TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

OSSI HUTTUNEN

TIETOTURVAPOLITIIKAN MERKITYS YRITYKSEN STRATEGIASSA

Kandidaatintyö

Tarkastaja: Jussi Myllärniemi

TIIVISTELMÄ

OSSI HUTTUNEN: Tietoturvapolitiikan merkitys yrityksen strategiassa
The significance of information security policy in business strategy
Tampereen yliopisto
Kandidaatintyö, 25 sivua
Huhtikuu 2019
Teknis-taloudellinen TkK-tutkinto-ohjelma
Pääaine: Tietojohtaminen
Tarkastaja: Jussi Myllärniemi

Avainsanat: tietoturva, tietoturvapolitiikka, yrityksen strategia

Tietoa on saatavilla jatkuvasti enemmän ja sen suojaaminen on muuttunut ratkaisevaksi tekijäksi yrityksissä liiketoiminnan kannalta. Liiketoiminnan ylläpitämiseksi yritysten täytyy muodostaa strategia, jonka pohjalta yritys toteuttaa toimintaansa. Yrityksen toiminnan ylläpitämiseksi yrityksen on myös huolehdittava tietoturvasta, sillä tieto on yritykselle tärkeä resurssi. Tietoturvan toteuttamiseen liittyy vahvasti tietoturvapolitiikka, joka antaa yritykselle ohjeita tietoturvan toteuttamiseen.

Tutkimuksen toteutustapana oli kirjallisuustutkimus, jossa tavoitteena oli aineiston perusteella etsiä vastaus, miten tietoturva ja tietoturvapolitiikka näkyvät yrityksen strategiassa. Tutkimuksessa käytetty aineisto koostui tieteellisistä julkaisuista, kuten kirjoista, artikkeleista ja konferenssijulkaisuista. Suurin osa käytetystä aineistosta oli sähköisessä muodossa. Tutkimusongelmaa selvitettiin pää- ja tutkimuskysymysten avulla, jotka rajasivat aihetta ja esittivät tarkentavia kysymyksiä, johon tutkimuksessa vastattiin.

Tutkimuksessa selvisi, että tietoturvalla, tietoturvapolitiikalla ja yrityksen strategialla on paljon yhteistä ja ne sitoutuvat monilta osin toisiinsa. Niille löydettiin myös useita määritelmiä. Tietoturva todettiin prosessiksi, josta on vastuussa koko yritys. Tutkimuksessa löydettiin myös, että tietoturva on moniuloitteista ja koostuu useasta tasosta. Myös strategian todettiin koostuvan erilaisista tasoista, jotka mukailevat organisaatiorakennetta. Tutkimuksessa löydettiin tietoturvapolitiikalle erilaisia tapoja jakaa se osiin, esimerkiksi tietoturvapolitiikka-arkkitehtuurin avulla. Lisäksi tietoturvapolitiikan tehokkuuteen yrityksissä löydettiin vaikuttavia tekijöitä. Tutkimuksessa selvisi myös, että tietoturvasta, tietoturvapolitiikasta ja yrityksen strategiasta on vastuussa samoja organisaation johdon henkilöitä.

ALKUSANAT

Tutkimus on toteutettu Tampereen yliopiston tietojohtamisen koulutusohjelmaan keväällä 2019. Tutkimuksen aiheena on tietoturvapolitiikan merkitys yrityksen strategiassa, ja aihe on valittu oman mielenkiinnon ja aiheen ajankohtaisuuden takia.

Haluan kiittää kaikkia kandidaatintyöhöni vaikuttaineita henkilöitä, erityisesti kandidaatintyöni ohjaajaa ja tarkastajaa, Jussi Myllärniemeä, joka antoi rakentavaa palautetta ja ohjeistusta työhön liittyen. Lisäksi haluan kiittää Jukka Huttusta, Lotta Saikkoa, Tiia Erosta, Emma Komulaista sekä Tuukka Haapakumpua rakentavasta palautteesta ja avusta. Suuri kiitos kuuluu myös koko kandidaatintyöseminaarissa mukana olleelle pienryhmälle, jolta sai oleellista palautetta työn eri vaiheissa.

Tampereella, 10.4.2019

Ossi Huttunen

SISÄLLYSLUETTELO

1. JOHDANTO

Tiedon määrä ja tiedon merkitys yhteiskunnassa ovat kasvaneet räjähdysmäisesti internetin yleistymisen myötä ja nykyään tietoa on saatavissa käden käänteessä esimerkiksi älypuhelimista. Tiedon helpon saatavuuden myötä myös tietoon liittyvät uhat ovat kasvaneet ja ne aiheuttavat huolta niin tavallisille ihmisille kuin myös yrityksille. Vaarat voivat liittyä esimerkiksi huolimattomaan sähköpostin käyttöön tai yrityksen tietokoneen jättämiseen paikkaan, jossa yrityksen ulkopuolisella henkilöllä olisi pääsy koneeseen. Esimerkkejä on paljon ja epätodennäköiseltä tai merkityksettömältä kuulostava tietoturvariski saattaa käydä toteen.

Tietoturvan merkitys on muuttunut tärkeäksi osaksi yrityksien toimintaa. Yritykset ovat alttiita erilaisille tietovuodoille ja -hyökkäyksille, joiden takia yrityksille saattaa koitua suuria kuluja. Esimerkiksi vuonna 2017 useisiin suuriin yrityksiin ja organisaatioihin, kuten esimerkiksi Nissaniin, FedExiin ja NSH:iin, kohdistunut kiristysohjelma WannaCry levisi ja sen seurauksena kiristysohjelman uhreja oli yhteensä noin 2 miljoonaa (Mohurle & Patil 2017). Cheng et al. (2017) mukaan tietomurron aiheuttamat kustannukset olivat keskimäärin yli 4 miljoonaa dollaria vuonna 2016. Tietoturvan laiminlyönti saattaa siis aiheuttaa suuria kuluja yrityksissä ja mahdollisesti vaikuttaa yrityksen imagoon.

Tietovuotojen, tietohyökkäysten ja muiden erilaisten tietoturvaa vaarantavien asioiden estämiseksi yrityksiä pyritään velvoittamaan toimimaan lakien ja säädösten avulla, ja suosittelemaan toimimaan muun muassa erilaisten standardien mukaan tietoturvan toteuttamisessa. Kansainvälisesti standardeja ja säädöksiä tietoturvalle määrittävät esimerkiksi OECD (Organisation for Economic Co-operation and Development) ja ISO (International Organization for Standardization). (Seymour et al. 2008) Suomessa yrityksiä velvoittaa huolehtimaan tietoturvasta esimerkiksi Tietosuojalaki, joka täydentää EU:n yleistä tietosuoja-asetusta eli Euroopan parlamentin ja neuvoston asetusta (EU) 2016/679 (Tietosuojalaki 5.12.2018/1050). Yrityksien on taloudellisesti järkevää huolehtia tietoturvasta, sillä sen laiminlyömisestä voi tulla esimerkiksi lain perusteella sanktioita ja sen lisäksi tietoturvan laiminlyönti voi myös aiheuttaa yhtiön maineen huonontumista esimerkiksi asiakkaiden tai sijoittajien silmissä.

1.1 Tutkimuksen rakenne

Tutkimus muodostuu useasta osasta, jotka ovat tutkimuksen menetelmien esittely, teoriaosio ja yhteenveto sekä lähdeluettelo. Tutkimuksessa on johdantoluku mukaan lukien 7 lukua.

Johdannon jälkeisessä luvussa eli luvussa 2, esitellään tutkimusmenetelmät ja tutkimuksessa käytettyä aineistoa. Lisäksi toisessa luvussa esitellään, miten tutkimus on toteutettu ja mitä aineistoa sen toteuttamiseen on käytetty. Kolmannessa luvussa käsitellään yleisesti tietoturvaa ja tiedon käsitettä. Lisäksi luvussa esitellään teorioita, miten tietoturvaa voidaan jakaa osiin ja esitellään, miten tietoturva on muuttunut. Neljäs luku käsittelee tietoturvapolitiikkaa ja erilaisia siihen liittyviä teorioita, kuten esimerkiksi tietoturvapolitiikka arkkitehtuuria eli jakoa pienempiin kokonaisuuksiin. Viides luku käsittelee strategiaa ja siinä esitellään erilaisia strategian käsitteitä ja strategian jakoa erilaisiin osiin. Kuudennessa luvussa käsitellään tietoturvapolitiikan suhdetta yhtiön strategiaan ja organisaation rakennetta tietoturvapolitiikan ympärillä. Viimeinen eli seitsemäs luku on yhteenvetoluku, jossa kootaan tutkimuksessa ilmenneitä asioita yhteen ja esitellään pohdintaa ja päätelmiä sekä jatkotutkimusmahdollisuuksia tutkitun asian ympäriltä.

