# ONNISTUNEEN TIETOTURVASTRATEGIAN EDELLYTYKSET

Prerequisites of a Successful Information Assurance Strategy

Lappeenrannan–Lahden teknillinen yliopisto LUT

Tuotantotalouden kandidaatintyö

2023

Kreetta Härkönen

Tarkastaja: Tutkijaopettaja Lea Hannola

TIIVISTELMÄ

Lappeenrannan–Lahden teknillinen yliopisto LUT
LUT Teknis-luonnontieteellinen
Tuotantotalous

Kreetta Härkönen

**ONNISTUNEEN TIETOTURVASTRATEGIAN EDELLYTYKSET**

Tuotantotalouden kandidaatintyö
2023
34 sivua, 3 kuvaa, 1 taulukko
Tarkastaja: Tutkijaopettaja Lea Hannola
Avainsanat: tietoturva, tietoturvastrategia, tietoturvaloukkaus, tieto-omaisuus, strateginen suunnittelu, johtoryhmätyöskentely
Keywords: information assurance, information assurance strategy, information security breach, information assets, strategic planning, executive management

Tietoturva pyrkii ehkäisemään tapahtumia, jotka voivat vahingoittaa yhtä yrityksen tärkeintä omaisuusluokkaa eli tieto-omaisuutta. Tämän kirjallisuuskatsauksena toteutetun kandidaatintyön tavoitteena on selvittää tärkeimmät menestystekijät onnistuneen tietoturvastrategian taustalla suurissa ja keskisuurissa yrityksissä. Työssä käsitellään ylimmän johdon roolia strategiaprosessissa, tieto-omaisuuden merkitystä yritykselle ja siihen yleisimmin kohdistuvia uhkia. Lisäksi tarkastellaan tietoturvastrategian sisältöä, suunnittelua ja implementointia käytännössä. Lopuksi määritellään menestystekijät sekä yleisimmät haasteet tietoturvastrategian toteuttamisessa.

Työssä havaittiin, että yrityksen ylimmän johdon sitoutumisen vaikutus on kiistämätön tietoturvastrategian onnistumiseen. Tärkeiksi menestystekijöiksi huomattiin myös tietoturva- ja yritysstrategian yhteensopivuus, selkeät tietoturvakäytännöt ja niihin liittyvä koulutus, sekä onnistumisen seuraaminen eri mittarein. Johtopäätöksenä voidaan todeta, että tietoturvastrategian muodostaminen ja implementointi on merkittävä askel kohti tietoturvallisempaa toimintaa. Pelkät teknologiset suojaukset eivät riitä tietoturvahyökkäysten kehittyessä, jolloin tietoturvastrategian tarjoamaa kokonaisvaltaista lähestymistapaa voidaan hyödyntää uhkien minimoimiseen.

**Sisällysluettelo**

# 1 Johdanto

Tiedonhallinta ja -käsittely toimii nykyisin yritysten liiketoiminnan mahdollistajana, eikä enää vain sen tukitoimintona. Tämä on saanut yritykset alttiiksi aivan uudenlaisille riskeille, jossa uhattuna on yrityksen omistama data ja tieto – eli tieto-omaisuus. Koska tieto-omaisuus on vahvasti läsnä yrityksen ydintoiminnoissa, tulee sitä käsitellä muiden strategisten kysymysten rinnalla – yrityksen ylimmässä johdossa. (Whitman 2019, 3; Kyberturvallisuuskeskus 2020, 3) Yritykset ovat pitkään nähneet tietoturvan vain teknologisena kysymyksenä, mutta nykypäivänä tutkimus kehottaa yrityksiä kokonaisvaltaisempaan lähestymistapaan. Tämä edellyttää tietoturvastrategian muodostamista, tietoturvahallinnon organisointia ja tietoturva-asiantuntijoiden nimeämistä. (Soomro et al. 2016, 215) Julkisuuteen tulleet huonosti hoidetut tietoturvaloukkaukset aiheuttavat yritykselle myös merkittävää mainehaittaa, jonka lopullinen vaikutus nähdään yrityksen liiketoimintatuloksessa.

## 1.1 Työn tavoitteet ja tutkimuskysymykset

Tutkimuksen tavoitteena on selvittää, mitä tekijöitä onnistuneen tietoturvastrategian ja sen implementoinnin taustalta löytyy. Aiheen käsittely strategisella tasolla johtaa myös pohtimaan, mikä ylimmän johdon rooli tietoturvastrategian onnistumisessa on. Tavoitteena on avata myös syitä, miksi tietoturvastrategia on tärkeä olla olemassa. Kandidaatintyön päätutkimuskysymys on:

*”Mitkä ovat tekijät onnistuneen tietoturvastrategian taustalla?”*

Päätutkimuskysymyksen lisäksi työn osakysymyksiä ovat:

*”Mikä on ylimmän johdon rooli tietoturvastrategian onnistumisessa?”*

*”Miksi tietoturvastrategian kehittäminen on tärkeää?”*

## 1.2 Työn tutkimusmenetelmät ja aiheen rajaus

Tämä kandidaatintyö toteutetaan kirjallisuuskatsauksena, joka rakentuu aiheesta julkaistuihin tieteellisiin artikkeleihin ja ammattikirjallisuuteen. Artikkeleita ja kirjallisuutta etsiessä on hyödynnetty pääasiassa LUT Primoa sekä Google Scholaria. Aiheeseen tutustuminen aloitettiin ammattikirjallisuuden kautta. Ammattikirjallisuus tässä tapauksessa tarkoittaa tietoturva-alan asiantuntijoille tarkoitettuja kirjoja, joissa ammatinkuvan läpikäymisen lisäksi syvennytään tietoturvan termeihin, vaatimuksiin ja asemoitumiseen suhteessa yrityksen muihin liiketoiminta-alueisiin. Termien tullessa tutuksi ja yritysten tietoturvan kokonaiskuvan hahmottuessa oli helpompi lähteä etsimään tieteellisiä julkaisuja aiheeseen liittyen.

Työn keskeisin teema on onnistumisen ajurit yrityksen tietoturvastrategian takana. Aihetta pohjustetaan käsittelemällä strategian ja tietoturvan teoriaa työn kannalta soveltuvin osin. Työn tavoitteena on löytää edellytykset strategian onnistumiseen, jonka takia strategiaprosessin teoreettinen käsittely keskittyy tarkastelemaan suunnittelua ja hallintoa, sekä miten strategia näkyy yrityksen toiminnan tasolla. Työn pääpaino on tutkia tietoturvastrategian merkitystä tietoturvaloukkausten ehkäisemisessä, ja aikaan tietoturvaloukkauksen jälkeen ei keskitytä. Työ on rajattu koskemaan suuria ja keskisuuria pörssiyrityksiä, sillä tutkimusaineistossa käsitellyt yritykset olivat suurelta osin näitä, eikä pienten yritysten voida olettaakaan näkevän erillisen tietoturvastrategian kehittämistä järkevänä olemassa olevien resurssien puitteissa.

## 1.3 Työn rakenne

Tutkimus sisältää viisi päälukua: johdannon, kolme teoriakappaletta ja johtopäätökset. Johdanto toimii orientaationa aiheeseen, sekä kertoo tutkimuksen tavoitteista ja siitä, miksi aihe on ajankohtainen. Teoriakappaleissa liikkeelle lähdetään laajimmasta aiheesta, ja ensimmäisenä määritellään yrityksen strategia, ylimmän johdon roolin strategiatyössä sekä strategisen suunnittelun periaatteet. Toinen teoriakappale käsittelee tietoturvaa ja sen peruskäsitteitä. Kappale käsittelee tietoturvaa myös yrityksen kontekstissa ja täsmentää tieto-omaisuuden käsitteen, sekä sen kohtaamat uhat ja merkityksen yritykselle. Kolmas teoriakappale yhdistää strategian ja tietoturvan. Kappaleessa käydään yleisesti läpi yrityksen tietoturvastrategian

sisältöä ja merkitystä, miten se konkretisoituu, sekä etsitään menestystekijät onnistuneen tietoturvastrategian takana. Kolmannessa kappaleessa sivutaan myös tietoturvastrategian muodostamisen yleisimpiä kompastuskiviä. Viimeinen kappale vastaa tutkimuskysymyksiin ja kertoo johtopäätökset työn tuloksista.

# 2 Strategia

Strategia terminä on verrattain abstrakti ja sen määrittelyyn vaikuttaa konteksti, missä strategiasta puhutaan. Ennen onnistuneen tietoturvastrategian käsittelyä, on syytä tarkastella strategian määritelmää, sen merkitystä liiketoiminnalle, strategista suunnittelua ja yrityksen ylimmän johdon roolia strategiaprosessissa.

## 2.1 Strategian määrittely ja merkitys liiketoiminnalle

Sana *strategia* juontaa juurensa muinaiseen kreikan kieleen sanoista ylipäällikölle (*strategos*) ja sotapäällikkyydelle *(strategia)*, näin liittäen termin historialliset juuret vahvasti sodankäyntiin ja armeijan kontekstiin (Kerttunen, 2007). Käsitteenä strategia ei siis ole uusi, mutta liiketoimintaan strategiaopit ovat levittäytyneet vasta 1900-luvun puolella, ensin taloudellisten tavoitteiden saavuttamiseen, vähitellen myös laajemmin organisaatioiden kokonaisvaltaisten päämäärien ja kauaskantoisen suunnitelman sanoittamiseen (Kamensky, 2015; Kerttunen, 2007).

Strategiatutkimukseen ja -kirjallisuuteen voimakkaasti vaikuttanut yhdysvaltalainen professori M. E. Porter (1996, 43) tiivistää strategian olevan liiketoiminnallisesti ainutlaatuisen ja arvokkaan aseman luomista kilpailijoihin nähden, joka saavutetaan suunniteltujen toimintojen avulla. Päätöksentekotilanteessa strategian tulisi ainakin rajata, mitä yritys ei lähde tekemään (Porter 1996, 45). Strategia voidaan ajatella kivijalkana, jonka pohjalta yrityksen päätökset tehdään. Tietyn asian tekeminen tai tekemättä jättäminen tulisi olla perusteltavissa ja linjassa strategian kanssa. Yksinkertaisimmillaan strategian voi tiivistää toimintaa edeltäväksi tietoiseksi suunnitelmaksi (Mintzberg 1987, 11).

