

6.2 Tietoturvastrategian määrittelyvaihe

Tietoturvastrategiassa tulee ilmaista, miten tietoturvallisuus linjataan organisaation keskeisten tavoitteiden kanssa, sen tulee olla sisällöltään riittävän ylätasoinen ja periaatteellinen, ylimmän johdon tukema ja hyväksymä sekä säännöllisesti katselmoitu. Lisäksi tietoturvastrategian tulee varmistaa organisaation kyky säilyttää valittu liiketoimintastrateginen suunta ympäröivän uhkamaiseman muutoksista huolimatta. Tietoturvastrategian tulee olla linjassa sekä liiketoiminta- että IT-strategioiden kanssa. Tällä pyritään varmistamaan organisaation tavoitteiden saavuttaminen ja päätöksentekijöiden yhteisymmärrys käytettävistä keinoista. Strategioiden integroinnilla pyritään ennakoimaan mahdollisia muutoksia sisäisessä ja ulkoisessa toimintaympäristössä. (Information Security Forum 2018, 22-23.)

Organisaation ylin johto on sitoutettava tietoturvatyöhön. Sen tulee ohjata ja tukea niitä henkilöitä, jotka ovat suoraan tekemisissä tietoturvan ja tietoturvallisuuden hallintajärjestelmän kanssa. Ylimmän johdon tulee antaa palautetta siitä, miten tietoturvallisuuden suunnitellut toiminnot ovat linjassa organisaation strategisten tarpeiden kanssa ja miten tietoturvallisuuden hallintajärjestelmän toimintoja priorisoidaan. (SFS-ISO/IEC 27003:2017, 13.)

Tietoturvatavoitteet tukevat organisaation strategisten tavoitteiden saavuttamisessa, joten organisaation tulee laatia ja asettaa tietoturvatavoitteet tarvittaville toiminnoille. Tavoitteiden asettamisessa tulee ottaa huomioon organisaatioon ja sen toimintaympäristöön sekä sidosryhmien tarpeisiin ja odotuksiin liittyvät analyysivaiheessa tunnistetut vaatimukset. Myös tietoturvallisuuden hallintajärjestelmän mukaisten riskien arviointien ja käsittelyn tuloksia tulee käyttää lähtötietoina tavoitteiden asettamisessa ja jatkuvassa katselmoinnissa. Tietoturvatavoitteiden tulee olla

tietoturvapolitiikan mukaisia ja niiden on oltava mahdollisuuksien mukaan mitattavissa. Tavoitteiden tulee olla linjassa tietoturvavaatimuksiin sekä riskien arviointiin ja käsittelyn tuloksiin. Tavoitteet tulee viestiä organisaatiolle ja ne tulee säilyttää dokumentoituina. (SFS-ISO/IEC 27003:2017, 25.)

Strategisen painopisteen suunnittelussa on kolme vaihetta, jotka ovat vaihtoehtojen arviointi, strategisten päätösten ja valintojen tekeminen sekä strategian laatiminen. Vaihtoehtojen arvioinnissa pyritään valitsemaan kullekin strategian osa-alueelle toimivimmat toimenpiteet. Eri vaihtoehtoihin liittyy erilaisia tunnistettuja uhkaskenaarioita, joihin jokaiseen pyritään löytämään sopiva ratkaisu. Vaiheen lopputulemana on käsitys toivotusta lopputulemasta ja sen toteuttamiseen tarvittavista resursseista. Strategisten päätöstenteon vaiheessa haluttu tavoitetila vahvistetaan ja samalla valitaan lopulliset keinot tavoitetilaan pääsemiseksi. Strategian laatimisen vaiheessa strategian rakenne ja formaatti kiinnitetään. Strategia saatetaan lopulliseen muotoonsa useamman iteratiivisen kehityskierroksen päätteeksi. (Sillanpää ym. 2015, 142.)

6.3 Strategisten projektien suunnitteluvaihe

Suunnitteluvaiheessa tulee huomioida esimerkiksi organisaation toimintaperiaatteet, tavoitteet ja strategia. Organisaation nykyisten toimintaperiaatteiden, tavoitteiden ja liiketoimintastrategian analyysi kertoo mitä organisaatio haluaa saavuttaa ja miten tietoturvatyön tavoitteet voidaan saada linjattua yhteen liiketoimintatavoitteiden kanssa siten, että varmistutaan yhteisten tulosten saavuttamisesta. (SFS-ISO/IEC 27003:2017, 9.)

Tietoturvastrategiasta tulee käydä ilmi millä tavoin se tukee organisaation keskeisiä tavoitteita. Strategian avulla tulee olla pääteltävissä, miten tietoturvatyö luo lisäarvoa organisaatiolle, mikä rooli tietoturvan kehitysprojekteilla on strategisessa mittakaavassa, mikä merkitys tietoturvalla on sääntelystä, toimintaympäristön muutoksista tai teknologian kehittymisestä seuraavien riskien hallinnassa. Lisäksi strategiassa tulee huomioida organisaation riskinottohalukkuus ja sääntelyn asettamat vaatimukset sekä varautuminen korkean vaikutustason poikkeamiin ja liiketoiminnan jatkuvuuden turvaaminen. Lisäksi tietoturvastrategian ja siihen liittyvien kehitysohjelmien pitää pystyä osoittamaan tietoturvahankintojen kohdalta sijoitetun pääoman tuotto. Tietoturvastrategian tulee korostaa tietoturvapoikkeuksien hallinnan merkitystä uhilta suojautumisessa. Projektien suunnitteluvaiheessa myös tulee varautua organisaation strategisten aloitteiden aiheuttamiin haitallisiin vaikutuksiin liiketoimintaa kohtaan. (Information Security Forum, 22.)

Suunnitteluvaiheessa organisaation tulee määrittää mitä tehdään, mitä resursseja tekeminen vaatii, kuka tai ketkä ovat vastuussa tekemisestä, missä aikataulussa työt tehdään ja kuinka tuloksia arvioidaan (SFS-ISO/IEC 27003:2017, 26).

Tietoturvatoiminnolla tulee olla tehtävä ja tavoite, jotka on huomioitava strategian rakentamisessa. Lisäksi strategian tulee sisältää mitattavissa olevat tavoitteet. Strategiassa tulee huomioida organisaation tietoturvatyön resursointi ja osaaminen sekä se miten tietoturvatyö organisaatiossa koetaan. (Information Security Forum 2018, 23.)

6.4 Tietoturvastrategian toteutusvaihe

Strategiasta tulee johtaa vuosittainen toimintasuunnitelma, jonka avulla voidaan seurata strategian etenemistä, pitää sidosryhmät tietoisina kulloisestakin tilanteesta ja varmistaa keskeisten projektien läpivienti. (Information Security Forum 2018, 23.)

Strategian toteutusvaiheessa tehdään muutoshallintaa, toiminnan kehittämistä ja resurssien kohdentamista. Muutoshallinnalla tarkoitetaan strategian toimeenpanovaiheen suoritusten mittaamista ja seurantaa toteutuksen onnistumisen todentamiseksi. Toteutusvaiheen edistymistä raportoidaan johdolle. Toiminnan kehittämisen osalta pyritään jatkuvan parantamisen mallin avulla tarkentamaan tarvittaessa suunnitelmia sekä varmistamaan kokonaiskuvan säilyminen. Resurssien oikea kohdentaminen pyrkii varmistamaan käytössä olevien varojen tehokkaan käytön ja on onnistuneen strategian toteutuksen keskeinen elementti. (Sillanpää ym. 2015, 142.)

Toteutusvaiheessa tulee myös panostaa viestintään ja muutosjohtamiseen. Tästä syystä tietoturvastrategian tulee rohkaista tiimirajat ylittävään yhteistyöhön ja ehkäistä siiloutumista organisaatiossa eri yksiköiden ja tiimien välillä. (Information Security Forum, 22.)

Sidosryhmät tulee pitää tietoisina tietoturvastrategian tuottamasta arvosta. Lisäarvoa sidosryhmille voi tuottaa esimerkiksi uskottavuutta parantavat nopeasti saavutettavissa olevat parannukset sekä pysyvän luottamuksen luominen osoittamalla tietoturvatoiminnon kyky toimittaa suunniteltuja ja sovittuja asioita. (Mts. 23).

6.5 Tietoturvastrategian seuranta, arviointi ja päivitys

Strategiajakson aikaiset muutokset organisaation kulttuurissa, arvoissa, hallintomallissa, liiketoimintaympäristössä ja taloudellisessa tilanteessa tulee ottaa tietoturvastrategiassa huomioon. Tietoturvallisuuden kehittämistä seuraavan työryhmän tai muun hallintoelimen tulee säännöllisesti seurata tietoturvastrategian toteuttamista. Tällä halutaan varmistaa, että strategia jatkuvasti tukee organisaation liiketoimintatavoitteita ja että se tuottaa haluttua arvoa sijoitetulle pääomalle. Tarvittaessa kyseinen taho hyväksyy muutokset tietoturvastrategiaan. (Information Security Forum 2018, 23-24.)

Tietoturvallisuuden hallintajärjestelmän mukaisista riskien arvioinneista ja käsittelystä esiin tulevia tuloksia tulee käyttää asetettujen tavoitteiden jatkuvassa katselmoinnissa ja seurannassa. Näin toimimalla pyritään varmistamaan tavoitteiden pysyminen asianmukaisina organisaatioon liittyvien olosuhteiden kanssa (SFS-ISO/IEC 27003:2017, 25). Tietoturvatavoitteet tulee päivittää silloin, kun se on tarkoituksen mukaista (SFS-ISO/IEC 27003:2017, 26). Muutokset liiketoimintastrategiassa, uhkamaisemassa tai sisäisissä tai ulkoisissa tekijöissä aiheuttavat muutostarpeita tietoturvastrategialle (Information Security Forum 2018, 23).