1.2 Keskeiset käsitteet

Tietoturva

Tietoturvan tehtävänä on tiedon luottamuksellisuuden, saatavuuden ja eheyden takaaminen (Goodman et al. 2008). Tietoturvalla määritellään, mitä tietoa suojellaan, miksi sitä suojellaan ja millä tavalla sitä suojellaan (Alberts & Dorofee 2002). Tiedon turvaaminen keskittyy ihmisiin, tuotteisiin ja prosesseihin (Desouza & Vanapalli 2005).

Tietoturvapolitiikka

Tietoturvapolitiikka on dokumentti, joka ohjaa tai sääntelee ihmisten tai järjestelmien tekoja (Lopes et al. 2017). Alqahtanin (2017) mukaan huono tietoturvapolitiikka voi johtaa tärkeän tiedon suojaamattomuuteen.

Tietohallintojohtaja

Tietohallintojohtaja on henkilö, joka on vastuussa tietoturvapolitiikan luomisesta ja ylläpidosta organisaatiossa (Vacca 2013). Whitmanin ja Mattordin (2013) mukaan tietohallintojohtaja myös hyväksyy tietoturvapolitiikan yrityksessä.

Tieto

Tieto voidaan jakaa dataan, informaatioon ja tietämykseen, ja tieto on aineeton resurssi. Data muodostuu faktoista, joilla ei ole selkeää rakennetta. Informaatio muodostuu rakenteellisesta datasta. Tietämys on kokemukseen perustuvaa tietoa. (Laihonen et al. 2013)

Tietovuoto

Tietovuodolla tarkoitetaan arkaluonteisen tiedon vuotamista luvattomille ulkopuolisille toimijoille. Tietovuoto voi olla aiheutettu tahallisesti tai tahattomasti. (Cheng et al. 2017)

Yrityksen strategia

Yrityksen strategia tarkoittaa, että yritys määrittelee päämääränsä ja toimintansa suhteutettuna toimintaympäristöön, tavoitteenaan menestyä kilpailutilanteessa (Martinsuo et al. 2016).

1.3 Tutkimusongelma

Tutkimuksen tarkoituksena oli selvittää kirjallisuuden avulla, miten tietoturva ja tietoturvapolitiikka näkyvät yrityksen strategiassa. Tutkimusongelmaa on lähdetty selvittämään pää- ja alatutkimuskysymysten avulla, jotka ovat lueteltuna alla.

Päätutkimuskysymys

- Minkälainen rooli tietoturvapolitiikalla on yrityksen strategiassa?

Alatutkimuskysymykset

- Mitä yrityksen tietoturva ja tietoturvapolitiikka tarkoittavat?
- Mistä tietoturva koostuu ja miten tietoturvapolitiikkaa voidaan jaotella?
- Miten tietoturvan rooli on muuttunut yrityksissä verrattuna aiempaan?

Pää- ja alatutkimuskysymysten tavoitteena on täydentää toisiaan sekä olla apuna selvittämässä tutkimusongelmaa.

2. TUTKIMUSMENETELMÄN ESITTELY

Kandidaatintyössä tutkimus toteutettiin kirjallisuuskatsauksena. Finkin (2019) mukaan kirjallisuuskatsauksella tarkoitetaan tutkijoiden ja ammattilaisten luomien valmiiden ja taltioitujen töiden systemaattista tutkimista. Kirjallisuuskatsaus voidaan toteuttaa esimerkiksi seitsemässä vaiheessa, jotka ovat:

1. Tutkimuskysymyksen valitseminen,
2. Tiedonhankintalähteiden valitseminen,
3. Hakulauseiden valitseminen,
4. Käytännöllisen rajauksen toteuttaminen (esim. kielen tai tutkimustyyppien valitseminen),
5. Metodologisen rajauksen toteuttaminen (lähteiden tieteellisen laadun tarkastaminen),
6. Kirjallisuuskatsauksen toteuttaminen,
7. Tulosten synteesi eli yhdistely.

Kirjallisuuskatsaus voidaan toteuttaa monesta erilaisesta alasta, kuten terveydenhuollosta tai liiketoiminnasta. (Finkin 2019)

Tutkimuksessa hyödynnettiin useiden eri tietokantojen lähteitä. Esimerkkejä tietokannoista, joita työssä on käytetty, ovat Andor, Scopus, IEEE Xplore, Google Scholar ja Web of Science sekä SpringerLink. Suurin osa aineistosta löytyi Andorin ja Google Scholarin avulla. Tutkimuksen toteuttamisessa on käytetty erilaisia menetelmiä, kuten helmenkalastusmenetelmää ja edellä mainittua Finkin (2019) kirjallisuuskatsauksen seitsemän vaiheen mallia sovellettuna. Esimerkiksi vaiheita ei täysin noudatettu samassa järjestyksessä kuin mallissa. Aiheesta löytyi runsaasti materiaalia englanniksi, joka toimi tiedonhaussa pääkielenä. Apuna erilaisten termien ja käsitteiden suomentamiseen käytin MOT-sanakirjaa ja sanakirja.org-sivustoa.

2.1 Hakusanojen ja niiden tuloksien määrien esittelyä eri tietokannoista

Taulukossa 1 on koottuna erilaisia hakusanoja eri tietokannoista ja niiden tuloksien määriä. Tulosten rajaamiseksi olen osassa hakusanoista käyttänyt Boolen operaattoreita (AND, OR ja NOT) ja fraasihakua sekä niiden yhdistelmiä. Taulukon 1 tarkoituksena on havainnollistaa erilaisten hakusanojen ja fraasien tuloksia, joiden avulla aineistoa on pyritty rajaamaan yhä pienempiin tuloksiin.

Taulukko 1. *Esimerkkejä erilaisista hakusanoista eri tietokannoista ja niiden tulosten määristä*

Hakusana	**Tietokanta**	**Tulosten määrä**
information security	Andor	26434869
	Google Scholar	3670000
	Web of Science	69333
information security policy	Andor	5520370
	Google Scholar	3510000
	Web of Science	7316
"information security in companies"	Andor	8319
	Google Scholar	82
information security AND company's strategy	Andor	4240998
	Google Scholar	167000
	Scopus	728
"information security policy" AND "company's strategy"	Andor	44
	Google Scholar	23
"information security policy" AND "strategy" AND "information security governance"	Andor	196
	Google Scholar	789

Taulukosta 1 huomataan, että hakutulosten tarkentuessa myös tulosten osumien määrä väheni niin pieneksi, että niitä pystyi tarkastelemaan huomattavasti tehokkaammin kuin väljien hakusanojen antamia tuloksia. Osa aineistosta on löytynyt tarkoilla hakusanoilla, jotka tuottivat vain vähän tuloksia ja osa aineistosta on taas löytynyt hakusanoilla, jotka

tuottivat suuren määrän tuloksia. Hakutuloksia on rajattu myös vuosiluvun perusteella, tavoitteena löytää mahdollisimman uutta ja relevanttia tietoa aiheista.

2.2 Tutkimuksessa käytetty aineisto

Tutkimuksessa hyödynnetty aiheeseen liittyviä kirjoja, artikkeleita, konferenssien julkaisuja sekä viranomaislähteitä. Suurin osa aineistosta oli sähköistä aineistoa ja kieleltään englanninkielistä. Taulukossa 2 on koottuna muutamia olennaisia työssä käytettyjä teoksia.

Taulukko 2. *Tutkimuksen kannalta tärkeitä aineistoja*

Tekijät	**Julkaisu-vuosi**	**Otsikko**	**Tyyppi**	**Merkitys tutkimuksen kannalta**
Peltier, T. R.	2014	Information security fundamentals.	e-kirja	Kirja sisältää yleisesti paljon asioita tietoturvasta ja tietoturvapolitiikasta.
von Solms, R. ja von Solms, S. H.	2009	Information Security Governance	e-kirja	Kirjasta kuvataan tietoturvapolitiikkaa ja tietoturvapolitiikka arkkitehtuuria sekä tietoturvanhallintaa.
Whitman, M. ja Mattord, H.	2013	Management of information security.	e-kirja	Kirjassa esitellään laajasti tietoturvaa ja tietoturvapolitiikkaa sekä strategiaa.
Alam, M ja Bokhari, M. U.	2007	Information Security Policy Architecture.	Konferenssi-julkaisu	Tietoturvapolitiikka arkkitehtuurimallin esittely.