Perinteistä, Yhdysvalloista lähtöisin olevaa strategiatutkimusta on myös kritisoitu ja nähty sen typistävän strategian pelkästään rationaaliseksi prosessiksi, jonka suunnittelussa yrityksen johdolla on ehdoton valta (Rouleau & Cloutier 2022; Clegg et al. 2004, 21). Strategia nähdään päättävänä, ohjaavana ja älyllisenä elimenä — aivoina, jonka täydellisessä ohjauksessa ”vartalo”, eli organisaation tai yrityksen konkreettinen toiminta on (Clegg et al. 2004,

21). Vastareaktiona näihin puutteisiin on strategian tutkimuskentällä parin viimeisen vuosikymmenen aikana noussut erilainen näkökulma: *strategy-as-practise* (SaaP) (Rouleau & Cloutier, 2022). Sen sijaan, että strategia on jotain, mitä yrityksellä on, tarkastelee SaaP strategiaa jonakin, mitä yritys tekee (Kolttola et al. 2010). SaaP korostaa, että strategian kehittäminen on jatkuvaa, käytännön toimintaa, joka vaatii tiimityötä, tietoa ja kokemusta organisaation sisältä. Strategian nähdään konkretisoituvan juuri koko henkilöstön aktiivisena toimintana, ei vaan johdon suunnitelmana, jonka perusteella organisaatio toimii. (Whittington 2007, 1578)

Tämän työn kontekstissa strategia määritellään suunnitelmaksi, jonka yritys tai organisaatio laatii saavuttaakseen tiettyjä tavoitteita tai päämääriä. Strategian suunnittelussa tehdään valintoja ja kohdennetaan resursseja halutun lopputuloksen saavuttamiseksi, ottaen huomioon sisäiset ja ulkoiset tekijät, jotka voivat vaikuttaa suunnitelman onnistumiseen. Strategia on keskeinen osa yrityksen tai organisaation päätöksentekoa ja tarjoaa viitekehyksen toimintojen ohjaamiseen yhteisen tavoitteen saavuttamiseksi, toisin sanoen menestymiselle. (Kamensky 2015) Määrittely on lähempänä perinteistä strategiatutkimusta, koska se on mielekkäämpää ja konkreettisempaa tämän kandidaatintyön kannalta.

## 2.2 Strateginen suunnittelu

Whitmanin (2019, 126) mukaan: ”*Suunnittelu on modernien organisaatioiden vallitseva tapa hallita resursseja.*” Strateginen suunnittelu tarjoaa yritykselle systemaattisen, analyyttisen ja harkitun lähestymisen strategian muodostamiseen samalla kirkastaen yritykselle sen prioriteetteja ja toimintaympäristöä (George et al. 2019, 816). Strategista suunnittelua on myös kritisoitu sen keskittymisestä liikaa strategisiin tavoitteisiin, jättäen strategian itseasiallisen toteuttamisen keinot vähemmälle huomiolle (Kamensky 2015). Kuitenkin George et al. (2019, 816) huomasivat strategisen suunnittelun vaikuttavan positiivisesti yrityksen liiketoimintatulokseen, edellyttäen että tausta-analyysit ja suunnitelmavaihtoehtojen kartoitus on tehty kattavasti. Strategista suunnittelua voidaan siis pitää tärkeänä tekijänä strategiatyön onnistumisen taustalla, muita strategisia työkaluja unohtamatta (Kamensky 2015).

Suunnitteluun lähdetään yrityksen aiemmin kehitetystä eettisestä, liiketoiminnallisesta sekä filosofisesta näkökulmasta, joka on kiteytetty yrityksen toiminta-ajatukseen, visioon ja

arvoihin (Whitman 2019, 126). Näiden pohjalta yrityksen täytyy lähteä perusteellisesti analysoimaan sisäistä ja ulkoista toimintaympäristöään, sekä muodostamaan tavoitteitansa. Analyysin pohjalta luodaan strategiavaihtoehtoja, joista huolellisen harkinnan jälkeen valitaan olennaisimmat ja joiden pitkällä aikavälillä nähdään vievän yritystä kohti tavoitetilaansa. (George et al. 2019, 817) Strateginen suunnittelu asettaa suunnan yleensä vähintään seuraavalle viidelle vuodelle, eikä sen vuoksi mene yksityiskohtien tasolle, sillä toimintaympäristöä on mahdotonta ennustaa monen vuoden päähän (Whitman 2019, 133).

Whitman (2019, 47) jakaa strategisen suunnittelun kattokäsitteen vielä taktiseen ja operationaaliseen tasoon. **Taktinen suunnittelu** luo osastokohtaiset puitteet seuraavalle 1–3 vuodelle ja sisältää suunnitelman, mihin osaston saamia resursseja, kuten rahaa ja työntekijöitä, on tarkoitus käyttää mainitun ajanjakson aikana. **Operationaalinen suunnittelu** pohjautuu taktisiin suunnitelmiin ja on aikahorisontiltaan lyhyin. Operationaaliset suunnitelmat auttavat päivittäisten tehtävien organisoinnissa ja sisältävät esimerkiksi kuvauksia toiminnan kannalta kriittisistä työtehtävistä ja viikoittaisista tapaamisista. Näillä tasoilla strategia konkretisoituu: suunnitelmien tulee sisältää yksityiskohtia – lukuja, päivämääriä ja toimintatapoja, joille ylemmän tason strateginen suunnitelma on antanut vain raamit (Whitman 2019, 133)

## 2.3 Hallitus- ja johtoryhmätyöskentely strategiatyössä

Tämä kappale avaa, mikä rooli yrityksen hallitus- ja johtoryhmätyöskentelyllä on strategiatyössä. Hallitus- ja johtoryhmätyöskentely on hyvin yleinen johtamismalli suurissa ja keskisuurissa yrityksissä (Kamensky 2015). Yrityksen osakkeenomistajat valitsevat yhtiökokouksessa hallituksen, joka toimii yrityksen ylimpänä johtoelimenä. Yrityksen hallitus nimittää toimitusjohtajan, joka hallinnoi yritystä ja on raportointivastuussa hallitukselle. Suuressa osassa suuria ja keskisuuria yrityksiä on johtoryhmä, joka koostuu yrityksen liiketoiminta-alueiden ja strategisten tukitoimintojen (talous, henkilöstö, viestintä, IT) päälliköistä. Johtoryhmän tehtävänä on tukea yrityksen toimitusjohtajaa toiminnan suunnittelussa ja päätöksissä. (Hallinnointikoodi 2020, 11) Tässä työssä viitataan yrityksen hallituksen ja johtoryhmän, toimitusjohtajan mukaan lukien, muodostamaan johtoelimeen termillä yrityksen ylin johto.

Kamensky (2015) kertoo hallituksen työkentän liittyvän ennen kaikkea yrityksen strategiaan ja tiivistää hallituksen tärkeimmiksi tehtäviksi:

- strategiatyön perustan, eli **toiminta-ajatuksen, vision ja arvojen määrittäminen**
- strategisten **tavoitteiden määrittäminen** yrityksen osakkeenomistajien etujen mukaisesti
- **osallistuminen ja vaihtoehtojen haastaminen** – oman näkemyksen ja ideoiden esiintuominen, sparraus, sekä strategian valintaan vaikuttavien olettamuksien kyseenalaistaminen
- strategian lopullinen **hyväksyminen**
- strategian **juurruttaminen** koko yritykseen hallitustyöskentelijöiden oman esimerkillisen käyttäytymisen kautta

Kamensky (2015) ja Valpola (2021, 32–46) kertovat johtoryhmän vastuita olevan:

- **strategian suunnittelu**
- **diagnoosi:**
    - **toimiala-analyysi** – ulkoisten mahdollisuuksien ja uhkien kartoittaminen
    - **sisäisten kyvykkyyksien analyysit** – esimerkiksi taloudellisen tilanteen tunnusluvut sekä henkilöstön osaaminen ja tyytyväisyys
    - **asemoituminen** toimialan kilpailijoihin nähden
- **strategiavaihtoehtojen muodostaminen** ja lopullisen strategian **kiteyttäminen**
- **strategian toteuttaminen** – yrityksen yhteisten käytäntöjen, toimintaperiaatteiden ja toimenpiteiden linjaaminen

Johtoryhmätyöskentelyn etu on, että yhdessä suoritettu suunnittelu yhdenmukaistaa liiketoiminta-alueiden tavoitteita, toimintoja ja toimintatapoja. Lisäksi johtoryhmätyöskentely tuo keskusteluun monipuolisia taitoja ja näkökulmia, mitä liiketoiminta-alueilla yksistään ei välttämättä olisi. Jotta työtavasta saadaan etua strategiatyöhön, tulee toiminnan olla yhteen hiileen puhaltamista, ei vain jokaisen johtoryhmän jäsenen oman liiketoimen edun ajamista muiden kustannuksella. (Kamensky 2015) Myöskään strategisen viestinnän tärkeyttä strategian jalkauttamisessa yritykseen ja sen työntekijöihin ei voida aliarvioida. Onnistuneen jalkauttamisen taustalta löytyy selkeä strategia, joka on helppo kertoa tarinallisesti, sekä

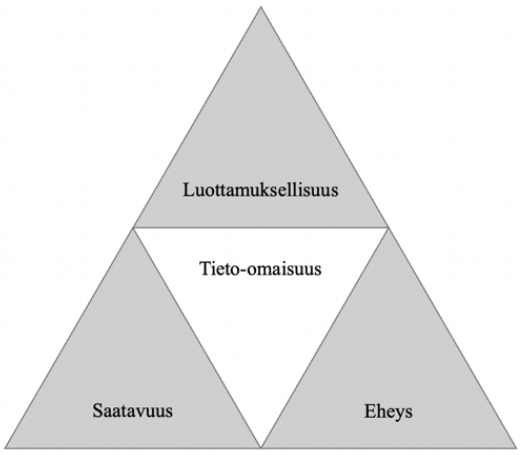
yrityksen ylimmän johdon yhteinen tahto ja sitoutuneisuus strategian viestintään ja toteuttamiseen. (Valpola 2021, 57)

# 3 Tietoturva

Sitä mukaa, kun tiedosta ja sen määrästä on tullut valuuttaa yhteiskunnassamme, on sen suojeleminen noussut myös yrityksien strategisiin intresseihin. Teknologia toimii yrityksien liiketoiminnan mahdollistajana, eikä enää vain sen tukitoimintona (Whitman 2019, 3). Toimintojen siirtyminen yhä voimakkaammin digitaalisille alustoille ja yrityksien kilpailuedun nivoutuminen teknologisiin ratkaisuihin altistaa yritykset ja organisaatiot aivan uusille riskeille, jonka vuoksi keskustelu tietoturvan merkityksestä on noussut hyvin ajankohtaiseksi aiheeksi (Kyberturvallisuuskeskus 2020, 3).