Tietoturvastrategian toteutusta tulee seurata säännöllisesti. Tämä voidaan tehdä keräämällä palautetta keskeisiltä sidosryhmiltä, mittaamalla edistystä asetettuja tavoitteita vasten ja varmistamalla strategisten tavoitteiden paikkansapitävyys liiketoimintaympäristön sekä toimintaympäristön muuttuessa. (Information Security Forum 2018, 23.)

Kaikki tietoturvatavoitteet eivät voi olla mitattavissa, mutta niiden tekeminen mitattaviksi mahdollisuuksien mukaan tukee tavoitteiden saavuttamista ja parantamista. Kvalitatiivisesti tai kvantitatiivisesti kuvattu tavoitteen saavuttamisen aste ohjaa ja helpottaa työhön liittyvien prioriteettien valitsemista, jos tavoite on jäänyt saavuttamatta tai antaa viitteitä mahdollisuuksista parempaan vaikuttavuuteen, jos tavoitteet on jo ylitetty. Tärkeintä on saada ymmärrys siitä, onko tavoitteisiin päästy vai ei. (SFS-ISO/IEC 27003:2017, 27.)

Muutokset liiketoimintastrategiassa, uhkamaisemassa tai sisäisissä tai ulkoisissa tekijöissä aiheuttavat muutostarpeita tietoturvastrategialle (Information Security Forum 2018, 23). Kun tietoturvaan liittyvät tarpeet ajan myötä muuttuvat, niistä koskevia tavoitteita tulee vastaavasti päivittää ja päivittämisestä on tarvittaessa viestittävä sisäisille ja ulkoisille sidosryhmille (SFS-ISO/IEC 27003:2017, 27).

ISO/IEC 27003 ohjeistaa myös suorituskyvyn arviointiin, johdon katselmointeihin ja jatkuvaan parantamiseen liittyen. Kaikista näistä voidaan poimia elementtejä strategian seurannan, arvioinnin ja päivityksen vaiheeseen. Suorituskyvyn arvioinnin osalta tavoitteena on arvioida, onko tietoturvatoiminnoille asetetut tavoitteet saavutettu riskien arviointi ja käsittely mukaan lukien. Seurannan ja mittaamisen sekä analysoinnin osalta organisaation tulee määritellä tähän liittyvät vastuut, aikataulut ja menetelmät. Johdon katselmointien tavoitteena on varmistaa hallintajärjestelmän ja kehitysohjelmien jatkuva soveltuvuus, tarkoituksenmukaisuus ja vaikuttavuus. Näistä erityisesti soveltuvuudella tarkoitetaan yhteensopivuutta organisaation tavoitteiden kanssa. Johdon katselmointeja suoritetaan organisaation eri tasoilla ja ne voivat vaihdella päivittäisitä, viikoittaisista ja kuukausittaisista määrämuotoisista tapaamisista yksittäisiin keskusteluihin. ISO-standardin mukaisten johdon katselmuksien asialis-

toilla olevat aiheet vastaavat pääpiirteittäin niitä asioita, joita strategiprosessin seurantavaiheessa olisi tarkasteltava. Näitä ovat käynnistettyjen toimenpiteiden tilanne, olennaisten ulkoisten ja sisäisten asioiden muutokset, tietoturvallisuuden tasoa koskeva palaute, sidosryhmien palaute, tietoturvariskien ja arviointien tulokset sekä käsittelysuunnitelmien tilanne ja jatkuvan parantamisen mahdollisuudet. Katselmusmenettelyjen tuloksina voi olla tarpeita tavoitteiden, toimenpiteiden, resursoinnin ja aikataulujen muutoksiin. Parantamisen osalta ISO/IEC 27003 vaatii organisaatiota reagoimaan poikkeamiin, arvioimaan ne sekä tekemään korjaavia toimenpiteitä tarpeen mukaan. Poikkeama voi olla yleisesti tiedossa olevan tavoitteen tai odotukseen täyttymättä jääminen. Poikkeamien tunnistamisen ja käsittelyn lisäksi organisaation tulee parantaa jatkuvasti tietoturvallisuuden hallintajärjestelmä soveltuvuutta, tarkoituksenmukaisuutta ja vaikuttavuutta. Tavoitteena jatkuvassa parantamisessa on tunnistaa toimintaympäristön muutokset ja tietojärjestelmiin kohdistuvien riskien ja uhkien kehitys. Järjestelmällisen jatkuvan parantamisen mallin mukaisella toiminnalla vaikuttavampaan tietoturvallisuuden johtamiseen ja proaktiivisempaan toimintamalliin. Ylin johto voi asettaa jatkuvan parantamisen tavoitteita strategisten linjausten mukaisesti. Jatkuvan parantamisen mukainen arviointi ottaa kantaa soveltuvuuteen eli siihen onko ulkoiset ja sisäiset asiat, sidosryhmien vaatimukset, asetetut tavoitteet ja tunnistetut tietoturvariskit otettu toteutuksessa huomioon. Lisäksi otetaan kantaa tarkoituksenmukaisuuteen eli ovatko prosessit ja hallintakeinot yhteensopivia organisaation yleisten tavoitteiden, toimintojen ja prosessien kanssa. Myös vaikuttavuus tulee ottaa huomioon eli onko halutut tulokset saavutettu ja sidosryhmien tarpeet täytetty, onko tietoturvariskit hallittu tietoturvatavoitteiden mukaisesti ja hallitaanko poikkeamia siten, että käytettävät resurssit vastaavat tavoiteltuja tuloksia. (SFS-ISO/IEC 27003:2017, 38-47.)

6.6 Yhteenveto

Useista tieto- tai kyberturvallisuuden viitekehyksistä on löydettävissä strategiaprosessin eri vaiheisiin kohdistuvia toimenpiteitä ja suosituksia. Esimerkiksi ISO 27001 -standardia vasten sertifiointia hakevia organisaatiota velvoitetaan tietoturvallisuuden strategisen tason johtamiseen standardin vaatimusten mukaisesti. Mutta myös muiden organisaatioiden osalta perustelut tietoturvallisuuden strategiselle johtamiselle on johdettavissa esitellystä teoreettisesta viitekehyksestä. Kyse ei vaikuta olevan yksittäisen tahon esiin nostamasta johtamisnäkökulman esiintuomisesta, vaan viittausten löytyminen useammasta viitekehyksestä kertoo strategisen johtamisen merkityksestä tietoturvallisuuden johtamisessa.

7 Toteutus

Tutkimuksessa haluttiin selvittää, ilmiönä tieto- tai kyberturvallisuuden strategista johtamista suomalaisissa suuryrityksissä ja millä tavoin merkityksellinen tietoturvastrategia rakennetaan. Tilastokeskuksen määritelmän mukaan pienillä ja keskisuurilla yrityksillä tarkoitetaan yrityksiä, joiden palveluksessa on vähemmän kuin 250 henkilöä ja joiden vuosiliikevaihto on enintään 50 miljoonaa euroa, tai joiden taseen loppusumma on enintään 43 miljoonaa euroa (Tilastokeskus N.d.) Tutkimuskohteiksi valittiin yrityksiä, jotka eivät täytä edellä mainittua määritelmää. Suuryritykset valittiin tutkimuskohteeksi, sillä niiden osuus Suomen bruttokansantuotteesta on noin 60% (Yrittäjyys Suomessa 2020) ja koska niillä on todennäköisemmin riittävät resurssit ja tahtotila tietoturvallisuuden strategisen johtamisen toteuttamiseksi.

Tutkimuksen tietoperustan avulla valmisteltiin teemahaastattelujen teemat ja apukysymykset haastattelujen toteuttamiseksi sekä sisällönanalyysin tekemiseksi. Lähdeaineiston avulla pyrittiin saamaan riittävä ymmärrys strategisesta johtamisesta kokonaisuutena sekä ottamaan huomioon tietoturvallisuuden teoreettisen viitekehyksen tuoma näkökulma aihealueeseen. Lisäksi selvitettiin, miten tunnetut tietoturvallisuuden hallintajärjestelmät huomioivat tietoturvallisuuden strategisen johtamisen.

7.1 Aineiston keräämisen toteutus

Tutkimuksessa käytetty aineisto kerättiin teemahaastatteluiden avulla. Tutkimuksessa käytetty teemahaastattelun runko on tutkimuksen liitteenä (Liite 2). Teemahaastattelujen pohjaksi oli valittu neljä teemaa, joista yksi oli tässä tutkimuksessa esitellyn lineaarisen strategiaprosessin mukainen vaiheistus. Haastatteluissa käytetyt teemat olivat:

1. Tietoturvallisuuden strategisen johtamisen ilmentyminen organisaatiossa
2. Merkityksellinen tietoturvastrategia
3. Tietoturvallisuuden vision ja mission määrittely
4. Strategiaprosessi

Haastattelujen toteutuksen aikana näitä teemoja lähestyttiin tarvittaessa apukysymysten avulla. Haastattelujen tyyppi oli ns. puolistrukturoitu haastattelu, jossa pääpiirteittäin seurattiin löyhästi suunniteltua haastattelurunkoa, mutta jonka aikana keskustelun annettiin tarvittaessa rönsyillä luonnollisesti uusiin suuntiin. Haastattelunrungon avulla pyrittiin varmistamaan, että kaikki suunnitellut teemat ja aihealueet tulivat haastattelun aikana käsitellyiksi. Teemahaastatteluihin kutsuttiin henkilöitä

tutkijan omasta verkostosta siten, että heidän edustamansa organisaatiot täyttivät tutkimuksen kohderyhmän kriteerit.

Tutkimuksen tiedonkeruuvaihe toteutettiin 26.3.-8.4.2020 välisenä aikana. Haastattelut toteutettiin Teams-kokouksina, jotka taltioitiin Teamsin nauhoitustoiminnallisuutta käyttäen. Haastattelun jälkeen mp4-tiedostomuodossa olevat tallenteet siirrettiin tutkijan omalle tietokoneelle litterointia varten.