Taulukossa 2 esitellyt lähteet ovat laajoja ja antavat hyvän yleiskuvan tietoturvasta, tietoturvapolitiikasta ja strategiasta. Niiden lisäksi tutkimuksessa on käytetty paljon muita tutkimuksen kannalta olennaisia aineistoja. Suurin osa tutkimuksessa käytetystä aineistosta on suhteellisen uutta eli 2000-luvulta ja 2010-luvulta.

3. TIETOTURVA

Tietoturva on nykyään yksi suurimmista organisaatioiden huolista ja se on saanut suurta huomiota organisaatioissa sen myötä, kun organisaatioissa on otettu käyttöön uusia tieto- ja viestintäteknologioita (Alqahtani 2017). Tieto- ja viestintäteknologioihin lukeutuvat esimerkiksi tietokonelaitteet, ohjelmistot, tietoliikenteen laitteet ja järjestelmät sekä palvelut (Pelkonen 2003).

Tietoturva on osa yrityksen turvallisuutta. Turvallisuudella tarkoitetaan asemaa, jossa ollaan turvassa vaaralta. (Whitman & Mattord 2011) Yleensä sopiva turvallisuustaso organisaatiolle saavutetaan käyttämällä samanaikaisesti useaa eri strategiaa tai niiden yhdistelmää (Whitman & Mattord 2013). On kuitenkin vaikea määrittää tarkasti tarkkaa tilaa, milloin on saavutettu turvallinen asema (Andress 2011). Muita organisaation turvallisuuden osa-alueita ovat esimerkiksi fyysinen turva, henkilöstön turva ja operaatioiden turva (Whitman & Mattord 2011).

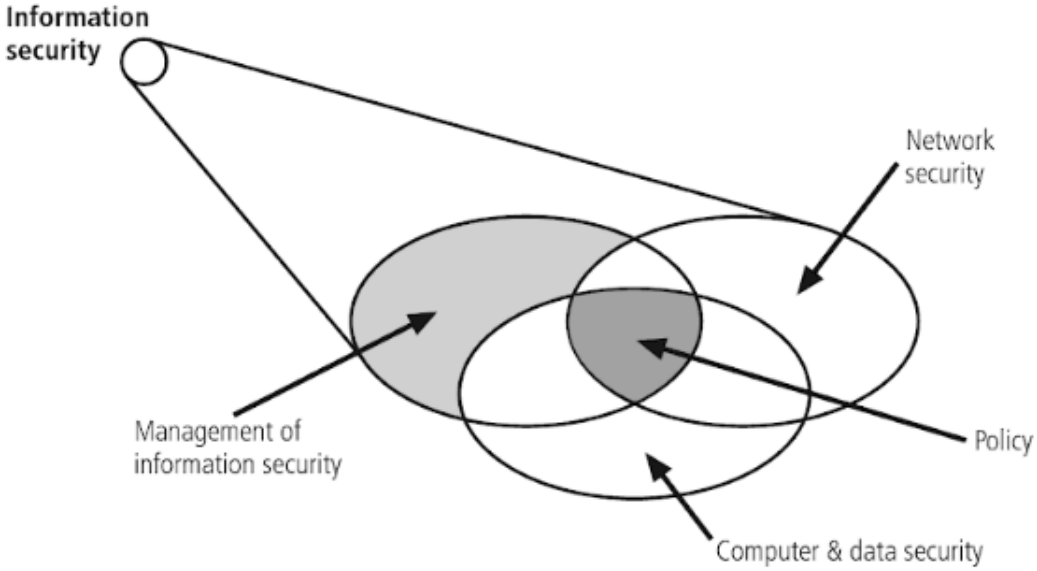
Yrityksille tieto on aineeton resurssi, jonka arvoa on vaikea arvioida ja tieto voi sijaita ympäri organisaatiota (Laihonen et al. 2013). Tietoa käytetään yrityksen jokaisessa osa-alueessa ja tiedosta on tullut välttämätön osa liiketoiminnan aloittamista ja ylläpitämistä (Lopes et al. 2017). Tietoa luodaan organisaatiossa jatkuvasti ja sen perusteella tehdään uusia päätöksiä (Ilvonen et al. 2015).

Tietoturvaan ei ole olemassa yksittäistä tietoturvatuotetta tai tuoteyhdistelmää, jonka avulla luotaisiin tietoturvallinen organisaatio. Tietoturva on prosessi, joka muodostuu sekä tietoturvatuotteista että ihmisistä, jotka konfiguroivat ja ylläpitävät turvallisuutta. (Vacca 2013) Tietoturvasta on siis vastuussa koko organisaatio. Tietoturva voidaan saavuttaa politiikan, koulutuksen, harjoittelun, tietoisuuden ja teknologian avulla (Whitman & Mattord 2011). Tietoturvaan vaikuttaa myös organisaation kulttuuri. Nosworthyn (2000) mukaan organisaation kulttuuri on olennaisessa osassa organisaation tietoturvassa. Kulttuuri on ryhmän muodostama malli jaetuista perusolettamuksista, jotka muodostuvat riittävän hyvin onnistuneesta ongelmanratkaisusta. Tällöin perusolettamuksia voidaan opettaa ryhmän uusille jäsenille oikeana tapana hahmottaa, ajatella ja tuntea ratkaistavia ongelmia. (Schein 2010)

3.1 Tietoturvan osat ja luonne

Tietoturvan komponentit ovat Whitman ja Mattord (2013) mukaan tietoturvan johtaminen (management of information security), kyber- ja dataturvallisuus (computer & data security) ja verkkoturvallisuus (network security) sekä näistä muodostuva politiikka

(*policy*). Tietoturvan komponentit ovat esitettynä kuvassa 1. Da Veigan ja Eloffin (2010) mukaan tietoturvan komponentit ovat johtaminen ja hallinto (leadership and governance), turvallisuuden hallinta ja turvallisuusoperaatiot (security management and operations), turvallisuuspolitiikat (security policies), turvallisuusohjelman hallinta (security program management), käyttäjäturvanhallinta (user security management), teknologian suojaaminen ja operointi (technology protection and operations), ja muutos (change).



Kuva 1 *Tietoturvan komponentit (Whitman & Mattord 2013)*

Tietoturvan (information security) tehtävänä on tiedon luottamuksellisuuden, saatavuuden ja eheyden takaaminen (Goodman et al. 2008). Tiedon luottamuksellisuus (confidentiality), eheys (integrity) ja saatavuus (availability) muodostavat CIA kolmion (von Solms & van Niekerk 2013). Whitmanin ja Mattordin (2013) mukaan tietoturva on kuitenkin laajentunut kattavammaksi kokoelmaksi tärkeitä erityispiirteitä ja prosesseja, kuten yksityisyys, identifointi ja tunnistautuminen.

Tiedon luottamuksellisuudella tarkoitetaan, että tieto on saatavilla vain henkilöille tai systeemeille, jotka tarvitsevat kyseistä tietoa ja joilla on tietoon pääsy (Vacca 2013). Luottamuksellisuutta voidaan suojata esimerkiksi tiedon luokittelulla, salauksella ja yleisten turvallisuuspolitiikoiden käytöllä (Whitman & Mattord 2013). Luottamuksellisuus voidaan saavuttaa salaamalla tieto niin, että vain tietyt henkilöt voivat avata salauksen. Luottamuksellisuus pitää taata kaikilla systeemin osa-alueella. (Vacca 2013)

Tiedon saatavuus tarkoittaa, että tieto pitää olla saatavilla sillä hetkellä, kun sitä tarvitaan. Tiedon saatavuutta tarvitaan prosesseihin, sillä kaikkien prosessien suorittamiseen tarvitaan dataa. Ilman pääsyä dataan, prosessia ei voida suorittaa. (Vacca 2013) Tiedon tulee olla saatavilla ilman häiriöitä tai keskeytystä ja sen pitää olla luettavassa muodos-

sa. Lisäksi tieto tulee olla saatavilla vain valtuutetuille henkilöille. (Whitman & Mattord 2013)

Tiedon eheydellä tarkoitetaan, että tietoa voi lisätä tai päivittää vain henkilöt, joilla on pääsy ja tarve kyseiseen tietoon. (Vacca 2013) Eheys on tila, jossa tieto on ehjää, kokonaista ja korruptoimatonta. Eheyttä voidaan ylläpitää suojaamalla tieto sisäisiltä ja ulkoisilta uhilta esimerkiksi systeemien virheenhallinta tekniikoilla. Tiedon eheys on uhattuna, mikäli siihen kohdistuu korruptiota tai vaurioitumista. Korruptio voi tapahtua tiedon syötössä, tallentamisessa tai siirrossa. (Whitman & Mattord 2013) Korruptiolla tarkoiteaan tiedon muuttumista lukemattomaan muotoon.