## 3.1 Tietoturvan ominaisuudet

Tietoturvan tavoite on säilyttää tiedon luottamuksellisuus (*confidentiality*), eheys (*integrity*) ja saatavuus (*availability*) (Whitman 2019, 7). Nämä kolme ominaisuutta muodostavat tietoturvan kolmiomallin, CIA-kolmion, joka on tietoturva-alalla ja -kirjallisuudessa laajasti hyväksytty ja käytössä oleva (Kuva 1.) (Samonas & Coss 2014, 21–22). CIA-kolmion ominaisuuksien turvaamisen lopullinen tavoite on suojella yrityksen tieto-omaisuutta – dataa ja tietoa, joka on tärkeää yrityksen menestyksen kannalta (Borek et al. 2013, 6). Tieto-omaisuutta käsitellään tarkemmin kohdassa 3.2.1.




*Kuva 1. CIA-kolmio (Campbell 2016, 6)*

**Luottamuksellisuus** tiedon ominaisuutena tarkoittaa, että tieto on saatavilla vain henkilöille ja systeemeille, jotka tarvitsevat sitä. Luottamuksellisuus edellyttää myös toimenpiteitä, joilla estetään pääsy tietoon niiltä, joilla ei ole siihen oikeutta tai tarvetta. (Whitman 2019, 8) Tieto on usein soveltuvaa ja sen tarkastelu tarpeellista vain tietyille henkilöille, jolloin saatavuuden rajaaminen on perusteltua. Rajaaminen voi johtua tiedon arkaluonteisuudesta ja sen leviäminen asiaankuulumattomien ihmisten käytettäviin saattaa johtaa epämieluisiin seurauksiin, kuten laillisiin kiistoihin tai rahallisiin sakkoihin. Tiedon tulisi olla saatavilla vain tarpeeseen ja valtuutetuille käyttäjille. (Alexander et al. 2020, 1–2)

Tieto on hyödyllistä vain, kun se on tarjolla kokonaisuudessaan, ehjänä ja paikkansapitävänä. Jotta tiedon **eheys** säilyy, tulee vain valtuutettujen ihmisten olla mahdollista muuttaa, päivittää tai poistaa tietoa. (Alexander et al. 2020, 2) Myös kysymykset vastuusta ja eettisyydestä voidaan käsittää kuuluviksi laajempaan määrittelyyn tiedon eheydestä. Eettisyys tässä kontekstissa tarkoittaa yleisesti hyväksyttyjen periaatteiden ja arvojen noudattamista, joita on kirjattu useisiin tietoturva-alan standardeihin ja kelvollisuusvaatimuksiin. (Samonas & Coss 2014, 33) On tärkeää tiedostaa, että tiedolla, koskipa se sitten henkilötietoja tai yrityssalaisuuksia, voidaan vahingoittaa niin yksilöitä kuin yrityksiä. Olipa epäeettinen toiminta seurausta piittaamattomuudesta, vahingosta tai tahallisuudesta, täytyy siitä olla seuraamuksia. (Whitman 2019, 73) Tietoturvaan liittyvässä kirjallisuudessa argumentoidaan vahvasti, että on johtotason vastuulla määrittää organisaatiossa eettisen toiminnan tärkeys sekä päättää noudattamattomuuden seuraamuksista, mikä motivoi henkilöstöä toimimaan oikein ja yleisesti hyväksytyn koodiston mukaan (Samonas & Coss 2014, 33–34).

**Saatavuus** tarkoittaa tehokasta ja luotettavaa pääsyä käytettävässä muodossa olevaan tietoon valtuutettujen käyttäjien sitä tarvitessa (Samonas & Coss 2014, 35). Tietoa, joka ei ole saatavilla tai käytettävässä muodossa silloin kun sitä tarvitaan, on vain dataa. Täydellinen tietoturva tarkoittaisi tiedon suojaamista esimerkiksi lukitsemalla tieto tallelokeroon, josta kukaan ei ikinä saisi sitä käsiinsä, joka on luonnollisesti täysin epäkäytännöllistä. Tästä syystä tietoturvan, sanan täydellisessä merkityksessä, ja tiedon saatavuuden välillä tulee aina tehdä kompromisseja. Saatavuus on tietoturvan ominaisuutena suhteellisen uusi ja sen merkitys korostuu entisestään, kun vaatimus yhä nopeammasta ja tehokkaammasta tiedonsaannista kasvaa. Haasteeksi onkin noussut saatavuuden parantaminen, kun toiminnan tietoturvallisuus halutaan samanaikaisesti säilyttää. (Alexander et al. 2020, 2)

CIA-kolmio on ytimekäs tiivistys tiedon ominaisuuksista, mutta sitä on kritisoitu yksipuolisesta näkökulmasta tietoturvaan vain teknisenä ongelmana. CIA-kolmion juuret pohjautuvat vahvasti armeijan ja valtion näkökulmaan turvallisuudesta, sillä alun perin tietokoneita ja niiden sisältämää tietoa uhkasivat samankaltaiset, ulkoiset uhkat. (Samonas & Coss 2014, 23) Mahdollisimman kattavan käsityksen saavuttamiseksi on tietoturvaan syytä liittää **kiistämättömyyden** (*non-repudiation*) ominaisuus. Tämä ominaisuus esiintyy CIA-kolmion rinnalla ja sitä on yhtä lailla harkittava, kun tietoturvan tilaa arvioidaan. Kiistämättömyys on todiste siitä, että väitetty kommunikaatio on tapahtunut, sekä kuka sen on aloittanut. Esimerkiksi vahingon sattuessa tiedon kiistämättömyys takaa, ettei kommunikaation alkuunpanija pysty jälkikäteen kiistämään, ettei ole toiminut yritystä vahingoittavalla tavalla. (Campbell 2016, 9)

## 3.2 Tieto ja sen turvaaminen yrityksissä

Tieto ja data on yrityksen valuuttaa, jota sen täytyy suojella varmistaakseen toiminnan jatkuvuus. Seuraavissa kappaleissa esitellään tieto osana yrityksen omaisuutta, sekä yleisimmät yrityksen tieto-omaisuuteen kohdistuvat uhat. Lisäksi sivutaan ulkoisia vaatimuksia ja yrityksen sisäisiä raameja tietoturvan toteuttamiseen.

### 3.2.1 Tieto omaisuutena

Maailmassa, jossa lähes kaiken voi ulkoistaa halvemmalle toimittajalle, ovat tieto ja henkinen pääoma usein yrityksen ainoat erottautumistekijät, kun muita perinteisiä markkinaesteitä ei ole olemassa. Tieto-omaisuus tulisikin käsittää strategisena voimavarana muiden omaisuusluokkien rinnalla ja tunnistaa se, jotta suojaamisen kohdistaminen on mahdollista. (Borek et al. 2013, 4–5; Hannila et al. 2022, 30, 36) Borek et al. (2013, 6) määrittelevät yrityksen tieto-omaisuudeksi datan ja tiedon, joka on tärkeää yrityksen menestyksen kannalta. Digitaalisen datan määrä on kasvanut eksponentiaalisesti vuosi toisensa jälkeen ja yritykset ovat suurenevissa määrin siitä riippuvaisia. Yrityksien haaste datan kanssa ei niinkään ole datan määrän niukkuus, vaan datan hyödyntäminen sen täydessä potentiaalissa. Toisin sanoen data

täytyy muuttaa tiedoksi, jotta yritys voi hyödyntää sitä yltääkseen pitkän aikavälin päämääriinsä ja tavoitteisiinsa. (Hannila et al. 2022, 29)

Miltei jokainen yrityksen tapahtuma on mahdollista tallentaa ja usein tallennetaankin, prosessoidaan ja jaetaan yrityksen käyttämien applikaatioiden ja järjestelmien kautta. Yrityksellä on dataa ja tietoa tallennettuna monissa eri muodoissa. Yrityksen data voidaan jaotella sen luonteen mukaan strukturoituun, puolistrukturoituun ja epästrukturoituun muotoon. **Strukturoitu data** on taulukkomuodossa olevaa dataa, jota säilytetään tietokannassa. Tämäntyyppinen data on pitkäikäistä ja hitaasti muuttuvaa tietoa, esimerkiksi asiakas- tai toimittajatietoa. **Epästrukturoidun datan** rakennetta ei puolestaan ole määritelty lainkaan etukäteen. Esimerkiksi sähköpostit, kuvat tai työkoneelle tallennettu diaesitys ovat kaikki esimerkkejä yrityksen omistamasta, epästrukturoidusta datasta. Näiden kahden väliin jäävää dataa kutsutaan **puolistrukturoiduksi dataksi**. Data on tietyssä rakenteessa, esimerkiksi XML-tiedostona, kuitenkin epätarkemmin kuin strukturoitu data. Dokumentoidun datan lisäksi tietoa syntyy ja sitä kommunikoidaan eteenpäin ihmisten välisissä keskusteluissa, sekä muodollisesti että epämuodollisesti. Tätä hiljaista tietoa on vaikea aineellistaa ja täten yrityksen on vaikea täysin tiedostaa ja hyödyntää tehokkaasti kaikkea tieto-omaisuuttaan. (Borek et al. 2013, 6–7)

Tieto-omaisuudella on muutamia uniikkeja ominaisuuksia, jotka erottavat sen yrityksen muusta omaisuudesta. Tietoa voidaan siirtää äärimmäisen nopeasti paikasta toiseen, toisin kuin esimerkiksi fyysistä omaisuutta. Tieto-omaisuus on myös suurelta osin uudelleenkäytettävää, eli sen arvo ei heikkene tai kulu, kun sitä käytetään. Tuoreella tiedolla on kuitenkin arvoa kilpailijoihin nähden ja voi oikein käytettynä luoda kilpailuetua, joten uudelleenkäytettävyys pätee vain yrityksen sisäisesti. Tieto-omaisuus voi myös vanheta ja tätä kautta menettää arvoaan, kun tieto ei ole enää relevanttia tai yksinkertaisesti pidä paikkaansa. (Borek et al. 2013, 8–9)

Tieto-omaisuuden rahallista arvoa on usein vaikea mitata. Vaikkakin se on yrityksen omaisuutta, jätetään se esimerkiksi ulkoisen laskentatoimen tuottamasta yrityksen tilinpäätöksestä usein pois epäluotettavien laskumallien takia (Borek et al. 2013, 8). Yrityksillä vaikuttaakin olevan puutteita tieto-omaisuutensa arvon ymmärtämisessä varsinkin strategisena

etuna ja arvoa luovana tekijänä, eli tieto-omaisuutta saatetaan hallita vain teknologisesta näkökulmasta yrityksen IT-osastolla (Hannila et al. 2022, 36).