Tutkimuksessa lähdettiin liikkeelle pienestä joukosta haastateltavia. Haastateltavien valinnassa painotettiin informanttien tutkimusongelman ratkaisuun hallussaan pitämää tietoa ja osaamista. Haastattelujen tekemistä eli aineiston keräämistä jatkettiin tämän jälkeen niin kauan, kunnes aineistossa alettiin havaitsemaan saturaatiota.

Haastateltavat ja heidän edustamansa yritykset ovat kuvattuina seuraavassa taulukossa.

Taulukko 2. Haastatteluihin osallistuneet henkilöt ja organisaation kuvaus

Haastateltava	Titteli	Henkilöstön määrä	Liikevaihto
Henkilö A	Turvallisuusjohtaja	3400	2 mrd. €
Henkilö B	Tietoturvajohtaja	700	168 milj. €
Henkilö C	Tietoturvajohtaja	19 000	5 mrd. €
Henkilö D	Head of Cybersecurity Development	12 000	3 mrd. €
Henkilö E	Chief Information Security Officer	10 000	6 mrd. €

Haastattelut toteutettiin siten, ettei haastateltavien henkilöllisyys tai heidän edustamansa organisaatio käy ilmi tutkimusaineistosta.

7.2 Aineiston analyysin toteutus

Tutkimusaineiston litteroinnissa käytetty tarkkuustaso vastasi yleiskielistä litterointia ja aineisto litteroitiin huhtikuun 2020 ja toukokuun 2020 välisenä aikana. Aineiston analysointi aloitettiin välittömästi teemahaastattelujen aikana sitä mukaa, kun litterointeja valmistui.

Aineiston luokittelussa käytettiin teorialähtöistä sisällönanalyysiä teoriasta johdettujen käsitteiden avulla. Analyysivaiheessa valittiin ensin analyysirunko tässä raportissa esitellyn teoreettisen viitekehyksen pohjalta. Analyysirungon yläluokat muodostettiin Sillanpään ja muiden esittelemän Cyber Strategy Process -mallin mukaisesti strateginen analyysista, strategisesta painopisteestä ja strategisesta toteutuksesta.

Cyber Strategy Process -malli valittiin yläluokkien lähteeksi, koska llineaarisen strategiaprosessin vaiheet voidaan tiivistää näihin kolmeen luokkaan. Tämä helpotti aineiston analyysin tekemistä. Edellä mainittujen yläluokkien lisäksi analyysirunkoon valittiin vielä yksi yläluokka ”Merkityksellinen strategia” tutkimuskysymysten mukaisesti. Tämän jälkeen tehtiin aineiston pelkistäminen sisällönanalyysiä noudattaen. Luokittelussa lähdettiin siitä, että aineistosta pyrittiin löytämään systemaattisen tarkastelun avulla analyysirungon mukaisia ilmiöitä, jotka kuvasivat tietoturvallisuuden strategisen johtamisen alaluokkia. Pelkistämisen jälkeen tunnistettiin alaluokat, jotka on esitelty alla olevassa taulukossa.

Taulukko 3. Aineistosta tunnistetut alaluokat

Yläluokka	**Alaluokat**
Strateginen analyysi	Sidosryhmä, ulkoinen toimintaympäristö, sisäinen toimintaympäristö, riskiarviointi, uhka-arviointi, nykytilan tunnistaminen
Strateginen painopiste	Johdon sitoutuminen, liiketoimintalähtöisyys, integraatio organisaation tavoitteisiin, strateginen päätös, vaihtoehtojen arviointi, strategian laatiminen, tavoitteet, mittaristo, visio, missio, liiketoimintastrategia, ICT-strategia, painopisteet
Strateginen toteutus	Resursointi, jatkuva parantaminen, muutoshallinta, muutostarpeet, seuranta, mittaaminen, raportointi
Merkityksellinen strategia	Motivointi, tuloksellisuus, relevanssi, haastavuus, ymmärrettävyys, kattavuus, liiketoimintalähtöisyys, seurattavuus, realismi, mahdollistaminen, riskitietoisuus, sitouttaminen

8 Tulokset

Tutkimuksessa kerätyn aineiston mukaan näyttää siltä, että tietoturvallisuuden strategisen tason johtaminen ei ole vakiintunutta toimintaa haastateltujen organisaatioiden joukossa. Haastatteluaineistosta on jokaisen organisaation osalta tunnistettavissa teorialähtöisen sisällönanalyysin yläluokkien mukaisia vastauksia mutta aineistoa tarkastelemalla käy ilmi, että näkökulma näihin asioihin on pikemminkin taktinen (keskipitkän aikavälin suunnitelmat) tai operatiivinen (päivittäisen toiminnan johtaminen). Tutkimuksen tuloksia on avattu tarkemmin seuraavissa alaluvuissa.

8.1 Vastaukset tutkimusongelmaan ja kysymyksiin

Tutkimuksessa kerätyn aineiston ja sille tehdyn sisällönanalyysin perusteella saatiin selville seuraavat vastaukset tutkimuskysymyksiin.

8.1.1 Johdetaanko tietoturvallisuutta suomalaisissa suuryrityksissä strategisesti?

Tutkimusaineiston analyysin tuloksena voidaan sanoa, että haastateltujen yritysten osalta tietoturvallisuuden strategisen tason johtaminen ei ole vielä vakiintunutta toimintaa. Tämä ei tarkoita, että organisaatiot johtaisivat kyber-tai tietoturvallisuutta huonosti vaan sitä, että määrämuotoiselle strategisen tason huomioimiselle tietoturvallisuuden johtamisessa ei ole tunnistettu erityistä tarvetta organisaation sisällä tai sitä ei ole vielä osattua ajatella yhtenä johtamisen muotona. Kaikki haastatelluista organisaatioista tekevät päämäärätietoisesti ja huolellisesti työtä tietoturvallisuuden kehittämiseksi ja liiketoiminnan jatkuvuuden varmistamiseksi sekä uusien liiketoimintamahdollisuuksien tukemiseksi. Kaikki nämä ovat teemoja, jotka nousevat esiin

myös tutkimuksen teoreettisesta viitekehyksestä. Aineistosta käy siis ilmi, että strategisen johtamisen teoreettisen viitekehyksen mukaisia toimia tehdään, mutta tulokulma on enemmän taktinen tai operatiivinen. Yritykset pyrkivät ainakin jossain määrin tunnistamaan sekä sisäisessä että ulkoisessa toimintaympäristössä tapahtuvia muutoksia. Yleisimmin nämä ilmenevät riskiarviointien ja uhkamallinnusten tulosten huomioimisena suunnittelutyössä. Myös muutoksia uhkamaisemassa pyritään aktiivisesti tunnistamaan.

> *" Se on pitkälti sitä et miten me voidaan ennakoida niit asioita niin että me ollaan, hyvä kumppani sinne liiketoimintaan päin, tuli asioita eteen minkälaisia tahansa, et me ymmärretään se kokonaisuus."*

Kahdella tutkimukseen osallistuneista yrityksistä oli valmis ja jalkautettu tietoturvastrategia. Yhdellä organisaatiolla tietoturvastrategian kehittämisen tarve oli tunnistettu, mutta työ strategiaprosessin toteuttamiseksi ei ollut vielä alkanut eikä esimerkiksi analyysivaiheen toimenpiteitä ollut vielä tarkemmin suunniteltu. Erään organisaation johtamisjärjestelmä ohjasi säännöllisin väliajoin tekemään keskipitkää suunnittelua ja näistä suunnitelmista oli mahdollista tunnistaa joitain strategiaprosessin mukaisia toimenpiteitä. Ne organisaatiot, joilla oli dokumentoitu ja määritelty tietoturva- tai kyberstrategia, olivat tehneet sen vastikään.

> *" Me viime vuoden aikana käytännössä, luotiin ensimmäisen kerran kyberturvallisuusstrategia."*

Sääntely vaikuttaisi vaikuttavan tietoturvallisuuden strategiseen johtamiseen. Ne haastatelluista yrityksistä, jotka toimivat vahvasti säännellyillä aloilla, olivat todennäköisesti tietoisempia tietoturvallisuuden strategisen tason johtamisen merkityksestä organisaation liiketoimintatavoitteiden saavuttamisen tukemisessa.

Strategiaa ei saa sanoa strategiaksi. Vain yhdessä organisaatiosta tieto- tai kyberturvallisuusstrategiaa kutsuttiin strategiaksi, toisessa sille oli keksitty organisaation sisällä kiertoilmaisu. Myös tietoturvastrategian tekemisen aloittamista suunnittelevan yrityksen sisällä oli jo ehditty käymään keskustelua siitä, millä nimellä strategiaa saisi sen valmistuttua kutsua. Syyksi haastatteluissa nostettiin ajatus siitä, että yrityksellä voi olla vain yksi strategia, joka on liiketoimintastrategia, ja muut strategiat vain aiheuttaisivat tarpeetonta hämmennystä.

> *” Se kulkee meidän organisaatiossa hieman toisella nimellä, puhutaan myös arkisesti kyberturvallisuuden toimintasuunnitelmasta.”*

Tuloksia arvioitaessa on syytä muistaa, että strategia itsessään ei ole itseisarvo. Se on keino suunniteltuihin tavoitteisiin pääsemiseksi mutta asetetut tavoitteet on mahdollista saavuttaa myös muilla keinoin.

Alla olevissa taulukoissa on esiteltyinä aineistosta sisällönanalyysin aikana esiin nousseet teemahaastatteluissa käsitellyt aihealueet, aihealueiden käsittelyn lukumäärä sekä maininta siitä, onko aihealueesta keskusteltu strategisen johtamisen näkökulmasta vai onko haastateltavan kuvailu ollut enemmän taktiseen tai operatiiviseen johtamiseen kuuluvaa.