Tietoturvalla määritellään, mitä tietoa suojellaan, miksi sitä suojellaan ja millä tavalla sitä suojellaan (Alberts & Dorofee 2002). Tiedon turvaaminen keskittyy ihmisiin, tuotteisiin ja prosesseihin (Desouza & Vanapalli 2005). Tietoturva pyrkii uhkien suojaamisen avulla takaamaan liiketoiminnan jatkumisen, minimoimaan riskejä ja maksimoimaan sijoitetun pääoman tuoton sekä mahdollistamaan liiketoimintamahdollisuudet (Lopes et al. 2017).

Tietoturva on luonteeltaan moniuloitteista. Tietoturvan ulottuvuudet ovat strategisia, taktisia ja operationaalisia. Erilaisia ulottuvuuksia ovat esimerkiksi hallinnollinen ulottuvuus, tekninen ulottuvuus ja polittinen ulottuvuus. (von Solms & von Solms 2009b)

3.2 Tietoturvan muutos

Informaatioteknologian kehittyessä myös tietoturva on kehittynyt yrityksissä ja muuttunut erilaiseksi. Tietoturvaan panostetaan yrityksissä huomattavasti aiempaa enemmän johtuen esimerkiksi kasvaneista riskeistä informaatioteknologiassa.

Vielä 1990-luvulla tietoturva koettiin tärkeydeltään vähäiseksi eikä internet rakentunut vielä standardien ympärille. Tietoturva muodostui tuolloin vielä datakeskusten fyysisestä turvasta. Kun internet yleistyi, datakeskusten fyysinen turva ei enää riittänyt suojaamaan tietoa ja tieto oli yhä alttiimpana tietoturvauhille. Tietoturva 2000-luvulla alkoi kehittymääm olennaiseksi osaksi tietokoneita ja tietoisuus tietoturvan merkityksestä alkoi leviämään laajemmalle. (Whitman & Mattord 2011)

Peltierin (2013) mukaan yrityksissä tietoturvan vastuu on vaihtunut vuosien mittaan tietokoneista vastanneesta turvallisuusyksiköstä koko yrityksen tietoturvasta vastaavaan koko yrityksen laajuiselle tietoturvayksikölle. Yritysten tietoturvaan on tuonut suuria muutoksia esimerkiksi EU:n yleinen tietosuoja-asetus. Se astui voimaan 24.5.2016 ja sitä alettiin soveltamaan 25.5.2018 (Euroopan komissio 2019e). EU:n yleinen tietosuoja-asetus velvoittaa yrityksiä huolehtimaan henkilötiedoista ja niiden käsittelystä asetuksen edellyttämällä tavalla (Euroopan komissio 2019a). Yrityksillä on esimerkiksi velvollisuus ilmoittaa yrityksen tietoturvaan kohdistuneista hyökkäyksistä 72 tunnin

sisällä sen huomaamisesta (Euroopan komissio 2019d). Yrityksillä on myös oltava tietosuojavastaava, mikäli yritys käsittelee henkilötietoja (Euroopan komissio 2019c). Mikäli yritys ei noudata EU:n yleisen tietosuoja-asetuksen velvoitteita, yritys voi saada sakon, joka on maksimissaan 20 miljoonan euroa tai 4% liikevaihdosta (Euroopan komissio 2019b).

Informaatioteknologia kehittyy jatkuvasti, joten sen myötä myös tietoturva muuttuu. Tulevaisuudessa tietoturva ja sen menetelmät ovat luultavasti erilaisia kuin nyt. Myös tietoturvaan lait ja yritysten käytännöt muuttuvat ja päivittyvät ajalle sopivaan muotoon.

4. TIETOTURVAPOLITIIKKA

Yleisesti politiikalla tarkoitetaan yleistä sääntöä, jolla ohjataan työntekijöitä organisaatiossa (Knapp et al. 2009). Peltierin (2013) mukaan politiikka on korkean tason ohje yrityksen uskomuksista, tavoitteista ja päämääristä.

Informaatioteknologiaan liittyessä politiikalla tarkoitetaan tietoturvapolitiikkaa. Tietoturvapolitiikalla tarkoitetaan työntekijöiden hyväksytyn käyttäytymisen, päätösten rajojen ja standardien suunnittelua ja hallitsemista. (Knapp et al. 2009) Tietoturvapolitiikka on dokumentti, joka ohjaa tai sääntelee ihmisten tai järjestelmien tekoja (Lopes et al. 2017). Peltierin (2013) mukaan tietoturvapolitiikka on dokumentti yrityksen laajuisesta päätöksenteosta, miten tietoa käsitellään ja turvataan. Alan ja Bokhari (2007) määrittelevät tietoturvapolitiikan kokoelmaksi turvallisuusvaatimuksia, joita systeemin pitää valvoa, ja tietoturvapolitiikan päämääränä on suojata tietoa luvattomalta käytöltä, muutokselta ja tuholta.

Ilman kunnollista tietoturvapolitiikkaa on hyvin vaikeaa tai mahdotonta toteuttaa tietoturvaa organisaatiossa (von Solms & von Solms 2009b). Heikko tietoturvapolitiikka saattaa johtaa tärkeän tiedon suojaamattomuuteen tai työntekijöiden organisaatiolle haitallisiin tekoihin (Alqahtani 2017). Tietoturvapolitiikka on siis tärkeä dokumentti yritykselle, ja sen laiminlyönnillä voi olla merkittäviä seurauksia.

Tietoturvapolitiikan kehittämisessä on välttämätöntä käyttää erilaisia tietoturvaan liittyviä standardeja. Standardit ovat pakollisia vaatimuksia, jotka tukevat yksittäisiä politiikkoja. (Peltier 2013) Tietoturvaan liittyviä standardeja ovat esimerkiksi COBIT (Control Objectives for Information and Related Technologies), GASSP (Generally Accepted System Security Principles) ja GMITS (Guidelines to the management of information technology security) sekä ISO/IEC 27002 (Höne & Eloff 2002a, von Solms & van Niekerk 2013)

Höne ja Eloff (2002a) mukaan tietoturvapolitiikkadokumentti koostuu useasta erilaisesta elementistä:

- tarpeen ja laajuuden sekä tavoitteiden määrittelystä,
- tietoturvan määrittelystä,
- johdon sitoutumisesta tietoturvaan,
- tietoturvapolitiikan tarpeesta tai tehtävästä,
- tietoturvan periaatteista,
- rooleista ja vastuista,
- tietoturvapolitiikan rikkomisen ja kurinpidon toimista,
- valvonnasta ja arvioinnista,
- käyttäjien tiedoksiannosta ja hyväksymisestä,
- ristikkäisistä viittauksista,
- kirjoittajista, päivämäärästä ja politiikan hyväksymispäivämäärästä.

Tietoturvapolitiikkadokumentin elementit muodostavat siis laajan kokonaisuuden erilaista tietoturvan kannalta olennaisista osista.

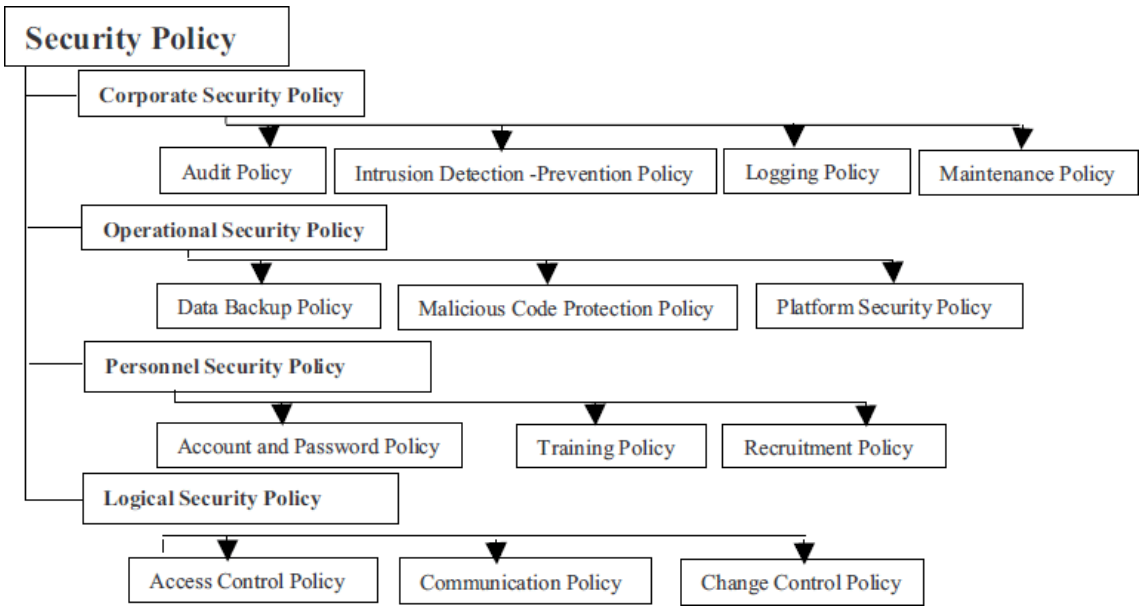
4.1 Tietoturvapolitiikan osa-alueet

Tietoturvapolitiikka voidaan jakaa monella erilaisella tavalla, eikä siihen ole yhtä yhtenäistä tapaa. Kirjallisuudessa tietoturvapolitiikan osa-alueita esitetään suoraan jakamalla tietoturvapolitiikka osiin tai arkkitehtuurimallilla.