### 3.2.2 Haavoittuvaisuus, riski ja tietoturvauhat

**Haavoittuvaisuus** on heikkous yrityksen omaisuudessa tai järjestelmissä, jota vahingoittaja voi hyväksikäyttää ja täten aiheuttaa yritykselle epämieluisia seurauksia. **Uhka** on potentiaalinen, epämieluisia seurauksia yritykselle aiheuttava tapahtuma. **Riski** on tapahtuma, kun uhka hyödyntää haavoittuvuutta, ja joka johtaa poikkeamaan yrityksen nykytilasta. (Alexander et. al. 2020, 36; Campbell 2016, 10) Riskien todennäköisyyden ja vaikutuksen arvioimisen kautta niihin voidaan varautua yrityksen valitsemalla tavalla ja tasolla. Riskien arvioiminen ja priorisointi on aina yrityskohtaista, ja huomioon otettavia tekijöitä ovat muun muassa yrityksen toimiala, koko ja riskinottohalukkuus. Olennaista arvioinnissa on riskin toteutumisen aiheuttaman rahallisen menetyksen vertailu riskiin varautumisen hintaan. Joihinkin riskeihin on kuitenkin varauduttava hinnasta huolimatta, jos lait ja säädökset niin vaativat. (Whitman 2019, 11; Alexander et. al. 2020, 33) Tietojensa suojelemiseksi on yrityksen tunnistettava omat haavoittuvaisuutensa, kohtaamansa uhat, sekä valita mihin riskeihin se haluaa varautua. Kuten aiemmin todettu, itse suojelemisen kohde, eli tieto-omaisuuden tunnistaminen on myös olennainen osa tätä prosessia (Whitman 2019, 11).

Uhat yrityksen tieto-omaisuutta kohtaan syntyvät niin sisäisistä kuin ulkoisista lähteistä. Työntekijät tarvitsevat päivittäisten työtehtäviensä suorittamiseen pääsyn yrityksen tieto-omaisuuteen, ja inhimilliset virheet aiheuttavat yrityksen tietojen luottamuksellisuuteen, eheyteen ja saatavuuteen merkittävän uhan (Whitman 2019, 23–24). Myös rikollisten keinot tietoturvahyökkäyksien toteutukseen ovat yhä hienostuneempia ja tehokkaampia kehittyen kaiken aikaa, johtaen jatkuvaan kilpajuoksuun rikollisten ja yrityksien suojautumismekanismien välillä (Campbell 2016, 15).

Organisaatioiden tieto-omaisuuden selkeimmät ja yleisimmät uhat voidaan jakaa kahdentoista kohdan listaan. Uhat on esitetty alla olevassa Taulukossa 1., jossa jokaista uhkaa vastaa esimerkki hyökkäyksestä. Tämän ajan kompleksisessa turvallisuusympäristössä hyökkääjät käyttävät monia keinoja samaan aikaan saavuttaakseen lopullisen tavoitteensa, eli uhat Taulukon 1. kategorioista voivat esiintyä samaan aikaan (Whitman 2019, 44).

*Taulukko 1. Tietoturvan 12 uhkakategoriaa (Whitman 2019, 13)*

| **Tietoturvan 12 uhkakategoriaa** | |
|---|---|
| **Uhkakategoria** | **Esimerkki hyökkäyksestä** |
| Immateriaaliomaisuuden vaarantuminen | Piratismi, tekijänoikeuksien rikkominen |
| Poikkeamat palvelun laadussa | Internet-palveluntarjoajan, virran, tai alueverkon palveluongelmat |
| Vakoilu tai laiton tunkeutuminen | Valtuuttamaton pääsy ja/tai tiedonkeruu |
| Luonnonvoimat | Tulipalo, tulva, maanjäristys, salamaniskut |
| Inhimillinen erehdys tai virhe | Vahingot, työntekijöiden virheet |
| Tiedon kiristäminen | Kiristys, tiedon paljastaminen |
| Sabotaasi tai vandalismi | Systeemien tai tiedon tuhoutuminen |
| Ohjelmisto- tai tietoturvahyökkäys | Virukset, madot, makrot, palvelunestohyökkäykset |
| Tekninen laitevika tai -virhe | Laitteiston vikaantuminen |
| Tekninen ohjelmistovika tai -virhe | Bugit, koodiongelmat, tunnistamattomat porsaanreiät |
| Teknologinen vanhentuminen | Vanhanaikaiset tai vanhentuneet teknologiat |
| Varkaus | Laitteiden tai tiedon laiton haltuunotto |

IBM:n vuonna 2022 julkaisema tutkimusraportti paljastaa yleisimmät syyt tietoturvaloukkauksen takana. Tutkimuksessa on haastateltu 3600 yritystä maailmanlaajuisesti, jotka ovat joutuneet yhden tai useamman tietoturvahyökkäyksen kohteeksi (IBM 2022, 3). Tietoturvaloukkauksista 24 % johtui IT-järjestelmien toimintahäiriöstä, joka johti tiedonmenetykseen. Toimintahäiriö saattaa johtua esimerkiksi virheestä koodissa. Inhimillinen erehdys, esimerkiksi työntekijän virhe, oli syynä 21 %:ssa tietoturvaloukkauksista. Muita syitä olivat käyttöjärjestelmien toiminnan kannalta kriittisiä tietoja tuhoavat hyökkäykset, jotka aiheuttivat 17 % loukkauksista, ja kiristyshaittaohjelmat, jotka aiheuttivat 11 % loukkauksista (IBM 2019). Kiristyshaittaohjelmat salaavat tai lukitsevat uhrin tiedot, jotka uhri saa takaisin maksamalla lunnaat (F-Secure 2023). Kiristyshaittaohjelmien yleisyys kasvaa – vuonna 2021 ne olivat syynä 7,8 %:iin hyökkäyksistä, kun taas vuonna 2022 osuus oli kasvanut 11 %:iin, jota voidaan pitää merkittävänä nousuna (IBM 2022, 32).

### 3.2.3 Tietoturvan ulkoiset vaatimukset

Kuten yrityksen toiminnassa yleisesti, myös tietoturvan toteuttamisessa on tietyt raamit. Ulkoiset toimintaa ohjaavat tekijät voidaan jakaa kolmeen: lainsäädäntöön perustuviin

vaatimuksiin, säädöksiin ja suosituksiin. **Lainmukaisten vaatimusten** täyttäminen on pakollista. Nämä vaatimukset on asetettu yleensä valtion, poliisin tai muiden viranomaisten taholta. (Alexander et al. 2020, 103–104) Yksi selkeä esimerkki tietoturvatoimintaan vahvasti vaikuttavasta, lainsäädäntöön perustuvasta vaatimuksesta on Euroopan Unionin yleinen tietosuoja-asetus (GDPR), joka otettiin käyttöön kaikissa EU:n jäsenmaissa vuonna 2018. Se asettaa yrityksille henkilötietojen keräämistä, säilytystä ja hallinnointia koskevat tarkat vaatimukset. (Your Europe 2022) **Säädökset** puolestaan kertovat, miten tietyllä liiketoiminta-alueella tulee operoida. Tietyn toimialan säädösten asettaminen ja valvominen on kyseisen toimialan sääntelyviranomaisten vastuulla. Vaikka ne eivät ole lainmukaisia vaatimuksia, noudattamatta jättäminen saattaa johtaa sakkoihin tai jopa toimintakieltoon. (Alexander et al. 2020, 104) **Suositukset** ovat yleisesti hyväksyttyjä, alan parhaita käytäntöjä (*best practise*), joiden avulla yritys voi parantaa toimintaansa. Suosituksia voivat laatia esimerkiksi valtioiden virastot. Yrityksiä kannustetaan niiden implementointiin, koska noudattaminen ohjaa parempaan ja turvallisempaan toimintaan. Yleisesti yhteyksien ylläpitäminen asiaankuuluvien ulkoisten tahojen kanssa on hyödyllistä – se auttaa yritystä paremmin ymmärtämään heille asetetut vaatimukset ja pysymään ajan tasalla mahdollisesti toimintaan vaikuttavista muutoksista. (Alexander et al. 2020, 104–105)

### 3.2.4 Tietoturvan sisäiset raamit

Yrityksen sisäistä toimintaa ohjataan yleensä neljällä eri tasolla – käytäntöjen, standardien, toimintatapojen ja ohjeiden kautta (Whitman 2019, 177). Whitman (2019, 177) jakaa yrityksen sisäiset, tietoturvatoimintaa ohjaavat dokumentit epätarkimmasta tarkimpaan seuraavasti: käytännöt, standardit, toimintatavat ja ohjeet. **Käytäntö** on yleinen linjanveto yrityksen suhtautumisesta tiettyyn toimintoon ja luo pohjan yksityiskohtaisemmille ohjeille. Käytäntö on yrityksen ylimmän johdon sanoitus siitä mitä tehdään, kun taas muut ohjeet kertovat, miten tehdään. **Standardi** on yksityiskohtaisempi selitys, miten yrityksen ja sen työntekijöiden tulee toimia noudattaakseen käytäntöä. Standardien tulisi asettaa minimivaatimukset, millä yrityksen linjaamat käytännöt toteutuvat. **Toimintatapa** on yksityiskohtainen työskentelyohje tietystä toiminnosta. Se selittää miksi, milloin ja kenen toimesta kyseinen toiminto tehdään. **Ohjeet** selkeyttävät käytäntöjä, standardeja ja toimintatapoja, ohjaten ohjeen lukijaa askel askeleelta eteenpäin. (Whitman 2019, 175–177)

# 4 Yrityksen tietoturvastrategia

Ward (1988, 206) määrittelee strategisiksi kysymyksiksi ne tekijät, joilla on potentiaalia vaikuttaa koko liiketoimintaan. Tietoturva voidaan määritellä strategiseksi tekijäksi, koska epäonnistunut tietoturvastrategia voi vaikuttaa yrityksen ydintoimintoihin ja näin asettaa yrityksen toiminnalle strategisen riskin. Toteutuessaan tietoturvauhat voivat muun muassa vahingoittaa yrityksen mainetta, aiheuttaa toiminnan pysähtymisen ja liiketoimintatappioita, sekä romahduttaa yrityksen osakkeiden hinnan. Onnistunut tietoturvastrategia puolestaan lisää arvoa suojaamalla ja hyödyntämällä yrityksen tieto-omaisuutta yrityksen toiminnan parantamiseen. Erityisen tärkeää on, että tietoturvastrategia on linjassa yritysstrategian kanssa, muuten se jää irralliseksi ja arvoa tuottamattomaksi osaksi yrityksen toimintaa. (McFadzean et al. 2011, 103)

## 4.1 Tietoturvastrategian sisältö ja merkitys

Yrityksen tietoturvastrategia on suunnitelma, joka kattaa yrityksen omistaman tieto-omaisuuden, järjestelmät, laitteet ja ohjelmistot, ja jonka tarkoituksena on suojata niitä tietoturvaloukkauksilta. Tietoturvastrategian tulee sisältää niin tietoturvaloukkauksia ehkäiseviä toimia kuin myös suunnitelman, miten toimia, jos tietoturvaloukkaus tapahtuu. Tietoturvastrategia asettaa myös suuntaviivat tulevaisuudelle. Strategian tavoitteiden tulee olla realistisia, mutta haastavia, jotta niiden tavoitteleminen ohjaa aidosti kohti parempaa toimintaa. (Campbell 2016, 63–64) Tavoitteiden ei tulisi kuitenkaan olla tietoturvastrategian keskiössä, vaan strategian tehtävä on ennen kaikkea ilmaista ne suuntaviivat ja toiminnot, joilla tavoitteet saavutetaan (Kamensky 2015).