Taulukko 4. Vastausten painottuminen analyysivaiheen osalta

	Strategisen aseman analyysi							
	Ympäristö		Sidosryhmät		Tarkoitus		Riskit / Uhat	
Näkökulma	Strateginen	Taktinen / Operatiivinen	Strateginen	Taktinen / Operatiivinen	Strateginen	Taktinen / Operatiivinen	Strateginen	Taktinen / Operatiivinen
Henkilö A	1	4				3		1
Henkilö B		4		1	1	1		3
Henkilö C			1		1			1
Henkilö D	7		6		3		2	
Henkilö E	1	4	1	3	1	1	1	2

Strategisen analyysivaiheen osalta riskit ja uhat nostettiin omaksi osa-alueekseen, vaikka niiden voidaan katsoa kuuluvan osaksi ympäristön analyysia. Valinta on perusteltu, sillä tietoturvastrategian kontekstissa riskien ja uhkien tunnistamisella on keskeinen merkitys, vaikka sisäisen ja ulkoisen ympäristön analyysi jäisi muutoin vähemmälle huomiolle. Taulukon 4 pohjalta voidaan sanoa, että strategisen tason huomioimista analyysivaiheen osalta on tehty niissä organisaatioissa, joissa määritelty strategia on olemassa ja muiden osalta analyysivaiheen asioita on huomioitu mutta näkökulma ei ole ollut strateginen.

Taulukko 5. Vastausten painottuminen strategisen painopisteen valinnan osalta

	Strateginen valinta							
	Suunta		Johdon sitoutuminen		Tavoitteet		Kehitysprojektit	
Näkökulma	Strateginen	Taktinen / Operatiivinen	Strateginen	Taktinen / Operatiivinen	Strateginen	Taktinen / Operatiivinen	Strateginen	Taktinen / Operatiivinen
Henkilö A	1	1	1	3	1	6	2	4
Henkilö B	1	2			1	5		1
Henkilö C	2		3		3		2	1
Henkilö D	4		2		7		7	
Henkilö E		1		2	2	4		5

Taulukossa 5 on esiteltynä vastausten painottuminen strategien määrittelyvaiheen osalta. Tulosten vetämistä yhteen vaikeuttaa se, että vaikka organisaatiolla ei olisi määriteltyä tietoturvastrategiaa, on se silti voinut tehdä strategisen tason valintoja, joita voivat olla liiketoiminnan strategisten tavoitteiden huomioiminen kehitysprojektien valinnassa, johdon sitoutumisen varmistaminen, tavoitteiden linjaaminen yrityksen tavoitteiden kanssa ja tietoturvatyön suunnan eli vision määrittely. Tulosta voidaan tulkita siten, että teoreettisen viitekehyksen mukaisia oikeita toimenpiteitä tehdään, vaikka valinnat tai päätökset eivät ole strategisen johtamisen viitekehyksen ohjaamia.

Taulukko 6. Vastausten painottuminen strategian toteutuksen osalta

	Strategian toteutus							
	Arviointi ja raportointi		**Muutos**		**Organisointi**		**Resursointi**	
Näkökulma	Strateginen	Taktinen / Operatiivinen	Strateginen	Taktinen / Operatiivinen	Strateginen	Taktinen / Operatiivinen	Strateginen	Taktinen / Operatiivinen
Henkilö A		2		2		1	1	2
Henkilö B	2	4		1			1	
Henkilö C		1	1		3		1	1
Henkilö D	4		1		2		2	
Henkilö E		5		2		3		4

Taulukossa 6 on näkyvissä vastausten painottuminen strategian toteutuksen osalta. Tulosten pohjalta on erotettavissa organisaatio, jonka lähestymistapa on ollut strateginen. Jälleen myös muut organisaatiot ovat tehneet viitekehyksen mukaisia asioita, mutta lähestyminen on ollut enemmän vuosisuunnittelun mukaista. Resursointia lähestytään kuitenkin lähes poikkeuksetta strategisesta näkökulmasta ja tällä on pyritty varmistamaan kyvykkyys liiketoimintastrategian tukemiseen.

8.1.2 Miten merkityksellinen tietoturvastrategia rakennetaan?

Tutkimusaineisto ei anna täysin luotettavaa vastausta tähän tutkimuskysymykseen, sillä ainoastaan kahdella haastatelluista organisaatioista oli teoreettisen viitekehyksen asettaman tason mukainen tietoturvastrategia tai -ohjelma ja näistä vain toisen osalta pystyttiin haastattelussa käymään strategiaprosessia ja strategian toteutusta vaihe vaiheelta läpi. Aineistosta voidaan kuitenkin tunnistaa merkityksellisen tietoturvastrategian rakentamiseen liittyviä teemoja kaikkien haastateltujen vastauksista.

Aineistosta nousee esiin sidosryhmien tunnistaminen, toimintaympäristöjen analyysi, uhkamaisemassa mahdollisesti tapahtumassa olevien muutosten tunnistaminen, uhkatoimijoiden tunnistaminen, vaihtoehtojen arviointi ja mittaamisen sekä seurannan suunnittelu.

Merkityksellisen tietoturvastrategian rakentaminen ei ole pienellä porukalla tehtävää komiteatyötä, vaan sen tekemiseen tulee sitouttaa henkilöitä organisaatiosta riittävän laajalti riittävän näkemyksen muodostamiseksi nykytilasta, tavoitetilasta, käytettävissä olevista resursseista ja tulevaisuuden visiosta. Työlle tulee varata myös aikaa varsinkin muiden töiden ohella tehtynä.

Merkityksellisen tietoturvastrategian rakentamisessa tulee erityisesti ottaa huomioon liiketoiminnan suunta, tavoitteet ja tahtotila. Tämä käy erityisesti ilmi tutkimusaineistosta. Liiketoimintastrategian etenemistä ja johdon strategisia päätöksiä on seurattava ja niihin on pyrittävä reagoimaan nopeasti.

> *”Mehän yritetään peilata jatkuvasti sit sitä, niitä asioita mitä liiketoiminta tekee ja mihin suuntaan se on menossa ja mitä strategisia päätöksiä siellä tehdään, digitaalisten tuotteitten osalta tai eri kanavaratkasuissa, ja ollaan niissä sitte mukana, tekemässä niitä asioita ja toisaalta sitte mahdollistamassa niitä.”*

Tietoturvallisuuden tavoitteita pyritään siis linjaamaan yhteneväisiksi liiketoimintatavoitteiden tai -strategian kanssa. Tutkimusaineistosta ei käy ilmi, että tietoturvallisuuden elementtejä olisi suoraan nostettu mukaan liiketoimintastrategiaan. Tämä voi johtua siitä, että tutkimukseen osallistuneiden yritysten toimiala on jotain muuta kuin suoraan tietoturvallisuuteen liittyvää järjestelmä- tai palvelutuotantoa.

Aineistosta nousee esiin myös ylimmän johdon tuen merkitys strategian ja strategisten projektien tarvitseman rahoituksen saamiselle. Tietoturvatyölle voi olla tukea johdon juhlapuheissa, mutta vasta tarvittavien resurssien eli rahoituksen antaminen kehityshankkeille kertoo todellisesta tuesta. Kehitysprojektien ja -hankkeiden eteenpäin viemisessä korostuu proaktiivinen ote ylimmän johdon suuntaan.

> *” Haetaan, myös kontaktia tai sponsoria sieltä BOM-tasolta, että siellä on joku tukemassa suoraan sitä hanketta tai muutamaki henkilö.”*

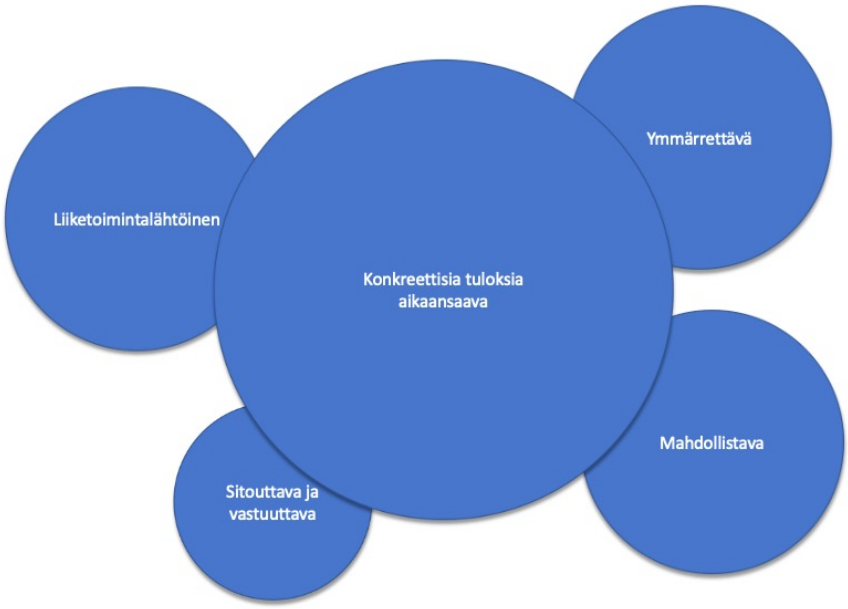
8.1.3 Mistä tekijöistä merkityksellinen tietoturvastrategia koostuu?

Teoreettinen viitekehys kuvaa mitä sisällöllisiä elementtejä tietoturvastrategiassa tulee ottaa huomioon, mutta yksistään näiden elementtien huomioiminen ei itsessään tuota merkityksellistä strategiaa. Merkityksellisyyden tuo se, mitä, miten ja kenelle tietoturvastrategian avulla viestitään.

” Siin on varmaan, et nimenomaan merkityksellinen ja merkityksellinen kenelle. Eli mihin se yrittää vastata tai kelle se yrittää vastata.”