Tietoturvapolitiikka voidaan jakaa kolmeen osaan: yleiseen, aihekohtaiseen ja sovelluskohtaiseen tietoturvapolitiikkaan. Yleinen eli tason 1 tietoturvapolitiikkaa käytetään organisaation yleisen näkemyksen ja suunnan luomiseen. Aihekohtaista eli tason 2 tietoturvapolitiikkaa sovelletaan tarkemmin konsernin tiettyihin kohteisiin, kuten sosiaaliseen mediaan, jotka tukevat tason 1 tietoturvapolitiikkaa. Sovelluskohtainen eli tason 3 tietoturvapolitiikka keskittyy tiettyyn systeemiin tai sovellukseen. (Peltier 2013)

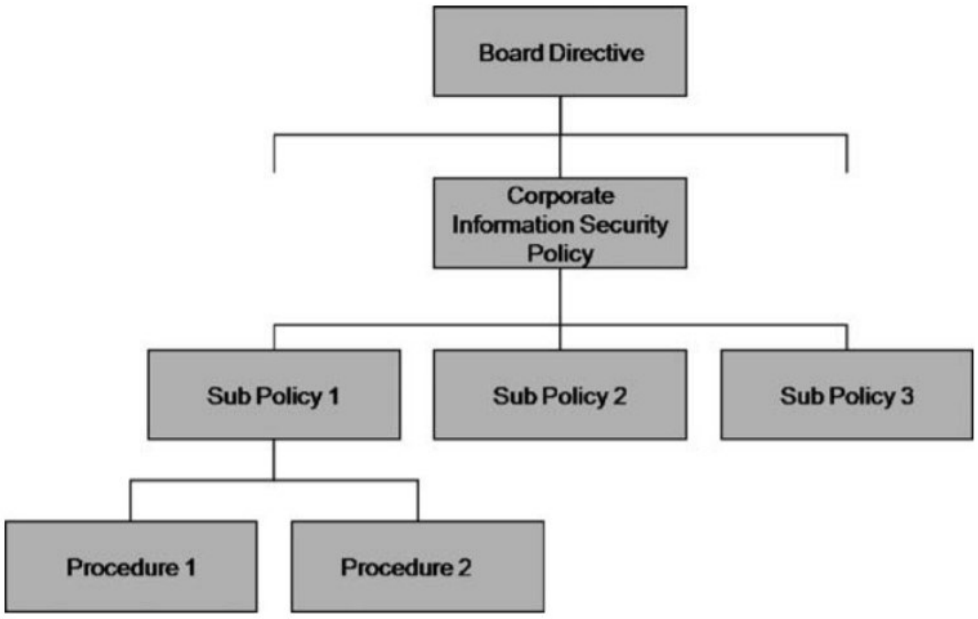
Whitman ja Mattord (2013) jakavat tietoturvapolitiikan yhtiön tietoturvapolitiikkaan (Enterprise information security policy, EISP), ongelmakohtaiseen tietoturvapolitiikkaan (Issue-specific security policy, ISSP) ja systeemikohtaiseen tietoturvapolitiikkaan (System-specific security policy, SysSP). Yhtiön tietoturvapolitiikka määrittelee yleisesti tietoturvan yhtiössä ja se on kehitetty yhtiön strategisen informaatiotekniikan mukaan. (Whitman & Mattord 2013) Vaccan (2013) mukaan tietohallintojohtaja on vastuussa yrityksessä tietoturvapolitiikan luomisesta ja ylläpidosta. Yhtiön tietoturvapolitiikan on hyväksynyt joko tietohallintojohtaja tai toimitusjohtaja (Whitman & Mattord 2013). Ongelmakohtainen tietoturvapolitiikka taas määrittelee, miten tietoturvaa sovelletaan tietylle teknologialle, kuten internetin käytölle. Systeemikohtainen tietoturvapolitiikka on luonteeltaan teknistä tai johdannollista ja sitä sovelletaan tietyn laitteen tai teknologian konfiguroinnin kontrolloimiseen. (Whitman & Mattord 2013)

Alam ja Bokhari (2007) esittää tietoturvapolitiikan arkkitehtuurin, joka jakaa tietoturvapolitiikan yhtiötietoturvapolitiikkaan (Corporate Security Policy), operationaaliseen tietoturvapolitiikkaan (Operational Security Policy), henkilöstön tietoturvapolitiikkaan (Personnel Security Policy) ja loogiseen tietoturvapolitiikkaan (Logical Security Policy). Yhtiötietoturvapolitiikka sovelletaan organisaation rakenteisiin ja niiden suhteisiin ulkopuolisiin kokonaisuuksiin, kuten standardeihin. Operationaalinen tietoturvapolitiikka määrittelee organisaation tietoturvan toimintatavat, kuten haitallisen koodin estämisen ja tiedon varmuuskopioinnin. Henkilöstön tietoturvapolitiikka määrittelee, miten tietoturvaa sovelletaan tietyissä työyksiköissä. Looginen tietoturvapolitiikka määrittelee erilaisten loogisten mittareiden avulla tiedon pääsynhallintaa. (Alam & Bokhari 2007) Kuvassa 2 on esitettynä tietoturvapolitiikan arkkitehtuuri, josta huomataan, että tietoturvapolitiikan osapolitiikat jakautuvat yhä pienempiin osapolitiikkoihin.



Kuva 2 *Tietoturvaopolitiikan osa-alueet (Alam & Bokhari 2007)*

Von Solms ja von Solms (2009a) esittävät tietoturvapolitiikan arkkitehtuurin (Information security policy architechture, ISPA), joka on esitetty kuvassa 3. Tietoturvapolitiikan arkkitehtuuri koostuu yrityksen tietoturvapolitiikasta (Corporate Information Security Policy, CISP), joka jakautuu useaan osapolitiikkaan, jotka taas jakautuvat erilaisiin proseduureihin. Proseduurit kertovat miten tietty politiikka pitää käytännössä toteuttaa. Yrityksen tietoturvapolitiikka muodostuu yrityksen hallituksen ohjeistuksesta (Board Directive) ja sen hyväksyy yrityksen toimitusjohtaja tai muu vastaavan tason johtaja. Erilaisia yrityksen tietoturvaspolitiikasta jakautuvia osapolitiikoita ovat esimerkiksi virustentorjuntapolitiikka, internetin käyttöpolitiikka ja varmuuskopiointipolitiikka. (von Solms & von Solms 2009a)



Kuva 3 *Tietoturvapolitiikka arkkitehtuuri (von Solms & von Solms 2009a)*

Tietoturvapolitiikkaa voidaan siis jakaa useaan erilaisiin osaan ja tietoturvapolitiikasta voidaan muodostaa erilaisia tietoturvapolitiikka-arkkitehtuureja. Eloff ja Eloff (2005) mukaan tietoturvapolitiikan arkkitehtuurin pitäisi olla organisaation koosta, luonteesta ja tyypistä riippumatta käsitteellinen, sisältää kattavaa tietoturvan riskienhallintaa ja olla mitattavissa.