Yrityksen arjessa tietoturvastrategia luo raamit tietoturvakäytännöille, jotka ohjaavat työntekijöitä toimimaan oikein ja ajamaan eteenpäin yrityksen pitkän aikavälin tietoturvatavoitteita. Tietoturvakäytäntöjen muodostaminen on ylimmän johdon tehtävä, joissa he ilmaisevat yrityksen periaatteet tieto-omaisuuden kanssa työskennellessä, ja jonka pohjalta muodostetaan yksityiskohtaisemmat ohjeet. **Yritystason käytäntö** tiivistää yrityksen tietoturvafilosofian ja asettaa strategisen suunnan, laajuuden ja yleisen vireen yrityksen

tietoturvatoimintaan. Yritystason käytäntö on johtotason dokumentti, jonka yleensä luo tietoturva- tai tietohallintojohtaja muiden johtotason henkilöiden kanssa. Tietoturva-asiantuntijoiden rooleja käsitellään tarkemmin seuraavassa kappaleessa. **Aihekohtainen käytäntö** tarkentaa, minkälaiseen käyttöön yrityksen tietty teknologia tai resurssi on tarkoitettu, ja kenellä on lupa sitä käyttää. Yrityksellä voi olla aihekohtaisia käytäntöjä esimerkiksi virushaittaohjelmien esto-ohjelmien käytöstä työntekijöiden laitteilla. **Systeemikohtainen käytäntö** toimii usein ohjeena, mitä käytetään ylläpitäessä tai korjatessa systeemiä. Verrattuna kahteen edelliseen, systeemikohtainen käytäntö on paljon käytännönläheisempi, ja voi ulkoasultaan olla enemmänkin ohjeen kaltainen. (Whitman 2019, 170; 177–178; 183–185; 190–191)

Tietoturvastrategian olemassaoloa voidaan pitää merkittävänä askeleena kohti tietoturvallisempaa toimintaa (Whitman 2019, 130). Se voidaan nähdä indikaattorina yrityksen kypsyydestä, sillä tietoturvastrategian laatiminen ja implementointi edellyttävät sekä osaamista että resursseja (Campbell 2016, 64). Erityisesti ulkoisille sidosryhmille, kuten asiakkaille ja medialle, tietoturvastrategian olemassaolo kuvastaa dynaamista ja riskitietoista toimintaa, sekä kertoo ymmärryksestä tieto-omaisuuden arvoa kohtaan ja sen suojelemisen tärkeydestä nykypäivänä. Tietoturvastrategia edistää myös sisäistä yrityskulttuuria, jossa tietoturva nähdään työntekijöiden keskuudessa voimavarana, ei prosesseja ja päivittäistä työtä hidastavana taakkana. Kuten aiemmin mainittu, inhimillinen erehdys on taustalla jopa 21 %:ssa tietoturvaloukkauksista, joten tietoturvamyönteisyyden integroiminen yrityskulttuuriin, sekä tietoturvatietoisuuden ja -koulutuksen lisääminen ovat avaintekijöitä tietoturvaloukkausten vähentämiseen. (AlGhamdi et al. 2020, 4)

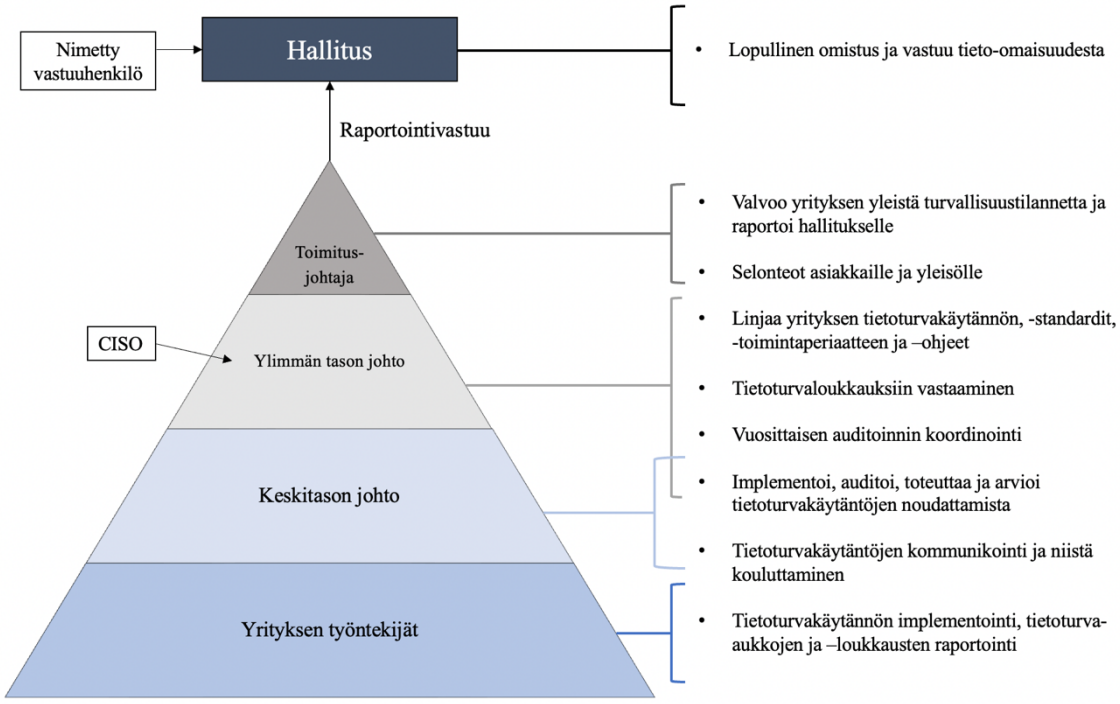
### 4.1.1 Hallinto ja sen sijoittuminen

Yrityksen ylin johto on vastuussa tietoturvan suunnittelusta, organisoimisesta, johtamisesta ja kontrolloinnista – eli tietoturvahallinnosta. Se suunnittelee tietoturvastrategian ja sen jalkauttamisen yrityksen käytäntöihin, toimintatapoihin, standardeihin ja ohjeisiin niin että tavoiteltu tietoturvan taso voidaan saavuttaa. Se myös valvoo, että yrityksen resursseja käytetään tarkoituksenmukaisesti ja tehokkaasti. (Whitman 2019, 135)

Yrityksissä tietoturva-asiantuntijoita on eri rooleissa, hyvin teknillisistä tehtävistä aina hallituspositioihin asti (Campbell 2016, 32). Yrityksen ylemmässä johdossa työskentelevän

tietoturva-asiantuntijan titteleitä ovat esimerkiksi *Head of Information Assurance*, *Information Security Manager*, *Chief Information Security Officer (CISO)* tai *Chief Information Officer (CIO)*. Suomenkielinen vastaava CIO:lle on tietohallintojohtaja, johon tekstissä viitataan, kun tarkoitetaan IT-osaston strategiasta vastaavaa, johtoryhmässä istuvaa päällikköä (Marbles 2023). CISO:n puolestaan viitataan tietoturvajohtajana, joka toimii yleensä tietohallintojohtajan alaisuudessa. On toivottavaa, että CISO muodostaa kokonaan oman tietoturvatiimin, ja raportoi jopa suoraan toimitusjohtajalle, jos yrityksen ydinliiketoiminta on vahvasti teknologiasta riippuvainen (Campbell 2016, 33). Tietohallintojohtajan paikka johtoryhmässä, sekä tietoturvajohtajan asettuminen korkealle tasolle organisaatiorakenteessa tai suora raportointi toimitusjohtajalle luo uusia mahdollisuuksia tietoturvan toteuttamiseen ja sen integroimiseen yrityksien toimintaan sen fundamentaalisena osana. (Campbell 2016, 43–44)

Tietohallinto- tai tietoturvajohtajien roolit ovat verrattain uusia, eikä yhtä vakiintunutta titteliä tai sijoittumista organisaatiorakenteeseen ole. Tärkeintä on varmistaa, varsinkin suuremmissa yrityksissä, että tietoturvajohtajien rooli on yksinomaan tietoturvaa koskeva, ei muun työn ohella tehtävää työtä. Roolin tulee omistaa riittävä senioriteetti, joka sitouttaa yrityksen ottamaan tietoturvakysymykset huomioon muiden johtoryhmätason kysymysten rinnalla. (Campbell 2016, 33) Tietoturvajohtajan tulee ymmärtää, mitkä ovat kyseisen yrityksen tietoturvariskit, miten niitä hallitaan ja missä yrityksellä on huomattavia heikkouksia. Tietoturva- tai tietohallintojohtajan tulee kommunikoida tämä tieto voimakkaasti yrityksen johtoryhmälle, jotta tietoturvakysymykset käsitellään samalla prioriteetilla muiden strategisten asioiden kanssa. (Alexander et al. 2020, 95–96) Myös yrityksen hallituksesta tulee nimetä yksittäinen henkilö, jonka vastuulla yrityksen tieto-omaisuuden lopullinen suojaaminen on. Hallitusjäsenen nimeäminen tietoturvan ja tieto-omaisuuden vastuuhenkilöksi kertoo yrityksen sitoutumisesta tietoturvaa kohtaan. (Campbell 2016, 33) Kuvassa 2 on havainnollistettu tietoturvajohtajan sijoittumista organisaatioon ja tietoturvahallinnon vastuut.