Merkityksellistä tietoturvastrategiaa rakennettaessa on siis syytä miettiä sitä kohderyhmää tai kohderyhmiä, joille strategian pääviestit on suunnattu. Valitsemalla hyvin rajatut tärkeimmät sidosryhmät ja varmistamalla, että heille strategiassa suunnattu viesti on selkeä, mahdollisuudet muodostaa merkityksellinen strategia kasvavat.

Tutkimusaineiston analyysissä nousi esiin selkeät viisi tekijää, joiden avulla merkityksellinen tietoturvastrategia on mahdollista luoda. Iso osa tekijöistä on sellaisia, jotka voidaan yhdistää teoreettisen viitekehyksen tietoturvastrategialle esittämiin vaatimuksiin, mutta mukana on myös ns. pehmeämpiä arvoja esiin nostavia tekijöitä, jotka liittyvät pääosin edellä mainittuun kohderyhmälähtöiseen viestintään.



Kuvio 17. Merkityksellisen tietoturvastrategian elementit

Kuviossa 17 on esiteltynä aineistosta esiin nousevat keskeiset merkityksellisen tietoturvastrategian osa-alueet. Kuviossa olevan osa-alueen koko kuvastaa osa-alueen saamien mainintojen määrää aineistossa.

Vaikka liiketoimintalähtöisyys oli aineistosta vahvasti esiin nouseva teema, nousi konkreettisuus ja tuloksellisuus tarkemman analyysin jälkeen kaikkein merkittävämmäksi tekijäksi. Merkityksellisen tietoturvastrategian tulee saada aikaan konkreettista tekemistä asetettujen tavoitteiden saavuttamiseksi ja tekemisellä tulee saada näkyviä tuloksia aikaiseksi. Teoreettisessa viitekehyksen mukaan tekeminen konkretisoituu ja muuttuu näkyväksi strategisten projektien kautta, jolloin projektien tulee olla hyvin asetettuja ja niiden pitää pystyä tuomaan näkyviä tuloksia riittävän nopeasti. Aineiston perusteella kehittämistoimenpiteiden tulee olla sellaisia, että niiden

tuottama arvo on mitattavissa. Lisäksi tekemiselle asetettujen tavoitteiden tulee olla asetettuina riittävän korkealle, jotta aitoa kehittymistä ja eteenpäin menemistä myös tapahtuu. Haastavien tavoitteiden kautta syntyy motivaatio, joka saa tuloksia aikaiseksi. Hieman aiempaa suoritustasoa paremman tason hakeminen ei riitä. Tavoitteiden asettamisessa pitää kuitenkin muistaa myös maltti, sillä aineiston perusteella strategian tulee olla reaalimaailmaan soveltuva.

Aineiston perusteella kolme seuraavaa osatekijää (liiketoimintalähtöisyys, ymmärrettävyys ja mahdollistavuus) olivat yhtä keskeisiä merkityksellisyyden luomiseksi. Liiketoimintalähtöisyydessä keskeistä on linkittyminen liiketoimintastrategiaan teoreettisen viitekehyksen suositusten mukaisesti. Aineiston perusteella ei ole yleistä, että liiketoimintastrategia itsessään sisältäisi vielä tietoturvallisuuteen liittyviä elementtejä ainakaan aloilla, jotka eivät suoraan tuota tietoturvallisuuteen liittyviä palveluita tai tuotteita. Aineiston pohjalta voidaan todeta, että strategiassa tulee selkeästi kuvata ne toimenpiteet, joilla edesautetaan liiketoimintastrategian toteutumista. Teoreettisen viitekehyksen mukaisesti ilman kytköstä liiketoimintaan ja liikeroimintastrategiaan tietoturvastrategia jää irralliseksi harjoitukseksi, joka ei tue organisaation keskeisiä tavoitteita.

Ymmärrettävyydellä tarkoitetaan aineiston perusteella sitä, että strategia puhuu kieltä, jota lukijat ymmärtävät. Strategian esitysmuoto, kieli ja lähestymistapa tulee olla sellaisia, että kuka tahansa organisaatiosta ymmärtää mistä strategiadokumentaatiossa puhutaan. Tietoturvastrategialle tulee tunnistaa keskeiset kohderyhmät, joiden toimintaan strategialla halutaan vaikuttaa. Kohderyhmien tunnistaminen on osa teoriapohjassa mainittua analyysivaiheen sidosryhmäanalyysia ja siitä saadun tiedon hyödyntäminen strategian luomisessa edesauttaa tavoitellun tulevaisuuden tilan saavuttamista. Aineiston yhdessä esimerkissä tietoturvastrategialle oli tunnistettu

kaksi keskeistä kohderyhmää: tietoturvallisuuden piirissä päivittäin töitä tekevät tietoturva-ammattilaiset sekä liiketoimintayksiköiden edustajat. Näiden kahden kohderyhmän ymmärrys aihealueesta sekä siihen liittyvät tarpeet poikkeavat toisistaan, jolloin nämä erot tulee ottaa strategian luomisessa huomioon. Kumpikin kohderyhmä on kuitenkin yhtä merkittävä. Ensimmäisten tulee saada tukea sekä vahvistusta omalle työlleen ja jälkimmäisten osalta tulee lisätä heidän ymmärrystään tietoturvallisuuden mahdollisista vaikutuksista liiketoimintaan ja sen kehittämiseen. Tietoturvastrategian sisältö siis tarkoittaa eri asioita eri kohderyhmille ja tämä tulee huomioida merkityksellisen tietoturvastrategian luomisessa.

Mahdollistamisen voi nähdä yhtenä liiketoimintalähtöisyyden elementtinä mutta se haluttiin nostaa omaksi erilliseksi osa-alueekseen selkeän aineistossa esiintymisen johdosta. Mahdollistamisella tarkoitetaan aineiston perusteella sitä, että merkityksellisen tietoturvastrategian pitää erityisesti nostaa esiin mahdollisuuksia kehittää yrityksen liiketoimintaa. Strategian avulla tulee pystyä luomaan tietoturvallinen toimintakenttä, jossa uusien liiketoimintamahdollisuuksien kokeilut voidaan tehdä paitsi turvallisesti mutta myös tehokkaasti ja joustavasti. Tietoturvastrategian avulla ei pidä luoda toimintaympäristöä, jossa tietoturva on liiketoiminnan kehittämisen este tai hidaste.

Viimeinen keskeinen merkityksellisen tietoturvastrategian elementti on sitouttavuus ja vastuuttavuus. Tietoturvastrategiassa määritellyt ylätasoiset toimenpiteet tulee olla selkeästi vastuutettu esimerkiksi organisatorisella tasolla siten, että tavoitteiden saavuttamisen ja siihen liittyvän mittaamisen vastuukysymykset eivät ole epäselviä. Tämä merkityksellisen tietoturvallisuuden osatekijä voidaan nähdä osana teoriapohjassa esitetyn seurannan, arvioinnin ja päivityksen vaihetta, johon sisältyy myös tar-

vittavat raportointivelvollisuudet yrityksen johdon ja strategian seurannasta vastaavien organisaation osien suuntaan. Sitouttavuudella tarkoitetaan aineiston mukaan sitä, että keskeiset vastuutahot myös sitoutuvat yhteisiin tavoitteisiin ja päämääriin. Keskeistä sitoutumisen kannalta on strategian ymmärrettävyys, jolloin päästään takaisin analyysivaiheen sidosryhmien tunnistamiseen ja strategian sisältämän viestin kohdentamiseen.

9 Johtopäätökset ja pohdinta

9.1 Keskeisten tulosten tarkastelu

Tutkimuksen yhtenä tarkoituksena oli selvittää tietoturvallisuuden strategisen johtamisen merkityksellisyyttä. Merkityksellisyyttä voi tarkastella kahdesta näkökulmasta: onko strategisella johtamisella itsellään merkitystä eli näkevätkö organisaatiot strategisen tason johtamiselle tarvetta tai onko tietoturvaorganisaation kehittämä strategia sen keskeisille kohderyhmille merkityksellinen.

Tutkimustuloksissa on näkyvissä teoreettisen viitekehyksen mukaisia tietoturvallisuuden strategisen johtamisen elementtejä. Kuitenkaan tutkimusaineiston perusteella ei voida sanoa, että tietoturvallisuuden strateginen johtaminen olisi ilmiönä selkeästi havaittavissa tutkimuksen kohteena olleissa organisaatioissa. Aineistosta nousee esiin teoreettisen viitekehyksen mukaisia toimenpiteitä mutta aineiston perusteella niihin liittyvä tulokulma on enemmän taktinen tai operatiivinen.

Edellisten perusteella johtopäätös on, ettei tietoturvallisuuden strategisen tason johtamiselle ole vielä nähty runsaasti tarvetta haastateltujen organisaatioiden keskuudessa Tähän voi olla lukuisia syitä. On mahdollista, ettei tietoturvan strategista johtamista nähdä vielä tarpeellisena tilanteessa, jossa organisaation pääliiketoiminta ei ole suoraan tietoturvaan liittyvää. Kuitenkin Suomen kyberturvallisuusstrategian määrittelemillä yhteiskunnallisesti kriittisillä toimialoilla, kuten tietoliikenne, energiantuotanto ja -jakelu, finanssi- ja vakuutusala sekä terveydenhuolto on niin vahvat riippuvuudet kyberturvallisuuteen ja siihen liittyviin häiriöihin, että jatkossa tilanne saattaa olla toinen.

Merkityksellisen tietoturvastrategian tekijöistä saatiin tutkimuksen perusteella hyvä kuva. Keskeiset osatekijät tunnistettiin ja ne huomioimalla toiminnan johtaminen merkityksellisen tietoturvastrategian avulla on mahdollista. Keskeinen tutkimustulos kuitenkin on, että pelkästään teoreettisen viitekehyksen asiat huomioimalla ei merkityksellistä tietoturvastrategiaa synny. Erityisesti keskiöön nousee tarve saada aikaiseksi konkreettisia tuloksia. Koska rinnakkaisuuden lisääminen kiinteillä resursseilla ei kasvata valmistuneiden töiden määrää, on strategisten kehitysprojektien laajuuden määrittelyssä ja aikatauluttamisessa pyrittävä myös nopeisiin voittoihin välittömien tulosten aikaansaamiseksi. Saavutetuista voitoista on myös muistettava viestiä keskeisille sidosryhmille positiivisen mielikuvan luomiseksi ja ruokkimiseksi.