4.2 Tietoturvapolitiikkaan ja sen tehokkuuteen vaikuttavat tekijät

Tietoturvapolitiikkaan ja sen tehokkuuteen vaikuttavat useat erilaiset tekijät. Organisaatiokulttuuri on yksi merkittävä tietoturvapolitiikan tehokkuuteen vaikuttavista tekijöistä, koska organisaatiokulttuurilla on vaikutusta työntekijöiden käsitykseen tiedosta (Knapp et al. 2009; Adéle 2016). Organisaatiokulttuurin lisäksi tietoturvaan ja tietoturvapolitiikkaan vaikuttaa myös organisaation tietoturvakulttuuri (Adéle 2016). Tietoturvapolitiikan lukemisella on positiivinen vaikutus tietoturvakulttuuriin. Muita tietoturvapolitiikkaan ja sen tehokkuuteen vaikuttavia tekijöitä ovat esimerkiksi tietoturvatietoisuus (information security awareness) ja harjoittelu. (Adéle 2016)

Tehokkaassa tietoturvapolitiikassa käyttäjien pitäisi tunnistaa selkeästi miten tietoa pitäisi käsitellä, jotta se toteuttaa tietoturvapolitiikan vaatimukset. Tietoturvapolitiikan tehokkuus ei myöskään ole täysin riippuvainen sisällön tiedon oikeellisuudesta, vaan tavasta miten tieto on dokumentissä esitetty ja onnistutaanko tieto välittämään tietoturvapolitiikan käyttäjille. Lisäksi tietoturvapolitiikan tehokkuuteen vaikuttaa dokumentin tyyli, kehitys, huolto, esitystapa, sitoutuminen ja levittäminen. (Höne & Eloff 2002b)

Tehokkaan tietoturvapolitiikan kehittämisessä ja toteuttamisessa johdon, työntekijöiden ja sidosryhmien tukea koko prosessin ajan. Tietoturvapolitiikan sidosryhmiä ovat esimerkiksi tekninen henkilökunta, henkilöstö, lakimiehet ja yrityksen ulkoiset edustajat. (Flowerday & Tuyikeze 2016) Tietoturvapolitiikan tehokkuuttaa lisää myös se, että työntekijöille korostetaan, että tietoturvapolitiikka on hyödyllinen työkalu (Karolsson et al. 2017).

Mikäli tietoturvapolitiikan kehittämisessä ja toteuttamisessa ei huomioida tietoturvapolitiikan tehokkuuteen vaikuttavia tekijöitä, on riskinä, että yritys kehittää tietoturvapolitiikan, joka on turha ja epäoleellinen, eikä saa käyttäjien tukea. (Flowerday & Tuyikeze 2016) Käyttäjien tuella tarkoitetaan, ettei yrityksen henkilöstö käytä tietoturvapolitiikkaa, kuten on suunniteltu.

5. YRITYKSEN STRATEGIA

Yrityksen strategia on käsitteenä laaja ja se voidaan jakaa useisiin erilaisiin tarkempiin käsitteisiin ja osiin, riippuen siitä, mihin strategia kohdistuu. Strategiaan on useita erilaisia määritelmiä ja näkökulmia.

5.1 Strategian määritelmä ja strategiaan liittyviä käsitteitä

Martinsuo et al. (2016) määrittelevät yrityksen strategian niin, että yritys määrittelee päämääränsä ja toimintansa suhteutettuna toimintaympäristöön, tavoitteenaan menestyä kilpailutilanteessa. Scholes et al. (2002) mukaan strategia on organisaation pitkäaikainen suunta, joka tuottaa kilpailukyvyn muuttuvassa ympäristössä resurssien ja pätevyyden avulla sekä täyttää sidosryhmien odotukset. Mintzberg (1987) taas määrittelee strategian yhtenäiseksi, kokonaisvaltaiseksi ja yhtenäistetyksi suunnitelmaksi, jonka tavoitteena on varmistaa, että yrityksen tavoitteet toteutuvat.

Whitmanin ja Mattordin (2013) mukaan strategian onnistuminen vaatii, että se virtaa organisaation ylimmästä johdosta organisaation kaikille tasoille, ja sen toteuttamiseksi vaaditaan systemaattinen menetelmä. Strategian kehitys siis lähtee yrityksen johdosta ja organisaation muut jäsenet noudattavat kehitettyä strategiaa sen strategian linjan mukaisesti.

Strategiaan liittyy myös käsite strateginen suunnittelu (Strategic planning). Strateginen suunnittelu ohjaa yrityksen pitkän aikavälin suuntaa ja kohdistaa resursseja tarkasti määriteltyihin tavoitteisiin muuttuvassa ympäristössä. Strategisen suunnittelun avulla voidaan toteuttaa taktista suunnittelua (Tactical planning), joka pilkkoo strategiset päämäärät pienemmiksi tavoitteiksi. Taktinen suunnitelma voi olla esimerkiksi projektin suunnitelma. Taktinen suunnittelu taas jakautuu operatiiviseen suunnitteluun (operational planning), joka on taktisen suunnittelun avulla toteutettavaa päivittäisten tehtävien suorittamista. (Whitman & Mattord 2013)

Strategialla on osuus myös organisaatiokulttuuriin, sillä organisaatiokulttuuri kehittyy organisaation vision ja strategian kehityksen sekä työntekijöiden tietotaidon myötä myötä (Adéle 2016). Organisaatiokulttuuri on Slater (2011) mukaan myös tärkeä yrityksen resurssi, sillä se lisää tehokkuutta organisaatiossa.

5.2 Strategian osat

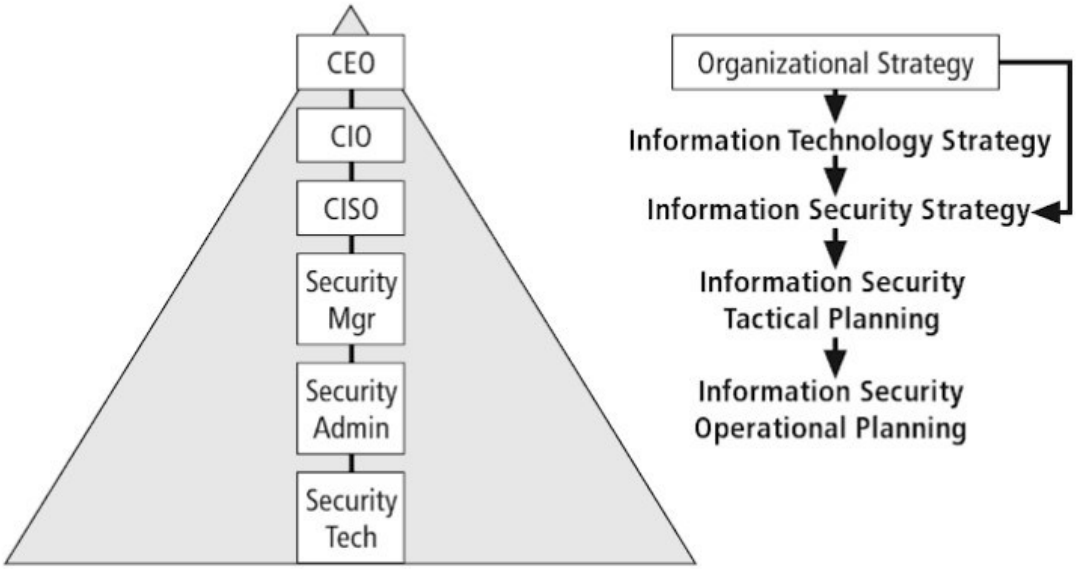
Strategia voidaan jakaa kolmeen osaan: yritystason strategia (corporate-level strategy), liiketoimintatason strategia (business-level strategy), ja operatiivinen strategia (operational strategy). Yritystason strategia määrittelee organisaation yleisen näkemyksen ja sen, miten liiketoiminta luo organisaatiolle arvoa. Liiketoimintatason strategia määrittelee miten yrityksen yksittäisten liiketoimintojen pitäisi kilpailla niiden markkina-alueilla. Operatiivinen strategia määrittelee, miten organisaation komponentit, eli resurssit, prosessit ja ihmiset, toteuttavat yritystason ja liiketoimintatason strategiaa. (Johnson et al. 2015)

Yrityksen strategiaan linkittyy olennaisesti käsite liiketoimintastrategia (business strategy). Liiketoimintastrategia on Croteaun ja Bergeron (2001) mukaan päätöksenteosta organisaatiolle syntyvä ohjeistus, joka ottaa huomioon organisaatioympäristön, rakenteen ja prosessit, jotka vaikuttavat organisaation suorituskykyyn. Nykyään liiketoimintastrategian toteuttamisessa olennaisena työkaluna toimii informaatioteknologia, jonka vuoksi liiketoimintastrategiaan kytkeytyy vahvasti myös informaatioteknologiastrategia (information technology strategy, IT strategy) (Rathnam & Johnsen 2005). Informaatioteknologiastrategia keskittyy pääosin erilaisiin teknologiapolitiikkoihin ja niihin liittyviin näkökulmiin, kuten teknologian arkkitehtuuriin, standardeihin, turvallisuustasoihin ja riskeihin suhtautumiseen. Muita liiketoimintastrategian strategioita ovat esimerkiksi tietojärjestelmästrategia (information systems strategy, IS strategy) ja tietohallintostrategia (information management strategy). (Sabherwal & Chan 2001)

6. TIETOTURVA JA TIETOTURVAPOLITIIKKA YRITYKSEN STRATEGIASSA

Tietoturva ja tietoturvapolitiikka ovat merkittävässä osassa yrityksen strategiassa. Yrityksen johdon tehtävänä on asettaa oikeanlainen strategia ja yhdistää siihen tietoturva (Knapp et al. 2006). Tietoturvan liittämisessä yrityksen strategiaan olennaisessa osassa on tietoturvapolitiikka, joka antaa yritykselle ohjeet, miten tietoturvaa tulisi toteuttaa.

Kun yritys on kehittänyt yleisen strategian, yrityksen täytyy luoda strateginen suunnitelma laajentamalla yleistä strategiaansa tarkemmiksi yksittäisiksi strategioiksi yrityksen eri osa-alueille (Whitman & Mattord 2013). Kuvassa 4 on esitettynä strategiat ja organisaation jäsenet organisaation informaatioteknologian näkökulmasta.



Kuva 4 Strategiat informaatioteknologian näkökulmasta (Whitman & Mattord 2013)

Organisaation strategia jakautuu informaatioteknologiastrategiaksi, joka taas jakautuu tietoturvastrategiaksi. Tietoturvastrategia on luonteeltaan samanlainen kuin mikä tahansa liiketoimintastrategia, eli tavoitteena on resurssien avulla kehittyä ja päästä tavoitteisiin (Sveen et al. 2009). Tietoturvastrategiassa resurssit ovat yrityksen tietoturvaan liittyviä erilaisia resursseja. Tietoturvastrategiaa sovelletaan taktisella suunnittelulla eli tietoturvan suunnittelua esimerkiksi projektin tasolla. Taktisesta suunnittelusta jalostuu tietoturvan operatiivinen suunnittelu, joka tietoturvaan liittyvien päivittäisten toimien suunnittelusta. Organisaation korkeimpien tasojen johtajat, eli toimitusjohtaja (Chief

executive officer, CEO), tietohallintojohtaja (Chief information officer, CIO) ja tietoturvajohtaja (Chief information security officer, CISO), ovat vastuussa strategioista ja taktisesta, ja operationaalisesta suunnittelusta vastaavat alemman tason johto ja työntekijät. (Whitman & Mattord 2013)

Von Solms & von Solms (2009a) esittävät tietoturvanhallintamallin, jossa johdon tasot muodostuvat strategisesta, taktisesta ja operatiivisesta tasosta. Tietoturvanhallintamallin prosessia ohjataan ylimmältä johdolta alimmalle yrityksen tasolle. Jokaisella tasolla on panoksia (input) ja tuotos (output). Strateginen taso koostuu yrityksen ylimmästä johdosta, ja se saa panoksena on ulkoisia ja sisäisiä tekijöitä. Ulkoisia tekijöitä ovat esimerkiksi lailliset tekijät. Sisäisiä tekijöitä ovat esimerkiksi yrityksen strateginen visio ja informaatioteknologian sijoittuminen yrityksen strategiassa, jotka strateginen taso antaa tuotoksena alemmalle tasolle, eli taktiselle tasolle. Taktisella tasolla, joka muodostuu keskitason johdosta, strategisen tason antamat toimintaohjeet toimivat panoksina, ja niitä laajennetaan joukoksi erilaisia tietoturvapoliitikoita, yrityksen standardeja ja proseduureja, jotka muodostavat myös taktisen tason tuotoksen. Operatiivinen taso saa panoksena taktisen tason tuotoksen, eli joukon erilaisia tietoturvapoliitikoita, yrityksen standareja ja proseduureja, jotka operatiivisella tasolla laajennetaan ohjeistuksiksi ja proseduureiksi. Nämä ohjeistukset ja proseduurit toimivat operatiivisen tason tuotoksena, joita toteutetaan alemmilla yrityksen tasoilla, kuten työntekijöillä. (von Solms & von Solms 2009a)

7. YHTEENVETO JA JOHTOPÄÄTÖKSET

Tutkimuksessa lähdettiin tarkastelemaan tietoturvan ja tietoturvapolitiikan merkitystä yrityksen strategiassa. Tutkimuksessa löydettiin tietoturvalle useita määritelmiä sekä selvitettiin mistä tietoturva koostuu. Lisäksi tutkimuksessa tarkasteltiin tietoturvan muutosta, josta selvisi tietoturvan muuttuneen paljon informaatioteknologian kehittymisen myötä ja tietoturvan luonteen yrityksissä olevan erilaista kuin ennen. Tutkimuksessa myös selvitettiin, että tietoturvaa ohjataan kansainvälisillä standardeilla ja säädöksillä sekä laeilla.

Tutkimuksessa määriteltiin tietoturvapolitiikka ja esiteltiin, miten se liittyy osaksi tietoturvaa. Lisäksi selvitettiin erilaisia tapoja jakaa tietoturvapolitiikkaa erilaisiin pienempiin kokonaisuuksiin erilaisten tietoturvapolitiikka-arkkitehtuurien kautta ja selvisi, ettei ole yksittäistä tapaa jakaa tietoturvapolitiikkaa osiin. Tutkimuksessa löydettiin myös, että tietoturvapolitiikan tehokkuuteen liittyy paljon erilaisia tekijöitä, ja tehokkaan tietoturvapolitiikan toteuttamiseen tarvitaan useita organisaation jäseniä.

Yrityksen strategiaan löytyi monta määritelmää sekä useita strategiaan liittyviä käsitteitä. Lisäksi selvisi, että strategiaa voidaan jakaa yrityksessä useaan eri tasoon tai osaan, joissa on vastuussa eri organisaation päätöksentekijöitä. Tutkimuksessa myös löydettiin, että tietoturvalla ja tietoturvapolitiikalla on selkeä osa yrityksen strategiassa, ja niiden suunnittelusta ja toteuttamisesta vastaavat yrityksessä korkean tason johtajat.

7.1 Jatkotutkimusmahdollisuudet

Tietoturva, tietoturvapolitiikka ja yrityksen strategia ovat kaikki laajoja käsitteitä, jotka mahdollistavat paljon erilaisia mahdollisuuksia tutkimuksille. Mielenkiintoisia jatkotutkimuskohteita ovat esimerkiksi, miten yrityksen toimiala vaikuttaa tietoturvapolitiikkaan tai mitä vaikutusta yrityksen koolla on tietoturvapolitiikkaan. Hyvä jatkotutkimuskohde on myös, miten esimerkiksi Suomessa käytännössä yrityksissä tietoturvapolitiikka sitoutuu yrityksien strategiaan.

7.2 Työn arviointi

Tutkimuksessa löydettiin esitettyihin pää- ja alatutkimuskysymyksiin vastaukset ja vastattiin samalla tutkimusongelmaan. Tutkimuksessa onnistuttiin esittämään teoriaa tietoturvasta ja tietoturvapolitiikasta sekä yrityksen strategiasta. Tutkimuksessa onnistuttiin myös löytämään, miten tietoturva, tietoturvapolitiikka ja yrityksen strategia liittyvät yhteen.

Tutkimuksessa oli myös haasteita, kuten esimerkiksi käsitteiden kanssa. Esimerkiksi eri aineistoissa saatettiin puhua samasta asiasta eri käsitteillä. Lisäksi joissain aineistoissa käsiteltiin vain hyvin vähän tämän tutkimuksen kannalta oleellisia asioita. Ongelmaa tuotti myös aineiston etsiminen, sillä tarkatkin hakusanat tuottivat välillä suuria määriä tuloksia. Haasteena tutkimuksessa oli myös työn suoritukseen annettu aika, joka oli suhteellisen lyhyt (noin 3 kuukautta). Pidemmällä aikavälillä tutkimuksesta olisi mahdollisesti saanut laadukkaamman. Tutkimuksessa käytetty aineisto oli tieteellistä kirjallisuutta, joten aineiston pitäisi olla luotettavaa. Riskeinä aineiston suhteen on voinut olla esimerkiksi vanhentunut tieto, ja riski vanhentuneeseen tietoon saattaa realisoitua esimerkiksi vanhemmissa lähteissä. Sen vuoksi tutkimuksessa on pyritty käyttämään suhteellisen uutta tietoa. Toinen riski on, ettei lähdettä ole tieteellisesti arvioitu hyväksi.

Tutkimuksen merkitys koostuu suurelta osalta henkilökohtaisesta merkityksestä, joka muodostui esimerkiksi uuden tiedon löytämisestä. Lisäksi tutkimuksessa selvinneitä asioita voitaisiin mahdollisesti hyödyntää esimerkiksi yrityksissä tai jatkotutkimuksissa.

LÄHTEET

Adéle, D. V. 2016. Comparing the information security culture of employees who had read the information security policy and those who had not. Information and Computer Security. Vol. 24(2). Pp. 139-151.

Alam, M. ja Bokhari, M.U. 2007. Information Security Policy Architecture. IEEE. Pp. 120.

Alberts, C. ja Dorofee, A. 2002. Managing Information Security Risks: The Octave Approach. Addison-Wesley Longman Publishing Co. Inc. Boston, MA, USA. Pp. 25.

Alqahtani, F. M. 2017. Developing an Information Security Policy: A Case Study Approach. Procedia Computer Science. Vol. 124. Pp. 691-697.

Andress, J. 2011. The Basics of Information Security. 1st edn. Syngress. Pp. 1-16

Baskerville, R. Straub ja D. W. Goodman, S. E. 2008. Information Security : Policy, Processes, and Practices. Armonk, NY: Routledge (Advances in Management Information Systems).

Cheng, L., Liu, F., ja Yao, D. 2017. Enterprise data breach: causes, challenges, prevention, and future directions. WIREs Data Mining Knowl Discov, 7: e1211.

Croteau, A. M. ja Bergeron, F. 2001. An information technology trilogy: business strategy, technological deployment and organizational performance. The journal of strategic information systems. Vol. 10(2). Pp. 77-99.

Da Veiga, A. ja Eloff, J.H.P. 2010. A framework and assessment instrument for information security culture. Computers & Security. Vol. 29. No. 2. Pp. 196-207.

Desouza, K. ja Vanapalli, G. 2005. Securing knowledge in organizations: lessons from the defence and intelligence sectors. International Journal of Information Management. Vol 25. Pp. 85-98.

Eloff, M.M. ja Eloff, J.H.P. 2005. Information security architecture. Computer Fraud & Security, vol. 2005. No. 11. Pp. 10-16.

Euroopan komissio. 2019. Mitä tietoja voidaan käsitellä ja millä ehdoilla? Saatavilla: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/what-data-can-we-process-and-under-which-conditions_fi (Viitattu 12.2.2019) (a.)

Euroopan komissio. 2019. Mitä jos yritykseni/organisaationi ei onnistu noudattamaan tietosuojasääntöjä? Saatavilla: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/sanctions/what-if-my-company-organisation-fails-comply-data-protection-rules_fi (Viitattu 12.2.2019) (b.)

Euroopan komissio. 2019. Pitääkö yrityksellläni/organisaatiollani olla tietosuojavastaava? Saatavilla: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/data-protection-officers/does-my-company-organisation-need-have-data-protection-officer-dpo_fi (Viitattu 22.3.2019) (c.)

Euroopan komissio. 2019. Mikä on tietoturvaloukkaus ja miten sellaisen sattuessa pitää toimia? Saatavilla: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_fi (Viitattu 22.3.2019) (d.)

Euroopan komissio. 2019. Tietosuoja EU:ssa. Saatavilla: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_fi (Viitattu 26.3.2019) (e.)

Fink, A. 2019. Conducting research literature reviews: from the Internet to paper. Sage Publications.

Flowerday, S.V. ja Tuyikeze, T. 2016. Information security policy development and implementation: The what, how and who. Computers & Security. Vol. 61. Pp. 169-183.

Goodman, S. Straub, D. W. Baskerville, R. ja Baskerville, R. 2008. Information security: policy, processes, and practices.

Höne, K. ja Eloff, J.H.P. 2002. Information security policy — what do international information security standards say? Computers & Security. Vol. 21. No. 5. Pp. 402-409. (a.)

Höne, K., ja Eloff, J. H. P. 2002. What makes an effective information security policy?. Network Security. Vol. 2002(6). Pp. 14-16. (b.)

Ilvonen, I., Jussila, J., Kärkkäinen, H., ja Päivärinta, T. 2015. Knowledge Security Risk Management in Contemporary Companies--Toward a Proactive Approach. 2015 48th Hawaii International Conference on System Sciences. Pp. 3941-3950. IEEE.

Johnson, G., Whittington, R., ja Scholes, K. 2015. Fundamentals of strategy. Pearson Education Limited. Harlow. U.K. Pp. 6-7.

Karlsson, F., Hedström, K., ja Goldkuhl, G. 2017. Practice-based discourse analysis of information security policies. Computers & Security. Vol. 67. Pp. 267-279.

Knapp, K. J., Marshall, T. E., Rainer Jr, R. K., ja Morrow, D. W. 2006. The top information security issues facing organizations: What can government do to help. Network security. 1. Pp. 51–58

Knapp, K. J., Morris Jr, R. F., Marshall, T. E., ja Byrd, T. A. 2009. Information security policy: An organizational-level process model. computers & security. Vol. 28(7). Pp. 493-508.

Lai, X. ja Zhou, J. Li, H. 2011. Information Security: 14th International Conference, ISC 2011, Xi'an, China, October 26-29, 2011. Proceedings. Berlin, Heidelberg: Springer Berlin Heidelberg.

Laihonen, H., Hannula, M., Helander, N., Ilvonen, I., Jussila, J., Kukko, M., Kärkkäinen, H., Lönnqvist, A., Myllärniemi, J., Pekkola, S., Virtanen, P., Vuori, V. ja Yliniemi, T. 2013, Tietojohtaminen, Tampereen teknillinen yliopisto, Tietojohtamisen tutkimuskeskus Novi. Pp. 17

Lopes, I.M., Pereira, J.P., ja Oliveira, P. 2017. Definition of Information Systems Security Policies. In: Rocha Á., Correia A., Adeli H., Reis L., Costanzo S. (eds) Recent Advances in Information Systems and Technologies. WorldCIST 2017. Advances in Intelligent Systems and Computing. Vol 571. Springer, Cham

Low, C. 2017. Information security policies every business must implement. Cio.

Martinsuo, M., Mäkinen, S., Suomala, P., ja Lyly-Yrjänäinen, J. 2016. Teollisuustalous kehittyvässä liiketoiminnassa. Edita. Pp. 178.

Mintzberg, H. 1987. The Strategy Concept I: Five Ps For Strategy. California Management Review. Vol. 30. No. 1. Pp. 11-24.

Mohurle, S. ja Patil, M. 2017. A brief study of wannacry threat: Ransomware attack 2017. International Journal of Advanced Research in Computer Science.

Nosworthy, J. D. 2000. Implementing information security in the 21st century—do you have the balancing factors? Computers & security. Vol. 19(4). Pp. 337-347.

Pelkonen, A. 2003. Tieto-ja viestintäteknologia teknologiavetoisen yhteiskunnan rakentajana ja yhteiskuntapolitiikan välineenä. Politiikka. Vol. 45(1). Pp. 50-61.

Peltier, T. R. 2014. Information security fundamentals. Second edition. Boca Raton [Florida]: CRC Press. Pp. xii, 7-12

Rathnam, R. G., Johnsen, J., ja Wen, H. J. 2005. Alignment of business strategy and IT strategy: a case study of a fortune 50 financial services company. Journal of Computer Information Systems. Vol. 45(2). Pp. 1-8.

Sabherwal, R. ja Chan, Y. E. 2001. Alignment between business and IS strategies: A study of prospectors, analyzers, and defenders. Information systems research, Vol. 12(1). Pp. 11-33.

Schein, E. H. 2010 Organizational Culture and Leadership. San Francisco: Jossey-Bass (The Jossey-Bass Business & Management Series). Pp. 22

Scholes, K., Johnson, G., ja Whittington, R. 2002. Exploring corporate strategy. Financial Times Prentice Hall. Pp. 9

Slater, S.F., Olson, E.M. ja Finnegan, C. 2011. Business strategy, marketing organization culture, and performance. Marketing Letters. Vol. 22. No. 3. Pp. 227-242.

von Solms, R. van Niekerk, J. 2013. From information security to cyber security. Computers & Security. Vol. 38. Pp. 97-102.

von Solms, R. ja von Solms, S. H. 2009. Information Security Governance. illustrat edn, Springer Verlag. DE. Pp. 63 (a.)

von Solms R. ja von Solms S. 2009. The Direct Part of the Model – An Information Security Policy Architecture. In: Information Security Governance. Springer, Boston, MA. Pp. 17-19. (b.)

Sveen, F.O., Torres, J.M., ja Sarriegi, J.M. 2009. Blind information security strategy. International Journal of Critical Infrastructure Protection.Vol. 2. No. 3. Pp. 95-109.

Tietosuojalaki 5.12.2018/1050. Finlex. Saatavilla: https://www.finlex.fi/fi/laki/ajantasa/2018/20181050 (Viitattu 12.2.2019)

Vacca, J. R. 2013. Computer and Information Security Handbook. Amsterdam: Morgan Kaufmann. Pp. 6, 410

Whitman, M. E. ja Mattord, H. J. 2011. Principles of information security. Cengage Learning. Pp. 8

Whitman, M. ja Mattord, H. 2013. Management of information security. Nelson Education. Pp. 6-7, 14, 44