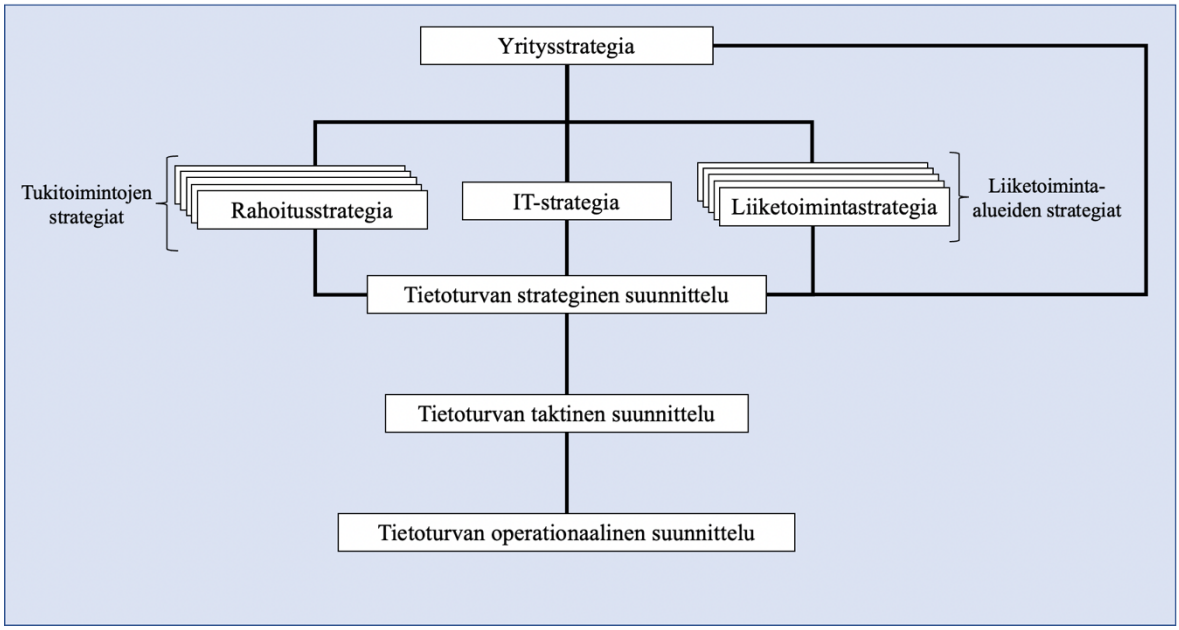

*Kuva 2. Tietoturvahallinnon vastuut (mukaillen Whitman 2019, 140)*

Aihetta käsittelevässä tutkimuksessa on kiinnitetty valitettavan vähän huomiota tietoturvahallinnon tavoitteisiin. Tämä osaltaan johtuu siitä, että tietoturva oli pitkään vain IT-osaston toteuttama teknologinen ratkaisu verrattuna tämänkin työn esille tuomaan kokonaisvaltaiseen lähestymistapaan, jossa tietoturva on yrityksen ylimmän johdon agendalla. (Mishra 2015, 123) Hallinnon perustavanlaatuisia tavoitteita tulisi muun muassa olla tietoturvakäytäntöjen selkeys ja helppo saatavuus, selkeä vastuunjako tietoturvapäätöksissä, tietoturvatietoiseen kulttuuriin kannustaminen ja tätä kautta vahinkojen ehkäiseminen, sekä lainmukaisten vaatimuksien ehdoton noudattaminen (Mishra 2015, 132). Tietoturvahallinnon selkeät tavoitteet ovat olennainen osa sen toimintaa, sillä niiden avulla hallinnon toimintaa voidaan arvioida ja seurata. Tavoitteiden asettaminen auttaa myös varmistamaan, että hallinto keskittyy oikeisiin asioihin ja että sen toiminta tukee yrityksen tavoitteita ja strategiaa. (Mishra 2015, 123)

### 4.1.2 Tietoturvan suunnittelu

Strateginen suunnittelu linjaa, miten resursseja tulisi käyttää strategiaan kirjattujen, selkeästi määriteltyjen tavoitteiden saavuttamiseen ottaen huomioon alati muuttuvan

toimintaympäristön (Whitman 2019, 129). Erityispiirteenä tietoturvasuunnittelussa on se, että huomioon tulee ottaa yrityksen kaikki liiketoiminta-alueet ja tukitoiminnot. Tietoturvahallinnon tavoitteena on turvata tieto-omaisuus koko yrityksen laajuudelta, joka onnistuakseen edellyttää tietoturvan suunnittelijoilta ymmärrystä koko yrityksen suunnitteluprosessista ja liike- ja tukitoiminnoista. (Whitman 2019, 126) Ylhäältä alaspäin ohjautuva strateginen suunnittelu, kuten esitetty Kuvassa 3., esittää yritysstrategian korkeimmalla tasolla, josta liiketoiminta-alueiden sekä tukitoimintojen strategiat johdetaan. Kuva havainnollistaa, kuinka kaikilla ylemmän tason strategioilla on vaikutusta tietoturvastrategian suunnitteluun.




*Kuva 3. Suunnitteluhierarkia mukaillen (Whitman 2019, 130)*

CISO:n ja tietoturvaosaston ensimmäisen prioriteetin tulee olla strateginen suunnitelma, joka mukailee ylempien tasojen strategioita. Sen pohjalta muodostetaan tarkat, mitattavat ja aikaan sidotut tavoitteet (Whitman 2019, 132). Näiden tavoitteiden saavuttamiseksi vaaditut toimet konkretisoituvat taktisissa ja operationaalisissa suunnitelmissa. **Taktisen suunnitelman** avulla CISO ja hänen alapuolellaan toimivat päälliköt organisoivat, priorisoivat ja hankkivat resursseja toteuttaakseen suunnitellut projektit ja valvovat, että toiminta tukee strategista suunnitelmaa. Tietoturvaosaston kontekstissa **operationaaliset suunnitelmat** voivat koskea esimerkiksi tietoturvakoulutuksen toteuttamista tai uuden palomuurin käyttöönottoa. (Whitman 2019, 133)

Tietoturvatoimet usein hidastavat liiketoiminnan prosesseja, joka aiheuttaa ristiriidan turvallisuuden ja liiketoimintayksiköiden tuloksen välille (Whitman 2019, 164). Esimerkiksi IT-osaston tavoite on tehokas ja tuloksekas tieto-omaisuuden saatavuus, kun taas tietoturvan tarkoitus on suojella sitä. Siksi suunnitteluvaiheessa on tärkeää käydä aktiivista poikkifunktionaalista keskustelua yksiköiden välillä, jotta eroavaisuudet tavoitteissa ja toimintatavoissa otetaan huomioon ja ”kultainen keskitie” voidaan löytää. Tasapainon löytäminen tietoturvallisen mutta liiketoiminnallisesti tehokkaan toiminnan välille vaatii joskus luovia ratkaisuja, jonka vuoksi suunnitteluvaiheessa päälliköiden henkilökohtaiset kyvykkyydet ja vuorovaikutustaidot korostuvat. (Whitman 2019, 130–132)

## 4.2 Tekijät onnistuneesti implementoidun tietoturvastrategian takana

Tässä kappaleessa avataan menestystekijöitä onnistuneen tietoturvastrategian taustalla. Käyttäen Whitmanin (2019, 141), Soomro et al. (2016) ja AlGhamdi et al. (2020) listaamia onnistumisen ajureita, on onnistuneen tietoturvastrategian menestystekijät jaoteltu aihepiireittäin seuraavasti:

- **Ylimmän johdon vastuu**
- **Tietoturvan- ja yritysstrategian yhdenmukaistaminen**
- **Tietoturvatietoisuus, -koulutus ja -käytännöt, sekä**
- **Menestyksen seuraaminen**

### 4.2.1 Ylimmän johdon vastuu

Suurin rooli tietoturvan onnistumisen kannalta on yrityksen ylimmällä johdolla (Soomro et al. 2016, 218; AlGhamdi et al. 2020, 6–19; Whitman 2019, 141). Tämä edellyttää, että tieto-omaisuuden arvo tunnistetaan johtoryhmän ja hallituksen tasolla, sekä sen turvaamiseen sitoudutaan. Tietoturvan noustessa ylimmän johdon agendalle, muovautuu se pelkästä teknologisesta ratkaisusta holistisempaan, arvoa tuottavaan osaan liiketoimintaa. Kirjallisuudessa on todettu, että ylimmän johdon osallistuminen tietoturvan toteuttamiseen parantaa myös työntekijöiden asennoitumista tietoturvakäytäntöjä kohtaan (Soomro et al. 2016, 218).

Roolit, vastuut ja tilivelvollisuus tietoturvaan liittyen tulee olla yrityksessä tunnistettuna (Al-Ghamdi et al. 2020, 6). Tietoturvaan liittyviä rooleja on monia ja ne riippuvat yrityksen koosta, organisaatiorakenteesta ja toimialasta. Keskisuurten ja suurten yrityksien olisi hyvä nimetä tietoturvapäällikkö johtamaan tietoturvatiimiä, joka koostuu myös teknillisiä taitoja omaavista työntekijöistä. Tämän tiimin menestys riippuu osittain siitä, kuinka arvokkaaksi sen tekemä työ yrityksessä mielletään, sekä sen saamasta hallituksen ja johtoryhmän tuesta (AlGhamdi et al. 2020, 6). Johtoryhmätasolla on joko CIO:n tai CISO:n vastuulla ottaa esiin tietoturvakysymykset johtoryhmän päätöksenteossa ja suunnittelussa. Tietoturvan lopullinen vastuu tulee kuitenkin olla nimetyllä hallituksen jäsenellä. (Alexander et al. 2020, 33)

### 4.2.2 Tietoturva- ja yritysstrategian yhdenmukaistaminen

Tietoturvastrategian tehokkuus on suoraan verrannollinen sen yhteneväisyyteen yrityksen laajempien tavoitteiden kanssa. Tietoturva- ja yritysstrategian yhdenmukaisuus onkin yksi avaintekijöistä onnistuneessa tietoturvassa parantaen käytäntöjen noudattamista ja lopulta johtaen tietoturvaloukkausten vähenemiseen. (Soomro et al. 2016, 220) Tietoturvastrategian kehittäminen yhdessä yritysstrategian kanssa kannustaa molempia alueita työskentelemään yhdessä kumppaneina, ei johtajana ja seuraajana. Strategioiden yhteensovittaminen ja tiedon jakaminen näiden funktioiden välillä mahdollistaa täten myös tieto-omaisuuden ja sen kyvykkyyksien hyödyntämisen täydessä potentiaalissaan samalla kilpailuetua luoden. (McFadzean et al. 2011, 104)

### 4.2.3 Tietoturvatietoisuus, -koulutus ja -käytännöt

Tietoturvatietoisuus, -koulutus ja -käytännöt ovat oleellisia työkaluja yrityksen työntekijän tekemästä virheestä johtuvien tietoturvaloukkausten vähentämiseen (Whitman 2019, 268). Hyvin laadittu ja implementoitu tietoturvakäytäntö lisäävät tietoturvan tehokkuutta, joten se yhdessä koulutuksen ja tietoisuuden kanssa voidaan nähdä merkittävänä tekijänä tietoturvan onnistumisen taustalla (Soomro et al. 2016, 219).