9.2 Luotettavuus ja eettisyys

Luotettavuuden ja eettisyyden osalta on pohdittava sekä havaintojen luotettavuutta että niiden puolueettomuutta. Puolueettomuuden osalta tutkijan on arvioitava, onko hän onnistunut ymmärtämään haastateltavilta saamaansa tietoa sellaisenaan vai suodattuuko sitä hänen omien asenteidensa ja uskomustensa läpi. Tutkijan oma

asenne vaikuttaa tuloksiin väistämättä, joten tämä on asia, joka tutkijan tulee aineistoa analysoidessaan ja tuloksia määritellessään ottaa aktiivisesti huomioon. Tämän tutkimuksen osalta käyttöön valittu teorialähtöinen sisällönanalyysi osaltaan vähentää tutkijan puolueellisuuden vaikutusta tuloksiin mutta ei toki poista sen mahdollisuutta kokonaan. Tutkimuksen analyysin ja tulosten kirjaamisen aikana tutkija pyrki tietoisesti varmistamaan puolueettomuuden toteutumisen palaamalla tarvittaessa litteroituun aineistoon tarkastamaan haastateltavien vastauksen sisällön ja tarkoituksen.

Luotettavuuden arvioinnin osalta yleinen käsitys on, ettei validiteetin ja reliabiliteetin käsitteitä tulisi käyttää laadullisen tutkimuksen luotettavuuden arvioinnissa. Sen sijaan luotettavuutta voidaan arvioida esimerkiksi uskottavuuden ja riippumattomuuden näkökulmasta. Tutkijan rooli tutkimuksessa oli olla tarkkailija eikä tutkija puuttunut tutkimuskohteiden toimintaan tutkimuksen aikana. Tutkijan oma organisaatio oli jätetty tutkimusaineiston keräämisen ulkopuolelle vääristymien välttämiseksi. Aineiston keruu tapahtui jokaisen haastateltavan kanssa samoja järjestelyjä ja samaa haastattelurunkoa käyttäen. Kaikki haastattelut taltioitiin. Aineiston keruu tapahtui varsin lyhyessä ajassa ja aineistoa olisi voitu kerätä enemmän. Toisaalta aineiston analysoinnin aloittaminen haastattelujen aikana paljasti aineiston saturoituneen jo pienellä määrällä haastatteluja eikä uusien haastattelujen tekeminen olisi välttämättä tuonut aineistoon enää uusia näkökulmia.

Luotettavan vastauksen saaminen tutkimuskysymykseen ”Miten merkityksellinen tietoturvastrategia rakennetaan” olisi vaatinut haastateltavien valintavaiheessa esiseulontaa, jotta haastateltaviksi olisi valikoitunut yrityksiä, joilla on olemassa oleva tietoturvastrategia ja kokemusta strategiaprosessin toteuttamisesta.

9.3 Johtopäätökset ja kehittämisehdotukset

Tietoturvallisuuden strategisen tason johtaminen on tunnetuissa tietoturvallisuuden viitekehyksissä esiin tuotu ilmiö, joka tähtää organisaatioiden liiketoimintatavoitteiden saavuttamisen varmistamiseen tietoturvallisuuden avulla. Lisäksi sillä pyritään varmistamaan liiketoimintastrategian toteuttamisen ja toteutumisen aiheuttamien muutosten huomioiminen yrityksen tietoturvatyössä. Vaikka viitekehykset ohjaavat niitä hyödyntäviä organisaatioita strategisen johtamisen mukaiseen toimintaan, ei tämän tason toiminta vaikuta tämän tutkimuksen perusteella olevan laajasti käytössä.

Tutkimuksen johtopäätös oli, etteivät organisaatiot koe vielä tarpeelliseksi johtaa tietoturvallisuutta strategisella tasolla tai yritysten tietoturvaorganisaatiot pystyvät saavuttamaan niille asetetut tavoitteet muilla keinoin. Digitalisaation edetessä myös kyberturvallisuuden huomioiminen nousee johtoryhmien ja yritysten hallitusten mielenkiinnon kohteeksi, jolloin jatkossa organisaatiot saattavat ottaa tietoturvallisuuteen liittyviä elementtejä jopa osaksi liiketoimintastrategiaansa.

Tutkimuksen olisi voinut tehdä ajankäytöllisesti tehokkaammin, jolloin aineiston keräämiseen ja analysointiin olisi jäänyt paremmin aikaa. Tutkimuksen varsinaista käynnistymistä hidasti tutkijan epätietoisuus käytettävästä tutkimusmenetelmästä ja lähestymistavasta. Kun tutkimusote oli saatu vaihdettua laadulliseen tutkimukseen, lähti tutkimus rullaamaan nopeasti eteenpäin. Aineiston keräämisen osalta olisi ollut tuloksellista kysyä potentiaalisilta haastateltavilta ennen haastateltavaksi valitsemista, onko organisaatiolla olemassa tietoturvastrategia tai 3-5 vuoden tietoturvallisuuden kehittämisohjelma. Tällöin vastaaminen tutkimuskysymyksiin 2. ja 3. olisi ol-

lut luotettavampaa laajemman aineiston ansiosta. Toisaalta tällöin olisi jäänyt saamatta vastaus 1. tutkimuskysymykseen (”Johdetaanko tietoturvallisuutta strategisesti”), johon jo näinkin pienellä aineistolla saatiin varsin selkeä vastaus.

9.4 Jatkotutkimusehdotukset

Tietoturvallisuuden strateginen johtaminen on mielenkiintoinen aihe, jossa yhdistyvät kompleksinen ja alati muuttuva kyber- ja tietoturvallisuuden kenttä ja johtamisoppi. Tässä tutkimuksessa esiin tuodun teoreettisen viitekehyksen ja tutkimustulosten valossa näkisin hyviä jatkotutkimusaiheita YAMK-opinnäytetöiksi esimerkiksi kehittämistutkimuksen avulla toteutettaviksi. Ehkäpä tällä tavoin saataisiin jalkautettua tietoturvallisuuden strategista johtamista laajemmalti käyttöön suomalaiseen yrityskenttään.

Toinen mielenkiintoinen jatkotutkimuskohde voisi olla Suomen kansallisen kyberturvallisuusstrategian ja siihen liittyvien kehitysohjelmien analysointi. Tutkimuksella voitaisiin selvittää mitä tähän mennessä kehitysohjelmilla on saatu aikaan ja miten strategiassa esitetty visio siitä, että Suomi on maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja häiriöiden hallinnassa on toteutunut.

Edellä mainittujen lisäksi olisi mielenkiintoista selvittää tutkimuksen avulla, miten Suomen kyberturvallisuusstrategia 2019:n mainitsemat toimialat (tietoliikenne, energiantuotanto ja -jakelu, finanssi- ja vakuutusala sekä terveydenhuolto) ovat varautuneet toimialakohtaisesti uusien kyberuhkien torjumiseen ja hyökkäyksistä toipumiseen, miten toimialakohtaista varautumista johdetaan ja tehdäänkö toimialoilla yhteistä strategisen tason suunnittelua reagointi- ja vastekyvyn parantamiseksi.

Laadullista tutkimusmenetelmää käytettäessä tiedonantajien määrän merkitys on vähäisempi kuin kvantitatiivisia menetelmiä käytettäessä. Mahdollisissa jatkotutkimuksissa olisikin hyvä lisätä myös tutkittavien organisaatioiden määrää, jolloin aihetta olisi mahdollista tarkastella laajemmin. Mahdollisella tutkimusotteen vaihtamisella ja laajemmalla aineistolla olisi mahdollista saada monipuolisempi kokonaiskuva. Tämä antaisi mahdollisesti myös luotettavamman kokonaiskuvan yritysten tietoturvan strategisen johtamisen tilanteesta. Mikäli aihetta tutkittaisiin laajemmin, tulisi mahdollisesti haastattelut laajentaa koskemaan myös esimerkiksi yritysten johtoryhmiä.

Lähteet

Akpeninor, J.O. 2013. Modern Concepts of Security. Viitattu 3.5.2020. https://books.google.fi/books?id=80LoJ9_dCC4C&printsec=frontcover&hl=fi#v=onepage&q&f=false

Dawson H. 2019. The Most Influential Security Frameworks of All Time. Infosecurity magazine. 27.6.2019. Viitattu 25.4.2020. https://www.infosecurity-magazine.com/opinions/most-influential-frameworks-1-1-1/

Dekker M, Karsberg C, Lakka M, Liveri D. 2013. Auditing Security Measures. An Overview of schemes of auditing security measures. European Union Agency for Network and Information Security (ENISA). Viitattu 29.4.2020. https://www.enisa.europa.eu/publications/schemes-for-auditing-security-measures/at_download/fullReport

ISACA Glossary N.d. Teknisten termien sanasto ISACA:n sivustolla. Viitattu 29.4.2020. https://www.isaca.org/resources/glossary

Information Security Forum. 2018. The Standard of Good Practice for Information Security 2018. Viitattu 25.4.2020. https://www.securityforum.org/tool/the-isf-standard-good-practice-information-security-2018/

IRAM2. 2017. The next generation of assessing information risk. Viitattu 22.3.2020. https://www.isflive.org/sfc/servlet.shepherd/document/download/0690J000005OwvpQAC

Kamensky, M. 2014. Strateginen johtaminen. Menestyksen timantti. E-kirja. Helsinki: Talentum. Viitattu 3.5.2020. https://bisneskirjasto-almatalent-fi.ezproxy.jamk.fi:2443/teos/DAJBBXXTBBAED#kohta:STRATEGINEN((20)JOHTAMINEN((20)Menestyksen((20)timantti((20)/piste:b4

Kananen, J. 2013. Case-tutkimus opinnäytetyönä. Jyväskylä: Jyväskylän ammattikorkeakoulu

Kananen, J. 2014. Laadullinen tutkimus opinnäytetyönä. Jyväskylä: Jyväskylän ammattikorkeakoulu. Viitattu 1.3.2020. https://www-booky-fi.ezproxy.jamk.fi:2443/lainaa/1049

Kiely L. & Benzel T. 2006. Systemic Security Management: A new conceptual framework for understanding the issues, inviting dialogue and debate, and identifying future research needs. IEEE Security and Privacy Magazine 4(6):74-77. Viitattu 25.4.2020. https://www.researchgate.net/publication/3437849_Systemic_Security_Management

Lindroos, J.-E. & Lohivesi, K. 2004. Onnistu strategiassa. Helsinki: WSOY

Mckeown, M. 2015. The Strategy Book. 2. p. FT Publishng International. Viitattu 18.8.2019. https://learning.oreilly.com/library/view/the-strategy-book/9781292084411/

Mitronen, L & Raikaslehto, T. 2019. Voittajan strategia. Lyhytjänteisyydestä kestävään menestykseen. E-kirja. Viitattu 4.5.2020. https://bisneskirjasto-almatalent-fi.ezproxy.jamk.fi:2443/teos/HAJBFXDTEB#kohta:((20)Voittajan((20)strategia

Framework for Improving Critical Infrastructure Cybersecurity. 2018. National Institute of Standards and Technology. Viitattu 25.4.2020

NIST Special Publication 800-30. 2012. Guide for Conducting Risk Assessments. Information Security. Viitattu 15.3.2020. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

NIST Special Publication 800-39. 2011. Managing Information Security Risk - Organization, Mission, and Information System View. Information Security. Viitattu 13.4.2020. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

NIST Special Publication 800-53 Rev. 4. 2013. Security and Privacy Controls for Federal Information Systems and Organizations. Viitattu 13.4.2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

NIST Special Publication 800-160 Volume 2. 2019. Developing Cyber Resilient Systems: A Systems Security Engineering Approach. Viitattu 3.5.2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2.pdf

Pienet ja keskisuuret yritykset. N.d. Käsitemäärittely Tilastokeskuksen sivustolla. Viitattu 1.3.2020. https://www.stat.fi/meta/kas/pienet_ja_keski.html

Porvari, P. 2012. Tietoturvallisuus liiketoiminnan johtamisessa, prosesseissa ja henkilöiden toiminnassa. Espoo: Sähkötekniikan korkeakoulu

RFC 2828. 2000. Internet Security Glossary. The Internet Society. Viitattu 26.4.2020. https://www.ietf.org/rfc/rfc2828.txt

Seitamaa-Hakkarainen, P. N.d. Kvalitatiivinen sisällönanalyysi. Viitattu 9.5.2020. https://metodix.fi/2014/05/19/seitamaa-hakkarainen-kvalitatiivinen-sisallon-analyysi/

SFS-EN ISO/IEC 27002:2017. Tietoturvallisuuden hallintakeinojen menettelyohjeet. Aihealueet: Informaatioteknologia, turvallisuus. Helsinki: Suomen Standardoimisliitto SFS. Vahvistettu 3.3.2017.

SFS-ISO/IEC 27003:2017. Ohjeistusta. Aihealueet: Informaatioteknologia, turvallisuustekniikat, tietoturvallisuuden hallintajärjestelmät. Helsinki: Suomen Standardoimisliitto SFS. Vahvistettu 10.11.2017.

Sillanpää, A. & Roivainen, H. & Lehto, M. 2015. Finnish Cyber Security Strategy and Implementation. Julkaisussa Cyber Security: Analytics, Technology and Automation. Toim. M. Lehto & P. Neittaanmäki. Springer International Publishing Switzerland, 129-144. Intelligent Systems, Control and Automation: Science and Engineering Volume 78.

Sydänmaanlakka, P. 2015. Älykäs julkinen johtaminen. E-kirja. Alma Talent Oy ja Pentti Sydänmaanlakka. Viitattu 17.8.2019. https://bisneskirjasto-almatalent-fi.ezproxy.jamk.fi:2443/teos/BAXBBXATFBCEC#kohta:((c4)LYK((c4)S((20)JULKINEN((20)JOHTAMINEN((20)

The Standard of Good Practice for Information Security. 2018. Information Security Forum Limited.

Tuomi, J. & Sarajärvi, A. 2018. Laadullinen tutkimus ja sisällön analyysi. E-kirja. Helsinki: Tammi. Viitattu 9.5.2020. https://www.ellibslibrary.com/jamk/9789520400118

Valtionhallinnon tietoturvallisuuden johtoryhmä. 2010. Vahti 2/2010 - Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta. Helsinki: Valtiovarainministeriö. Viitattu 18.4.2020. https://www.vahtiohje.fi/c/document_library/get_file?uuid=b4a90e50-7307-4004-ac8e-b9103220db6a&groupId=10128&groupId=10229

Valtionhallinnon tietoturvasanasto. 2008. Helsinki: Valtiovarainministeriö. Viitattu 12.4.2020. https://www.vahtiohje.fi/c/document_library/get_file?uuid=7e2220f1-cc93-4ba6-8c70-a67869c526cc&groupId=10229

Viitala, R. & Jylhä, E. 2019. Johtaminen: Keskeiset käsitteet, teoriat ja trendit. E-kirja. Helsinki: Edita. Viitattu 8.5.2020. https://www.el-libslibrary.com/jamk/9789513776077

Vuorinen, T. 2013. Strategiakirja - 20 Työkalua. E-kirja. Helsinki: Talentum. Viitattu 3.5.2020. https://bisneskirjasto-almatalent-fi.ezproxy.jamk.fi:2443/teos/CACBEXDTEB#kohta:STRATEGIAKIRJA((20)-((20)20((20)TY((d6)KALUA((20)

Yrittäjyys Suomessa. 2020. Artikkeli Suomen yrittäjien verkkosivustolla. Viitattu 1.3.2020. https://www.yrittajat.fi/suomen-yrittajat/yrittajyys-suomessa-316363

Liitteet

Liite 1. Tietojen keruun ja analyysivaiheen analysointimenetelmiä

Ympäristöanalyysi

Toimintaympäristössä tapahtuvia muutoksia tulisi kirjata ylös jatkuvana työnä. Mahdollisen strategiaprosessin alkaessa on tämän kerätyn tiedon pohjalta mahdollista tehdä arvioita muutosten vaikutuksesta organisaation liiketoimintaan. (Lindroos & Lohivesi 2004, 24.)

Muutoksen vaikutus / Muutoksen kuvaus	Vaikutus toiminnalle	Vaikutus tarjontaan	Vaikutus asiakkaisiin	Vaikutus osaamistarpeisiin	Vaikutus tietotekniikkaan	Muutoksen ajoitus	Kenen vastuulla valmistella toimenpiteet
	1=pieni - 5=suuri					Vuosi / Kuukausi	Vastuuhenkilö

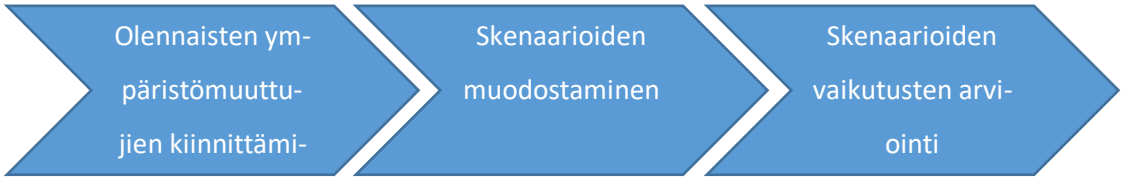
Kuvio 18. Toimintaympäristön muutosten analyysi (Lindroos & Lohivesi 2004, 214)

Toimintaympäristön muutokset vaikuttavat yleensä moneen eri asiaan. Ympäristöanalyysillä tavoitellaan parempia valmiuksia kohdata muutoksia ennen niistä seuraavia muutoksia toimintaan. Analyysin avulla pyritään tunnistamaan mihin muutokset

organisaation toiminnassa vaikuttavat, miten merkittävät vaikutus on ja mikä on muutoksen ajankohta. (Lindroos & Lohivesi 2004, 213.)

Skenaarioanalyysi

Nopeasti muuttuvassa tai vaikeasti ennakoitavassa toimintaympäristössä voidaan tulevaisuutta yrittää analysoida skenaariomenetelmän avulla. Toimintaympäristön muutokset voivat olla seuratusta esimerkiksi globalisoitumisesta, digitalisaatiosta tai teknologisesta läpimurrosta, jolloin organisaatiolle voi tulla kokonaan uusia kilpailijoita tai sen pitää pystyä itse toimimaan täysin uusissa kanavissa. (Lindroos & Lohivesi 2004, 33.) Skenaariot ovat ikään kuin tulevaisuuden käsikirjoitus tai mahdollisten tapahtumaketjujen kuvaus, joiden avulla tarkastellaan vaihtoehtoisia tulevaisuuksia. Skenaariot auttavat strategisissa valinnoissa ja päätöksenteossa ja niiden on tarkoitus lisätä joustavuutta sekä valmiutta varautua samanaikaisesti useampiin tulevaisuuksiin (Vuorinen 2013, 109-110).



Kuvio 19. Skenaarioprosessin vaiheet (Lindroos & Lohivesi 2004, 216)

Skenaarion peruselementit ovat nykytilan kuvaus, tulevaisuuden kuvaus ja kuvaus prosessista, joka liittää kaksi edellä mainittua toisiinsa (Vuorinen 2013, 110). Skenaarioanalyysissä rakennetaan useita (3-5 kpl) toisistaan täysin eroavia tulevaisuuden kuvia, siten ettei lähtökohtana ei ole arvioida tai painottaa yksittäisten skenaarioiden

toteutumisen todennäköisyyttä vaan jokaista skenaariota kohdellaan samanvertaisena mahdollisena tulevaisuuden tilana. Kehitettyjen skenaarioiden pohjalta arvioidaan miten organisaation tulisi toimia, jos tulevaisuuden toimintaympäristö olisi skenaarion mukainen. Kutakin skenaariota käsitellään analyysissä itsenäisesti toisista riippumatta. Skenaarioanalyysin etuna on, että tällöin kyetään paremmin havaitsemaan oman strategian kriittiset kohdat sekä ne seikat, jotka nousevat vuorollaan toisia tärkeämmiksi toimintaympäristössä. Skenaariotyöskentelyn avulla tarkastellaan millä tavoin strategialinjausten on muututtava toimintaympäristön suurten muutosten yhteydessä. Tämä työskentelytapa voidaan nähdä myös riskienhallinnallisena työkaluna, kun tuleviin muutoksiin on varauduttu ennakolta. Skenaarioanalyysi ei pyri ennustamaan tulevaisuutta vaan se pyrkii nostamaan esiin ne seikat, jotka tulisi huomioida ja miten organisaation tulisi toimia erilaisissa vaihtoehtoisissa tulevaisuuden tiloissa. Skenaariot itsessään ovat malleja tai kuvauksia näistä tiloista. (Lindroos & Lohivesi 2004, 215-216.)

SWOT-analyysi

SWOT-analyysin avulla organisaatio voi tarkastella niin oman toimintansa kuin kilpailijoidenkin vahvuuksia, heikkouksia, mahdollisuuksia ja uhkia (Lindroos & Lohivesi 2004, 35). Luonteeltaan SWOT on kokoava synteesin omainen analyysi, jolla on tarkoitus tuottaa kokonaisnäkemys vallitsevasta tilanteesta strategisten valintojen pohjaksi (Vuorinen 2013, 88).

Kuvio 20. SWOT-analyysi

SWOT-analyysin avulla voidaan tarkastella omaa toimintaa kokonaisuutena tai osia siitä esimerkiksi jonkun tuotteen tai palvelun näkökulmasta. Analyysin avulla voidaan myös tarkastella esimerkiksi jonkun kilpailijan toimintaa ja kilpailukykyä. (Lindroos ja Lohivesi 2004, 217.) Analyysin tekemisen aikana saatetaan huomata, että samat asiat voivat olla sekä vahvuuksia, heikkouksia, mahdollisuuksia että uhkia (Vuorinen 2013, 89). Yleinen haaste menetelmän käytössä on sekä nykytilaan että tulevaisuuteen liittyvien arviointien tekeminen. Ratkaisuna voidaan käyttää kahden SWOT-taulukon tekemistä, joista toinen kuvaa nykytilaa ja toinen tulevaisuutta. Näin toimimalla voi selkeämmin saada esille omaan toimintaan merkittävästi vaikuttavat asiat. SWOT-analyysin lopputulemana voi olla suunnitelma siitä, miten vahvuuksia voidaan hyödyntää, kuinka heikkoudet muutetaan vahvuuksiksi, miten mahdollisuuksia hyödynnetään ja miten uhat torjutaan. (Lindroos ja Lohivesi 2004, 217-218.)

Sidosryhmäanalyysi

Sidosryhmien odotukset vaihtelevat ajan myötä. Sidosryhmiä löytyy organisaation omasta henkilöstöstä, ulkoisista kumppaneista ja viranomaisista. Yrityksen asiakkaita ei yleensä tarkastella sidosryhmänä, sillä he ja heidän tarpeensa on koko liiketoiminnan perusta. Sidosryhmien odotusten analyyseja voi tehdä esimerkiksi haastatteluiden tai kyselytutkimusten avulla. Sidosryhmien odotusten muutoksista tulee kerätä dokumentoitua tietoa ja pitää tämä tieto tarvittavien henkilöiden saatavilla. Strategiaprosessin yhteydessä tulee käsitellä sidosryhmissä tapahtuvat muutokset ja arvioida muutosten merkitys strategiaan. (Lindroos & Lohivesi 2004, 41.)

Sidosryhmien odotuksiin voivat vaikuttaa lait, säädökset, kilpailutilanne, jakelu-, myynti- ja palvelukanavien kehitys, yhteistyökumppanit, toimittajasuhteet sekä henkilökunnan odotukset. Sidosryhmien odotusten huomioiminen on tärkeässä asemassa mutta näihin liittyvien muutosten huomiointi on haastavaa työnohessa. Muutokset sidosryhmissä tai heidän odotuksissaan voivat vaikuttaa merkittävästikin organisaation toimintaan. (Lindroos & Lohivesi 2004, 233).

Organisaation valmiusanalyysi

Lindroosin ja Lohiveden mukaan myös oman organisaation lähtötietojen kartoittaminen on tärkeää, sillä näiden tietojen avulla on helpompi täsmentää strategiatyössä tarvittavia toimenpiteitä ja helpottaa strategian toimeenpanoa. (Lindroos ja Lohivesi 2004, 42).

Organisaation valmiusanalyysin avulla pyritään kartoittamaan yrityksen valmiudet toimia erilaisissa tilanteissa. Analyysi voidaan tehdä taulukon avulla, jossa valmiudet on jaettu osa-alueittain ja jokaisen osa-alueen nykytilanne arvioidaan asteikolla 1-10. Lisäksi arvioidaan kunkin osa-alueen tärkeys strategian kannalta asteikolla 1-5. Analyysin lopputuloksena saadaan 2-3 eniten lisäpanostuksia vaativaa osa-aluetta. Lisäksi tunnistetaan vähemmän tärkeät tai nyt jo riittävällä tasolla olevat osa-alueet. Tavoitteena on löytää ne muutamat osa-alueet, joita tulisi kehittää seuraavan strategiakauden aikana. (Lindroos & Lohivesi 2004, 235.)

Organisaation valmiudet	Mistä on kysymys	Arvio 0-10	Tärkeys 1-5
Tahto	Henkilökuntamme on motivoitunutta, osaavaa ja sitoutunutta		
Nopeus	Osaamme viedä läpi tärkeitä muutoksia nopeasti		
Kulttuuri ja identiteetti	Asiakkaillamme on henkilöstöstämme positiivinen ja yhtenäinen kuva ja kokemus		
Vastuunkanto	Henkilökuntamme on valmis ottamaan vastuun hyvän tuloksen aikaansaamisesta		
Yhteistyökyky	Teemme tarvittaessa yhteistyötä yli rajojen varmistaaksemme tehokkaan toiminnan		
Oppiminen	Olemme hyviä ideoimaan sellaisia uusia asioita, joilla on merkitystä toimintamme ja tavoitteidemme kannalta		
Johtajuus	Osaamme sijoittaa kykeneviä johtajia tärkeisiin tehtäviin		
Asiakas-kontaktit	Meillä on kestävät ja molemmin puolin luotettavat suhteet keskeisten asiakkaiden kanssa		
Strateginen yhtenäisyys	Olemme hyviä kiteyttämän ja toteuttamaan strategisen näkemyksen		
Innovatiivisuus	Kykenemme uudistumaan sekä sisällöllisesti että toimintaprosessiemme suhteen hyvin		
Tehokkuus	Olemme kustannustehokkaita		

Kuvio 21. Esimerkki organisaation valmiusanalyysistä (Lindroos & Lohivesi 2004, 236).

Benchmarking

Yksi organisaation valmiutta ja nykytilaa mittaava menetelmä on benchmarking eli esikuva-analyysi tai vertailukehittäminen on menetelmä, jossa pyritään oppimaan systemaattisesti hyviltä esikuvilta. Tavoitteena on saada toisilta organisaatioilta tietoja ja taitoja, joita voidaan hyödyntää oman organisaation toiminnassa. Benchmarking toteutetaan vertaamalla omaa toimintaa valitulla aihealueella kyseisessä asiassa huppuluokkaa edustaviin toimijoihin. Benchmarkingin ideana ei ole toisen organisaation kopiointi vaan toisilta opittujen asioiden tuominen ja soveltaminen omaan organisaatioon. Prosessi alkaa organisaation omien kehitystarpeiden tunnistamisella ja nykytilan mahdollisimman tarkalla kuvauksella. Tämän jälkeen pitää löytää vertailukohde ja tarvittaessa päästä tämän kanssa yhteistyöhön. Vertailukohteen löytymisen jälkeen pyritään tuomaan esille toiminnan keskeiset erot ja tämän jälkeen yritetään löytää syyt erojen taustalla. (Vuorinen 2013, 158-161.)

Liite 2. Teemahaastattelurunko

Strategian merkitys tietoturvan johtamisessa

Teemahaastattelurunko

Henri Heinonen, YTJ17S1

Opinnäytetyön teemahaastattelu
Tekniikan ja liikenteen ala
2020

Yrityksen taustatiedot

Haastattelu nro:

Yrityksen toimiala:

Liikevaihto:

Henkilöstö:

Teemahaastattelun toteutus

Haastattelija: Henri Heinonen

Ajankohta: pp.kk.vvvv klo xx:xx

Kesto:

Asema yrityksessä:

Teemat

Teema 1 – Tietoturvallisuuden strategisen johtamisen ilmentyminen organisaatiossa

Teema 2 – Merkityksellinen tietoturvastrategia

Teema 3 - Tietoturvallisuuden vision ja mission on määrittely

Teema 4 – Strategiaprosessi

- Strategisten tietojen keruun ja analysinnoin järjestäminen
- Strategian määrittelyvaihe
- Strategisten projektien suunnitteluvaihe
- Strategisten projektien toteutus
- Seuranta, arviointi ja päivitys