Tietoturvakäytännöt eivät ole erityisen tehokkaita ilman tietoturvatietoisuutta ja -koulutusta, johtaen siihen, että näiden kolmen tekijän tulisi esiintyä yhtä aikaa yrityksen suunnitellessa

tietoturvaansa. Tietoisuus ei tarkoita pelkästään tietoisuutta yrityksen sisäisistä käytännöistä, toimintatavoista ja ohjeista tietoturvaan liittyen, vaan myös tietoisuutta tieto-omaisuutta kohtaavista uhista. Tietoisuus uhista lisää varovaisuutta työntekijöiden keskuudessa ja harjoittaa silmää huomaamaan mahdolliset huijausviestit tai puutteet suojauksessa. Koulutus puolestaan neuvoo, miten tulee toimia tieto-omaisuuden suojelemiseksi. (Soomro et al. 2016, 219)

### 4.2.4 Menestyksen seuraaminen

Tietoturvastrategian ja -käytäntöjen menestyksen seuraaminen voidaan jakaa arviointiin, monitorointiin, mittaamiseen ja raportointiin. Tietoturva ei ole staattinen prosessi ja vaatii jatkuvaa toimintaympäristön havainnointia tieto-omaisuuden suojelemiseksi. Strategiaa ja käytäntöjä tulee arvioida ja tarkastaa säännöllisesti, sekä reagoida ketterästi uusiin uhkiin. (AlGhamdi et al. 2020, 14)

Paras tapa varmistaa, että yritys toimii lakeja ja säädöksiä noudattaen, on suorittaa arviointia. Arviointiprosessin avulla voidaan havainnoida, vastaavatko yrityksen käytännöt ja toimintaohjeet tietoturvatavoitteita sekä ulkoisia ja sisäisiä vaatimuksia. (AlGhamdi et al. 2020, 14) Monitorointi puolestaan mahdollistaa nopean reagoinnin riskeihin, uhkiin tai haavoittuvuuksiin, joita havaitaan. Monitoroinnin avulla yritys voi havaita ja näin hallita tietoturvatapahtumaa, ennen kuin vahinkoa on kerennyt tapahtua. (AlGhamdi et al. 2020, 19)

Raportointi on keino lisätä ymmärrystä tietoturvan merkityksestä hallituksen ja johtoryhmän jäsenien keskuudessa, jonka vuoksi panostukset selkeään raportointiin ovat arvokkaita. Mittauksesta ja arvioinnista tulee raportoida ei-teknillisesti, jotta tulokset ymmärretään yksikäsitteisesti johtoryhmässä ja hallituksessa. (AlGhamdi et al. 2020, 19) Ylimmän johdon tehtävänä on päättää hyväksyttävä riskitaso, jonka pohjalta luotuihin konkreettisiin tavoitteisiin mittaustuloksia verrataan. Mittaustulokset eivät siis itsessään kerro tietoturvan tilasta, vaan niitä pitää verrata yrityksen kirjaamiin tavoitteisiin ja edellisiin tuloksiin toiminnan kehittymisen seuraamiseksi. Mittauskohteita voi olla esimerkiksi työntekijöiden tietoturvatietoisuus ja sitoutuminen käytäntöjen noudattamiseen. Mittauksen tulee olla jatkuvaa ja tavoitteita tulee ja pitääkin päivittää, kun tavoite on saavutettu tai yrityksen strategiaa muutetaan. (AlGhamdi et al. 2020, 16)

### 4.3 Tietoturvastrategiaan liittyvät haasteet

Vaikka kokonaisvaltaisempi lähestymistapa tietoturvaan yrityksissä on yleistymässä, monet yritykset kohtaavat haasteita strategian suunnittelussa ja toteutuksessa (AlGhamdi et al. 2020, 2). Von Solms & Von Solms (2004, 372) argumentoivat, että yksityiskohdilla on suuri rooli onnistuneessa tietoturvastrategiassa, ja tietoturvan kaikkia osa-alueita tulee harkita, jotta suojaus on riittävä. Yleinen ongelma on vääriin uhkiin varautuminen, kun strategian suunnitteluvaiheessa riskianalyysiä ei ole tehty asianmukaisesti. Mikäli yritys varautuu todennäköisyydeltään olemattomiin riskeihin ja jättää samalla huomiotta mahdollisesti erittäin vahingolliset tietoturvauhat, voi sinänsä hyvin rakennettu strategia olla yrityksen resurssien haaskaamista. (Von Solms & Von Solms 2004, 373)

Ongelmia voi myös muodostua, jos kukaan ei ole vastuussa tietoturvapäätöksistä ja -strategiasta. Asianmukaisen tietoturvahallinnon rakentamisen lisäksi ylimmässä johdossa tulee olla nimettyjä vastuuhenkilöitä, joiden lopullisella kontolla tietoturvaan ja -omaisuuteen liittyvät päätökset ovat. (Von Solms & Von Solms 2004, 375) Tietoturvapäälliköiden työ myös onnistuu sitä paremmin, mitä enemmän sitä tuetaan ja resursoidaan ylimmän johdon toimesta (Soomro et al. 2016, 217–218). Ylimmän johdon vastuun lisäksi koko yrityksen tulee kantaa vastuuta tietoturvallisesta toiminnasta, ja sen huomiotta jättämisestä tulee olla seuraamuksia. (Von Solms & Von Solms 2004, 375)

Tietoturvan vähäinen tai olematon seuranta luo myös uhan tietoturvallisen toiminnan edellytyksille. Tietoturvan tilaa tulee jatkuvasti seurata myös strategian implementoinnin jälkeen, jotta mahdolliset puutteet huomataan ja korjataan. Tuudittautuminen kerran muodostetun tietoturvastrategian olemassaoloon ei riitä, vaan monitoroinnin tulosten perusteella sitä pitää olla valmis muuttamaan, esimerkiksi ulkoisen tilanteen, uhkien ja teknologioiden kehittyessä. (Von Solms & Von Solms 2004, 374–375)

Tietoturva on monen asian summa: useita asioita pitää olla tehty hyvin, ennen kun voidaan odottaa tuloksia ja perusteellista suojausta yrityksen tieto-omaisuuteen. Niin teknisten suojausmekanismien, käytäntöjen ja toimintaohjeiden, sekä henkilöstöön liittyvien tekijöiden tulee olla tasapainossa, jotta riskejä aidosti minimoiva tietoturvan taso voidaan saavuttaa (Soomro et al. 2016, 218–219). Kaikki turvallisuusulottuvuudet – fyysiset, inhimilliset ja

tekniset – on otettava huomioon tietoturvastrategian suunnittelemisessa ja toteuttamisessa, koska yksikään ulottuvuus ei yksinään tarjoa asianmukaista, tarpeeksi kattavaa ratkaisua tieto-omaisuuden suojeluun (Von Solms & Von Solms 2004, 373).

# 5 Johtopäätökset

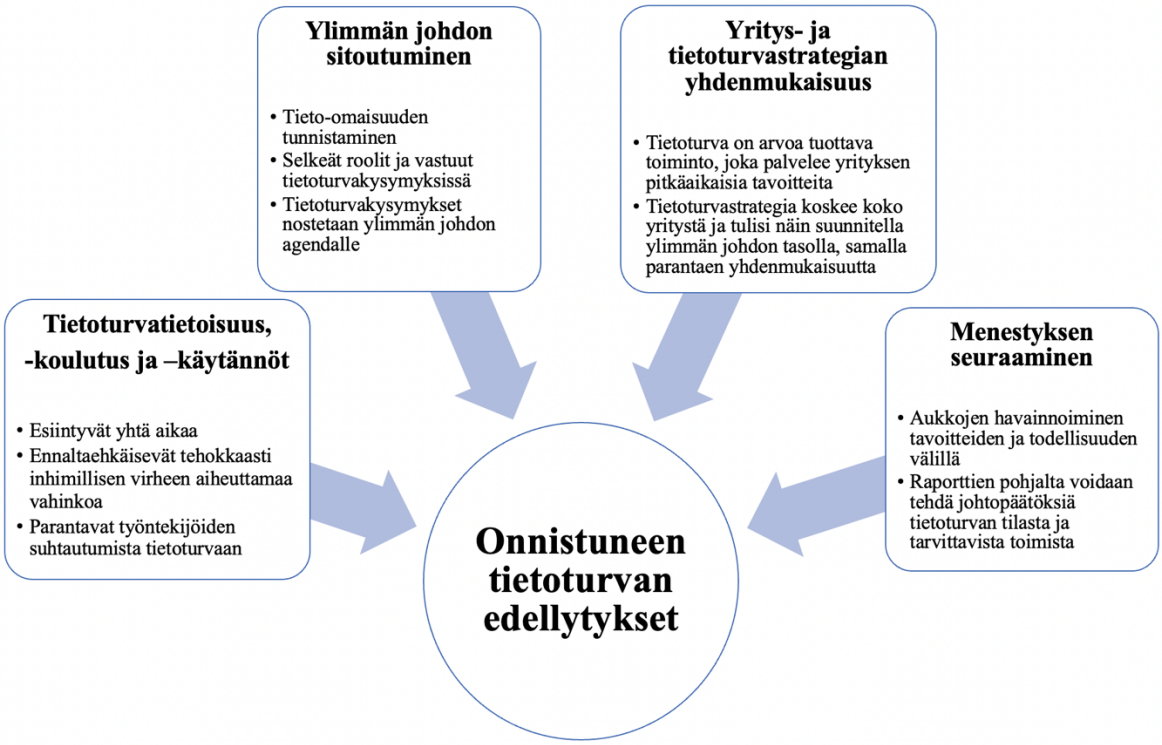
Tämän kandidaatintyön tarkoitus oli selvittää, mitkä ovat onnistumisen ajurit yrityksen tietoturvastrategian takana. Näiden lisäksi työssä käsiteltiin yrityksen ylimmän johdon roolia tietoturvastrategian suunnittelussa ja implementoinnissa, sekä tieto-omaisuuden merkitystä yrityksen toiminnassa. Lisäksi työ sivusi yrityksen yleisimmin kohtaamia tietoturvauhkia ja niiden yleisyyttä. Työn asettamiin tutkimuskysymyksiin pyrittiin löytämään vastauksia aiheesta julkaistuista tieteellisistä artikkeleista, ammattikirjallisuudesta ja tietoturva-alan raporteista. Työn teorian tavoitteena oli varmistaa, että lukija ensin ymmärtää strategian ja tietoturvan käsitteet olennaisilta osin, ennen kuin tietoturvastrategiaa käsiteltiin. Tämä kandidaatintyö etsi vastauksia yhteen päätutkimuskysymyksen, sekä kahteen osakysymykseen, jotka käydään seuraavaksi läpi kysymys kerrallaan.

*”Mitkä ovat tekijät onnistuneen tietoturvastrategian taustalla?”*

Kirjallisuuden perusteella kävi selväksi, että ylimmän johdon rooli tietoturvastrategian onnistumisessa on kiistämätön. Ilman ylimmän johdon sitoutumista ei tietoturvastrategian suunnittelu tai implementointi ole mahdollista. Ylimmän johdon sitoutuminen vaikuttaa myös voimakkaasti työntekijöiden suhtautumiseen tietoturvaan ja yrityksen yleiseen tietoturvakulttuuriin. Yrityksen ylin johto ei myöskään voi vain puhua tietoturvan merkityksestä, vaan heidän pitää luoda puitteet sen onnistumiselle ja toimia itse tietoturvakäytäntöjen mukaisesti.

Muita tärkeitä edellytyksiä tietoturvastrategian onnistumiseen olivat yritys- ja tietoturvastrategian yhdenmukaisuus, tietoturvatietoisuus, -koulutus ja -käytännöt, sekä menestyksen seuraaminen. Yhtä lailla kuin yrityksen liiketoimintastrategioiden, myös tietoturvastrategian tulee heijastaa yrityksen yleistä strategiaa. Tämä korostuu erityisesti strategian suunnitteluvaiheessa, jolloin tietoturvastrategian arvo ja menestyminen riippuvat siitä, kuinka hyvin se tukee yrityksen kokonaisvaltaisia tavoitteita ja arvoja. Kun tietoturvatietoisuus, -koulutus ja -käytännöt esiintyvät yhtä aikaa, saavutetaan niistä suurin hyöty. Kun työntekijät ovat

tietoisia tietoturvan merkityksestä ja tietoturvakäytännöistä ja saavat koulutusta aiheeseen liittyen, ovat he motivoituneempia noudattamaan niitä ja suhtautuvat aiheeseen varovaisemmin. Tämä johtaa parempaan tietoturvakäyttäytymiseen ja ennaltaehkäisee inhimillisten virheiden aiheuttamia tietoturvaloukkauksia. Yrityksen tietoturvatilanteen seuraaminen on myös avainasemassa tietoturvastrategian menestyksessä. Mittauksen, monitoroinnin, arvioinnin ja raportoinnin perusteella voidaan huomata aukkoja tietoturvastrategian ja yrityksen todellisuuden välillä, sekä varmistaa, että yritys on ylipäätään varautunut oikeisiin uhkiin. Tuloksien perusteella voidaan suunnitella tarvittavat toimenpiteet, jotta tietoturvan taso saadaan vastaamaan yrityksen tavoitteita. Päätutkimuskysymyksen vastaukset on tiivistetty Kuvassa 4.




*Kuva 4. Onnistuneen tietoturvan edellytykset*

*”Mikä on ylimmän johdon rooli tietoturvastrategian onnistumisessa?”*

Yrityksen ylimmän johdon rooli on varmistaa, että tietoturva on sisäänrakennettuna yrityksen normaaliin toimintaan. Kuten aiemmin todettu, on yrityksen ylimmän johdon sitoutuminen tietoturvastrategiaan sen menestyksen kulmakivi, sillä he ovat strategiaprosessin jokaisessa askeleessa mukana, sekä vastuussa tietoturvan tärkeyden kommunikoinnista koko

yritykselle. Vastuuta voidaan korostaa nimeämällä hallitusjäsen lopulliseksi tieto-omaisuuden omistajaksi, jolloin tietoturva otetaan todennäköisemmin päätöksenteossa huomioon. Ylimmän johdon tulee myös turvata riittävät resurssit tietoturvatyön tekemiseen, esimerkiksi muodostamalla tietoturvatiimin, jota CISO johtaa.

*”Miksi tietoturvastrategian kehittäminen on tärkeää?”*

Työssä havaittiin, että tietoturvastrategian kehittäminen on olennaista, kun halutaan siirtyä tietoturvan teknologisesta ulottuvuudesta laajempaan, koko yritystä koskevaan lähestymistapaan tietoturvasta. Tietoturvan strateginen taso vaatii yritykseltä tiettyä kypsyyttä, osaamista ja resursseja, ja on merkittävä askel kohti tietoturvallisempaa toimintaa. Pelkät teknologiset suojaukset eivät enää luo tarpeeksi laajaa suojausta tietoturvauhkia vastaan, kun nykypäivänä tietoturvaloukkauksia toteutetaan aina vain kehittyneemmin työkaluin. Tietoturvastrategia luo yritykseen ja sen työntekijöihin kulttuuria, missä tietoturva ja tietoturvakäytäntöjen noudattaminen koetaan tärkeäksi. Tämä vähentää tietoturvaloukkauksien määrää, kun siihen yhdistetään riittävä koulutus ja selkeät tietoturvakäytännöt. Tietoturvastrategian tärkeys näkyy työn tuloksien perusteella tietoturvaloukkausten vähenemisenä, koska strategian kautta implementoidut toimet ja tietoturvatietoisuus vähentävät niitä.

Tiedon määrän ja sen arvon kasvaessa tietoturvan rooli yrityksissä tulee entistä merkityksellisemmäksi. Aihepiirin jatkotutkimusaiheena voisikin olla tietoturvastrategian merkitys tietoturvaloukkauksen sattuessa ja siihen reagoitaessa. Toinen mielenkiintoinen tutkimusaihe laajempaan tietoturvateemaan liittyen on tekoälyn rooli tietoturvassa, koska jo nyt tekoälyä käytetään yrityksiä kohtaan hyökättäessä. Tutkimisen arvoista on nykyisen maailmanpoliittisen tilanteen valossa myös se, miten valtiot voivat suojautua informaatiovaikuttamiselta sekä tietojen urkkimiselta ja väärinkäytöltä.

# Lähteet

Alexander, D., Finch, A., Sutton, D., Taylor, A. 2020. Information Security Management Principles. 3. painos. BCS Learning & Development Limited. 268 s.

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. 2020. Information security governance challenges and critical success factors: Systematic review. Computers & security. 99 (102030). S. 1–39.

Arvopaperimarkkinayhdistys ry. 2020. Hallinnointikoodi. [Verkkoaineisto] [Viitattu 19.3.2023] Saatavissa: https://cgfinland.fi/wp-content/uploads/sites/39/2019/11/hallinnoin-tikoodi-2020.pdf

Borek, A., Parlikad, A. K., Webb, J., & Woodall, P. 2013. Total information risk management: maximizing the value of data and information assets. Elsevier Science & Technology. 316 s.

Campbell, T. 2016. Practical Information Security Management: A Complete Guide to Planning and Implementation. 1. painos. Berkeley, CA: Apress. 264 s.

Clegg, S., Carter, C. & Kornberger, M. 2004. Get up, I feel like being a strategy machine. European Management Review. 1 (1). S. 21-28.

F-Secure, 2023. Mikä on ransomware?. [Verkkoaineisto] [Viitattu 19.3.2023] Saatavissa: https://www.f-secure.com/fi/articles/what-is-a-ransomware-attack

George, B., Walker, R. M., & Monster, J. 2019. Does strategic planning improve organizational performance? A meta-analysis. Public Administration Review. 79 (6). S. 810-819.

Hannila, H., Silvola, R., Harkonen, J., & Haapasalo, H. 2022. Data-driven begins with DATA; potential of data assets. Journal of Computer Information Systems. 62 (1). S. 29-38.

IBM, 2019. What is destructive malware?. [Verkkoaineisto]. [Viitattu 19.3.2023] Saatavissa: https://www.ibm.com/downloads/cas/XZGZLRVD

IBM, 2022. Cost of a Data Breach Report 2022. [Verkkoaineisto] [Viitattu 19.3.2023] Saatavissa: https://www.ibm.com/downloads/cas/3R8N1DZJ

Kamensky, M. 2015. Menestyksen timantti: strategia, johtaminen, osaaminen, vuorovaikutus. Talentum. 376 s. [E-kirja]. [Viitattu 19.3.2023]. ISBN 978-952-14-2285-0

Kerttunen, M. 2007. Strategia. Maanpuolustuskorkeakoulu, strategian laitos. Julkaisusarja 3, Strategian asiatietoa. [Verkkoaineisto]. [Viitattu 7.3.2023] Saatavissa: https://urn.fi/URN:NBN:fi-fe201201241125

Kolttola, E., Westling, J. & Huhtinen, A. K. 2010. Strategia käytäntönä – Johdatus jalkautuksen tutkimukseen. Maanpuolustuskorkeakoulu, johtamisen ja sotilaspedagogiikan laitos. Julkaisusarja 3. [Verkkoaineisto]. [Viitattu 7.3.2023] Saatavissa: https://urn.fi/URN:ISBN:978-951-25-2068-8

Kyberturvallisuuskeskus. 2020. Kyberturvallisuus ja yrityksen hallituksen vastuu. [Verkkoaineisto]. [Viitattu: 11.4.2023]. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf

Marbles. 2023. CIO / Chief Information Officer / Tietohallintojohtaja. [Verkkoaineisto]. [Viitattu 1.4.2023] Saatavilla: https://www.marbles.fi/digiammatit/esimiehet-ja-johtajat/cio-chief-information-officer

McFadzean, E., Ezingeard, J. N., & Birchall, D. 2011. Information assurance and corporate strategy: A Delphi study of choices, challenges, and developments for the future. Information Systems Management. 28 (2). S. 102-129.

Mintzberg, H. 1987. The strategy concept I: Five Ps for strategy. California management review. 30 (1). S. 11-24.

Mishra, S. 2015. Organizational objectives for information security governance: a value focused assessment. Information & Computer Security. 23 (2). S. 122-144.

Porter, M. E. (1996). What is strategy?. Harvard Business Review. 74 (6). S. 61-78.

Rouleau, L., & Cloutier, C. 2022. It's strategy. But is it practice? Desperately seeking social practice in strategy-as-practice research. Strategic Organization. 20 (4). S. 722-733.

Samonas, S., & Coss, D. 2014. The CIA strikes back: Redefining confidentiality, integrity and availability in security. Journal of Information System Security. 10 (3). S. 21-45.

Soomro, Z. A., Shah, M. H., & Ahmed, J. 2016. Information security management needs more holistic approach: A literature review. International journal of information management. 36 (2). S. 215-225

Valpola, A. 2021. Toimiva johtoryhmä. 2. painos. Kauppakamari. 272 s. [E-kirja]. [Viitattu 19.3.2023]. ISBN: 9789522466907

Von Solms, B., & Von Solms, R. 2004. The 10 deadly sins of information security management. Computers & security. 23 (5). S. 371-376.

Ward, J. M. (1988). Information systems and technology application portfolio management–an assessment of matrix-based analyses. Journal of Information Technology. 3 (3). S. 205-215.

Whitman, M. E., & Mattord, H. J. (2019). Management of information security. 6. painos. Cengage Learning. 728 s. [E-kirja]. [Viitattu 19.3.2023]. ISBN: 9781337671545

Whittington, R. 2007. Strategy practice and strategy process: family differences and the sociological eye. Organization studies. 28 (10). S. 1575-1586.

Your Europe. 2022. Yleinen tietosuoja-asetus. [Verkkoaineisto]. [Viitattu 4.4.2023] Saatavilla: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm