Samu Turunen

TIETOTURVAPOLITIIKAN LUOMISEN TAKSONOMIA

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2019

TIIVISTELMÄ

Turunen, Samu
Tietoturvapolitiikan luomisen taksonomia
Jyväskylä: Jyväskylän yliopisto, 2019, 33 s.
Tietojärjestelmätiede, pro gradu
Ohjaaja: Siponen, Mikko

Tämä pro gradu -tutkimus käsittelee tietoturvapolitiikan luomista ja tarkastelee sitä systemaattisen kirjallisuuskatsauksen keinoin. Tutkimusaineisto on kasattu keväällä 2016 ja se käsittää vuosien 1999 – 2016 välillä julkaistut tieteelliset artikkelit. Tutkimuksessa kuvataan niitä metodeja, joilla tietoturvapolitiikka voidaan luoda organisaatioon joko tyhjästä tai vanhan tietoturvapolitiikan päälle. Tietoturvapolitiikan katsotaan tässä tutkimuksessa olevan ylätason dokumentti, joka ohjaa organisaation toimintaa tietoturvallisuuteen liittyvissä kysymyksissä ja askareissa. Tietoturvapolitiikan luomisen keinoja havaittiin teemoitetusti olevan kolme: Riskien tunnistaminen ja hallinta, yleiset analyysityökalut ja organisaation tehtävät ja arvot. Aineiston perusteella yleisin tapa tietoturvapolitiikan luomiseen tieteellisessä kirjallisuudessa on organisaation keskeisten tehtävien ja tapojen havainnoinnin ja kartoituksen pohjalta tehtävä selvitys.

Asiasanat: tietoturvapolitiikka, tietoturvallisuus, kyberturvallisuus, systemaattinen kirjallisuuskatsaus

ABSTRACT

Turunen, Samu
Taxonomy of creating information security policies
Jyväskylä: University of Jyväskylä, 2019, 33 p.
Information Systems, Master's Thesis
Supervisor: Siponen, Mikko

This master's thesis describes the creation of information security policies by using methodology of systematic literature review. The data is gathered during Spring 2016 and it includes scientific articles from 1999 to year 2016. This research describes methods of creating an information security policy from start or after old information security policy is at end of life. In this research information security policy is described as high-level policy, which steers organisation's security and normal activity. Three methods to create an information security policy were found: Risk observation and management, general analysis tools, and organisation's key processes and core values. According to the analyzed data the most common methodology to create an information security policy is to base the creation on observation and analyzation of organisation's key processes and core values.

Keywords: information security policy, information security, cyber security, systematic literature review

Kuviot

TAULUKOT

SISÄLLYS

1 JOHDANTO

Tutkimuksen tavoitteena on luoda systemaattisen kirjallisuuskatsauksen keinoin taksonomia tietoturvapolitiikan luomisessa käytetyille tavoille.
Yritysten suurimmat tietoturvahaavoittuvuudet ovat Ernst & Youngin (Ernst & Young Global Limited, 2015) mukaan huolimattomat työntekijät ja vanhentuneet eli päivittämättömät turvallisuusmekanismit tai -arkkitehtuuri. Vaikka työntekijöiden muodostama tietoturvauhka organisaatioille on laskenut vuonna 2014 57 %:sta 44 %:iin, voidaan työntekijöiden aiheuttamia ongelmia pitää suurina ja organisaatioiden toimintaa vaarantavina. Siponen, Mahmood ja Pahnila (2014) esittävät yrityksen työntekijöiden olevan suurin uhka yrityksen tietoturvallisuudelle. Työntekijöiden virheistä tai piittaamattomuudesta johtuviin haittoihin ja ongelmiin organisaatiot vastaavat yleensä tietoturvapolitiikalla.

EY:n (2015) kyselyssä 27 % yrityksistä myönsi tietoturvapolitiikkansa olevan epämuodollisia, tai politiikat luodaan ad hoc. Ad hoc -tietoturvallisuuspolitiikka ei välttämättä ole riittävä ja ajan mittaan ongelmaksi voi muodostua lennosta tehtyjen säädöksien ristiriitaisuus ja riittämättömyys. Tämän perusteella voidaan sanoa, että tietoturvapolitiikan luomiselle ja olemassaololle on suuri tarve. Hyökkäysten onnistuessa organisaatio voi kärsien informaation menetyksen lisäksi myös taloudellista tappiota menettämällä asemiaan markkinoilla. (Ernst & Young Global Limited, 2015; Calder ja Watkins, 2010)
Tutkimusongelmana tässä tutkimuksessa on, miten tietoturvapolitiikan luomista on käsitelty tieteellisessä kirjoittamisessa.

Tietoturvapolitiikkojen luomista ei ole laajasti käsitelty tieteellisessä kirjallisuudessa, joten tutkimukselle on tarve. Tietoturvallisuutta on käsitelty lähinnä tietoturvapolitiikkojen ja -ohjeistusten noudattamisen näkökulmasta. Tämä tutkimus on merkityksellinen erityisesti yritysmaailmalle, sillä tietoturvaloukkauksen tai -rikoksen kohteeksi joutunut yritys voi joutua kärsimään välittömien taloudellisten tappioiden lisäksi myös oman julkisuuskuvansa tahriintumisesta. Yritysten tavoitteena on tuottaa voittoa osakkeenomistajilleen, ja yrityksen arvo riippuu osakekurssista. Yrityksen imagon tahriintuminen voi aiheuttaa negatiivista

kehitystä yrityksen arvolle. Onnistuneen hyökkäyksen kohteeksi joutunut yritys ei välttämättä ole ainut taho, joka voi kärsiä haittaa: jos yritys toimii esimerkiksi terveydenhuollon alalla, tai muulla asiakkaiden arkaluonteisia tietoja käsittelevällä alalla, voivat asiakkaat saada osakseen mittavaa haittaa tietojen varastamisen takia. Tällaisessa tilanteessa yrityksen asiakkaiden turvallisuus ja tietosuoja voivat vaarantua, jolloin yksittäiset ihmiset menettävät yksityisyydensuojansa ja heille voi koitua jopa merkittävää haittaa.
Motivaatio tämän pro gradu -tutkimuksen tekemiseen on kirjoittajan omien mieltymysten mukaista ja sisäsyntyistä. Lisäksi tämä opinnäytetyö tehdään Tietojenkäsittelytieteen laitokselle tilaustyönä. Tämä opinnäytetyö etenee seuraavalla tavalla: aluksi esitellään tutkimuksen aihepiiri, toisessa luvussa esitellään tietoturvapolitiikan kannalta keskeiset käsitteet ja ympäristö, minkä jälkeen seuraavassa luvussa esitellään systemaattisen kirjallisuuskatsaus tutkimusmetodina. Tämän jälkeen esitellään tutkimuksen toteutus, jonka jälkeen esitellään tutkimusaineiston kuvaus, analyysi tulokset ja viimeisenä johtopäätökset.

1.1 Tietoturvapolitiikka

Organisaatiot ovat nykypäivänä yhä riippuvaisempia tietotekniikasta, tietojärjestelmistä ja internetistä. Ne mahdollistavat työnteon tehostamisen, mutta saattavat organisaatiot myös alttiiksi uusille uhille. Tämän tähden tietoturva on tärkeä ja ajankohtainen aihe. Tietoturvan perusteisiin kuuluva tietoturvapolitiikka – tai vähintään tietoturvaohjeistus – tulisi olla jokaisella organisaatiolla. Yritysten suurimmat tietoturvahaavoittuvuudet ovat huolimattomat työntekijät ja vanhentuneet eli päivittämättömät turvallisuusmekanismit tai arkkitehtuuri (Ernst & Young Global Limited, 2015). Vuoteen 2014 verrattuna työntekijöiden muodostama uhka on laskenut 57 %:sta 44 %:iin, voidaan ongelmaa pitää suurena ja organisaatioiden toimintaa vaarantavana. Työntekijöiden virheistä tai piittaamattomuudesta johtuviin haittoihin ja ongelmiin organisaatiot vastaavat yleensä tietoturvapolitiikalla. Vaikka tietoturvapolitiikka olisi laadittu asianmukaisesti ja hyvällä tavalla, se ei välttämättä ole onnistunut: jos politiikan alaiset henkilöt eivät käyttäydy ja toimi politiikan ohjeistamalla tavalla, on politiikka hyödytön ja samalla muut järjestelmään sisällytetyt tietoturvaratkaisut menettävät tehonsa. (Dhillon ja Backhouse, 2001; Straub ja Welke, 1998).

2 TIETOTURVAPOLITIIKAN OLEMUS

Tässä luvussa esitellään tietoturvapolitiikan pääperiaatteet ja tietoturvapolitiikan olemassaolon tarkoitus. Luvussa käydään läpi, mitä osa-alueita tietoturvapolitiikka pitää sisällään, ja miksi ja mihin tietoturvapolitiikkaa tarvitaan.

2.1 Politiikan käsite

Tietoturvapolitiikka-termi voidaan jakaa kahteen osaan: tekniseen tietoturvaan ja tietoturvan johtamiseen. (Baskerville ja Siponen, 2002). Tietoturvapolitiikka teknisestä näkökulmasta sisältää lähinnä järjestelmien teknilliseen turvallisuuteen liittyviä toimintoja, kuten pääsyn- ja käytönhallintaa. Tietoturvan johtamisella (jatkossa tietoturvapolitiikka) tarkoitetaan niitä hallinnollisia toimia, jotka luovat organisaatiolle toiminnan lait ja raamit tietoturvan näkökulmasta. Toisin sanoen ne luovat mahdollisuuden tietoturvan johtamiseen.

Tietoturvallisuuden tarkoituksena on suojella tiedon luotettavuutta, eheyttä ja tiedon saatavuutta varastoinnin, prosessoinnin tai siirron aikana. Tätä kolminaisuutta on kutsuttu englanniksi lyhenteellä "CIA": luotettavuus (confidentiality), eheys (integrity) ja saavutettavuus (availability) (Whitman ja Mattord, 2011.)

Työkaluna tietoturvapolitiikkaan käytetään dokumenttia, joka ohjaa ja määrittelee tietoturvalliset työskentelytavat ja säännöt – toisin sanoen lait – koko yrityksen toiminnalle. Dokumentti yleensä kattaa edellä mainitut kuusi osa-aluetta, muodostaen näin pelisäännöt yrityksen kaikille toiminnoille. Dokumentin tarkoituksena on suojella ja varmistaa tiedon eheyttä, luotettavuutta ja saatavuutta. (Straub, Goodman ja Baskerville, 2008). Tietoturvapolitiikkaan liitetään usein myös tulevaisuuden kannalta tärkeät prioriteetit ja aikomukset, joiden katsotaan liittyvän organisaation tietojärjestelmien ja tietojen suojaamiseen. (Karyda, Kiountouzis ja Kokolakis, 2005). Tietoturvapolitiikan luo yleensä erikseen valtuutettu ryhmä, minkä jälkeen dokumentti ratifioidaan täysivaltaiseksi osaksi organisaation sääntökokoelmaa. Tämän jälkeen politiikka julkaistaan henkilöstölle, ja samalla tuodaan julki rangaistukset sääntöjen rikkomisesta (Straub ym., 2008; Von Solms ja Von Solms, 2004 a).
Yrityksen politiikan tulee osoittaa johdon sitoumus ja tuki tietoturvan noudattamiselle, ja tietoturvapolitiikan on oltava keskeisessä asemassa tukemassa organisaation tavoitteita (Joint Information Systems Committee, 2001). Koska yrityksen johto on vastuussa organisaation tilasta, he myös osoittavat yrityksen kehityssuunnan kohti menestystä. Apuvälineenä suunnan määrittämiselle he voivat käyttää erilaisia politiikoita, kuten esimerkiksi tietoturvapolitiikkaa. Tällöin yrityksen johto epäsuoralla tavalla ohjaa työntekijöiden toimintaa vastaamaan

organisaation tavoitteita. (Von Solms ja Von Solms, 2004 a.) Höne ja Eloff (2002) esittävät, että vaikka tietoturvapolitiikka on tärkeä ja keskeinen yrityksen toimintaa ohjaava ja yrityksen turvallisuudesta vastaava dokumentti, on sen luominen vaikeaa. He myöntävät, että tietoturvapolitiikan sisällöstä ei ole konsensusta, vaan jokainen tietoturvapolitiikka on kirjoitettu tietylle yksittäiselle yritykselle. Tällöin samaa sisältöä ei voida välttämättä käyttää toisessa organisaatiossa.

2.2 Tietoturvapolitiikan rooli

Tietoturvapolitiikan rooli organisaatiossa on suojella tietoturvan periaatteiden mukaisesti tiedon luottamuksellisuutta, eheyttä ja saatavuutta. Luottamuksellista tieto on silloin, kun sitä voivat käyttää vain valtuutetut tahot, kuten järjestelmät ja henkilöt. Vain auktorisoidut toimijat pääsevät käsittelemään luottamuksellista tietoa. Tietoturvapolitiikan mukaisesti tieto on eheää vain silloin, kun tieto on täydellistä ja kokonaista. Tieto ei ole eheää, jos se altistuu korruptoitumiselle, tuhoutumiselle tai muulle vahingolle. Saatavaa tieto on silloin, kun tiedon käsittelyyn valtuutetut henkilöt ja järjestelmät kykenevät pääsemään siihen käsiksi ilman esteitä tai häiriötekijöitä. (Straub ym., 2008).
Tietoturvapolitiikka ei voi olla pelkästään teknisiä ratkaisuja, vaan käyttäjät on otettava huomioon (Furnell ja Clarke, 2012; Von Solms ja Von Solms, 2004a). Raggadin (2010) luoman taksonomian mukaisesti organisaation kohdistuva uhkat voivat olla myös yrityksen työntekijöistä lähtöisiä, olivatpa uhkaavat tilanteet tahallisia tai tahattomia. Tietoturvapolitiikan riittävällä ohjeistuksella voidaan ohjeistaa ihmisiä käyttäytymään tietoturvaa edistävästi, jolloin riski virheiden tapahtumiseen vähenee (Raggad, 2010).
Piittaamattomuus tietoturvapolitiikan suhteen voi esimerkiksi johtua vaikeasti löydettävästä tietoturvapolitiikasta tai ymmärryksen puutteesta. (Herath ja Rao, 2009; Von Solms ja Von Solms, 2004b). On tärkeää, että tietoturvapolitiikka on koulutettu jokaiselle organisaation jäsenelle ja se helposti saavutettavissa, esimerkiksi organisaation sisäisillä verkkosivuilla. Tällöin organisaation jäsenet todennäköisemmin toimivat tietoturvapolitiikan säädösten mukaisesti. (Puhakainen ja Siponen, 2010.) Tietoturvapolitiikkaa voidaan pitää yhtenä tärkeimmistä tekijöistä organisaation tietoturvan kannalta, sillä se luo ne pelisäännöt, joiden mukaan organisaation tietoturva järjestetään ja toteutetaan. Tietoturvapolitiikka voi olla myös itsessään niskoittelua aiheuttava tekijä: ohjeistus ei välttämättä sovi kaikkiin tilanteisiin, sillä se voi hankaloittaa suuresti tai jopa estää yksittäisissä tapauksissa työntekoa (Puhakainen ja Siponen, 2010.)
Von Solms ja Von Solms (2004a) esittävät tietoturvapolitiikan olevan viestinnän väline eri osapuolten välillä. Politiikan avulla yrityksen johto pyrkii välittämään halutun viestin eri osapuolille, tässä tapauksessa organisaation eri jäsenille. Tässä kontekstissa viestillä pyritään muuttamaan organisaation jäsenten käyttäytymismalleja tietoturvalliseen käyttäytymiseen.

2.1.1 Työntekijöiden rooli

Tietoturvapolitiikan noudattaminen on työntekijöiden velvollisuus ja tehtävä. Tietoturvapolitiikka ja -käytännöt voivat aiheuttaa ongelmia työntekijöille tai jopa estää työn tekemisen. Baskerville ja Siponen (2002) ovat teoretisoineet tilanteen, jossa tietoturvapolitiikkaa on rikottava, jotta työnteko onnistuisi. Heidän esimerkissään projektin onnistumisen kannalta tärkeitä tietoja on siiloutunut yhden työntekijän tilille niin, että muut eivät pääse käsiksi niihin. Tämä voi aiheuttaa muille organisaation tekijöille tarpeen sääntöjen vastaisesti käyttää luvattomasti toisen työntekijän tunnuksia saadakseen projektin onnistumaan.

2.1.2 Kulttuurin rooli

Yrityksen organisaatiokulttuurilla on myös oma roolinsa, sillä se voi joko sallia tai estää uusien toimintatapojen omaksumisen organisaatiossa (Thomson ja von Solms, 2005: Atkinson, 1997). Kotimaisten kielten keskus määrittelee kulttuurin yksilön tai yhteisön ajattelu- tai toimintatapojen kehittyneisyydeksi tai vakiintuneiksi toimintatavoiksi (Kotimaisten kielten keskus, 2016). Kulttuuria voidaan pitää vaikuttavana tekijä organisaation jäsenten jokapäiväisissä työtehtävissä. Siksi tietoturvapolitiikan on tultava osaksi organisaation kulttuuria tai muutettava sitä pysyvästi, jotta tietoturvalliset toimintatavat saisivat organisaatiossa jalansijaa.

3 SYSTEMAATTINEN KIRJALLISUUSKATSAUS

Tässä luvussa esitellään tutkimusmetodi ja perustelut sen valintaan. Tämän jälkeen luvussa esitellään tutkimusprosessin kulku. Jotta tutkimuksessa voidaan tarkastella, miten aiemmat tutkimukset ovat kartoittaneet tietoturvapolitiikan luomista, käytetään tutkimusmetodina systemaattista kirjallisuuskatsausta.

3.1 Systemaattinen kirjallisuuskatsaus metodina

Tutkimusmetodina systemaattinen kirjallisuuskatsaus on järjestelmällinen, tarkka ja toistettava tutkimusmetodi. Se arvioi, tarkastelee ja yhdistelee aiempia tutkimuksia. (Fink, 2013.) Jotta tutkimus olisi toistettavissa, kirjallisuuskatsauksen tulee olla täsmällisesti suunniteltu prosesseiltaan ja toteutukseltaan. Toistettavuuteen systemaattisessa kirjallisuuskatsauksessa pyritään seuraamalla kolmea tavoitetta: ensimmäiseksi on tärkeää kerätä kattavasti alkuperäiskirjallisuutta, jotta tietoa ei valikoituisi satunnaisesti valituista yksittäisistä lähteistä. Toiseksi aineistoksi valikoituvista tutkimuksista selvitetään menetelmällinen laatu. Kolmanneksi olemassa olevia tutkimustuloksia yhdistetään, jotta tutkimuksia voidaan hyödyntää mahdollisimman tehokkaasti. (Fink, 2013.) Okoli ja Schabram (2010) määrittelevät artikkelissaan kuusi erilaista ja yleistä syytä, miksi kirjallisuuskatsaus tehdään:

- Analyysi tietyn tutkimusalan edistymisestä
- Uusien tutkimuskysymysten synnyttäminen tutkitusta aiheesta
- Arvioidakseen teoreettisen mallin soveltamista alan kirjallisuudessa
- Arvioidakseen metodologian käyttöä alan kirjallisuudessa
- Uuden mallin tai viitekehyksen luominen
- Tiettyyn tutkimuskysymykseen vastaaminen

Tämän tutkimuksen tarkoituksena on pyrkiä viidennen kohdan mukaiseen lopputulokseen, eli uuden mallin luomiseen edeltävien tieteentekijöiden työn pohjalta. Aineistona systemaattiseen kirjallisuuskatsaukseen tulee käyttää kaikkia aiheeseen ja tutkimuskysymykseen liittyviä tutkimuksia, jotka mahdollisesti tuovat lisäarvoa tutkimukseen (Aveyard, 2014).

Systemaattisen kirjallisuuskatsauksen luonteeseen ei kuulu vain toistaa alkuperäisen tutkimuksen löydöksiä, vaan luoda ja edistää aiheen tutkimista yhdistelemällä edeltävän tutkimuksen materiaalia ja tarkastelemalla sitä kriittisesti (Kekäle, Weerd-Nederhof, Cervai ja Borelli, 2009; Hart, 1998). Tämän tutkimuksen aineistona on käytetty sekä laadullista että määrällistä tutkimusta. Järjestelmällisen kirjallisuuskatsauksen käyttöä tutkimusmetodina voidaan tässä tapauksessa perustella tutkimuksen päämäärällä: tavoitteena on kartoittaa, miten edeltävät

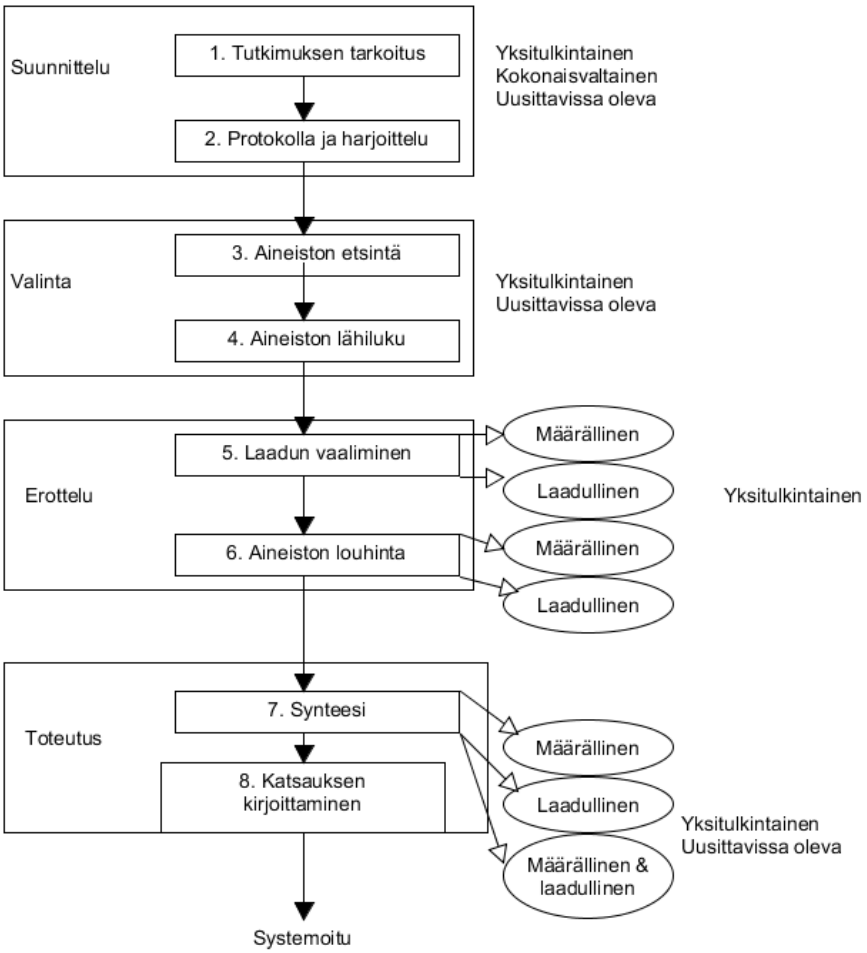
tutkimukset ovat käsitelleet tietoturvapolitiikan luomista. Lisäksi systemaattisen kirjallisuuskatsauksen käyttöä tässä tutkimuksessa puolustaa kolme keskeistä seikkaa:

1. Järjestelmällinen kirjallisuuskatsaus mahdollistaa selkeän kuvan luomisen siitä, miten tietoturvapolitiikkaa on aikaisemmin tutkittu, ja millä tavoin sitä on tutkittu.
2. Järjestelmällisen kirjallisuuskatsauksen tuloksia voidaan todennäköisesti hyödyntää jatkotutkimuksessa.
3. Kirjoittajan henkilökohtaiset mieltymykset ja taidot puoltavat systemaattisen kirjallisuuskatsauksen käyttöä. Myös ohjeistus systemaattisen kirjallisuuskatsauksen tekemiseen on kirjoittajan kannalta suotuisa.

Systemaattinen kirjallisuuskatsaus ei kuitenkaan ole täysin ongelmaton tutkimusmenetelmä. Petticrewin ja Robertin (2006) mukaan menetelmän käyttö ei ole suotuisaa tutkimusaiheen ollessa uusi ja vielä nuori tai aihetta ei käsitelty laajasti tieteellisessä kirjallisuudessa. Kirjallisuudesta ei voida tällöin muodostaa selkeää kokonaiskuvaa, jonka seurauksena tutkimuksen tuloksena on todennäköisesti suppea näkemys. Jatkotutkimuksen kannalta hedelmällinen tilanne tällöin ei ole hedelmällinen (Petticrew ja Robert, 2006.)

3.2 Tutkimusprosessi ja protokolla

Protokollalla tarkoittaa tutkimussuunnitelmaa, jossa määritellään kriteerit, joiden perusteella aineistoon otetaan mukaan tutkimuksia. Tässä tutkimuksessa systemaattinen kirjallisuuskatsaus noudattaa Okolin ja Schabramin (2010) luomaa mallia, joka on esitetty kuviossa 1. Heidän mallinsa on valittu selkeyden ja sovellettavuuden takia.



KUVIO 1 Systemaattisen kirjallisuuskatsauksen prosessi (Okoli ja Schabram, 2010, 9)

Tutkimusprosessin eri vaiheet ovat seuraavat:

1. Tutkimuksen tarkoitus
    a. Tutkimuksen tarkoitus sekä tavoite ovat selkeästi määriteltyinä. Tällöin lukijalle tutkimuksen tarkoitus on selvä alusta alkaen.
2. Protokolla ja harjoittelu
    a. Yksityiskohtainen kirjallinen selostus toimintatavasta, jotta kirjallisuuskatsaus toteutuu oikeaoppisesti.
3. Aineiston etsintä
    a. Tarkka kuvaus aineiston valinnasta, sisäänottokriteereistä, hakusanoista sekä perustelut hakusanojen valinnoista. Tämä on ensimmäinen ns. karsintakierros.
4. Aineiston lähiluku
    a. Aineiston karsinta, jossa valitaan kirjallisuus jatkoon tutkimusta varten, tehdään tässä vaiheessa. Artikkelien valinta

tapahtuu artikkelien syvällisemmän tarkastelun perusteella. Karsinnan jälkeen jäljelle tulee jäädä tutkimuksen kannalta olennainen aineisto.

5. Laadun vaaliminen
    a. Aineiston kolmas karsintakierros, jossa jäljelle jääneestä kirjallisuudesta seulotaan järjestelmällisesti tutkimuksen laadun perusteella riittävä aineisto johtopäätösten tekemistä varten.
6. Aineiston louhinta
    a. Tutkimuksen kannalta olennaisten sisältöjen kerääminen lomakkeella yksittäisistä artikkeleista järjestelmälliseen muotoon, jotta synteesin tekeminen mahdollistuu.
7. Synteesi
    a. Jäsennetyn aineiston analysointi ja yhdistely joko laadullisen, määrällisen tai molempien metodien tavoin.
8. Systemaattisen kirjallisuuskatsauksen kirjoittaminen
    a. Tutkimuksen tulosten kirjaaminen niin, että tuloksena on toistettavissa oleva, itsenäinen ja omilla jaloillaan seisova raportti.

4 TUTKIMUKSEN TOTEUTUS

Edellisessä luvussa esiteltiin systemaattisen kirjallisuuskatsauksen prosessi ja sen eteneminen teoriassa. Tässä luvussa esitellään, miten tämän tutkimuksen prosessi ja sen kahdeksan vaihetta etenevät. Aineisto on kerätty tietojärjestelmätieteen ja informaatioteknologian arvostetuista lehdistä. Seulonnassa on käytetty ennakkoon määrättyä kriteeristöä. Aineiston seulonta on ensimmäinen vaihe, jossa aineistoa on tulkittu kriittisesti tutkimuskysymyksen avulla.
Tässä luvussa esitellään aluksi, miten tutkimuksen suunnittelu, aineiston valinta, aineiston erottelu ja laadun vaalinta on toteutettu. Tämän jälkeen esitellään, miten tutkimuksen aineistosta on seulottu tutkimuksen kannalta olennainen data. Lisäksi luvussa esitellään myös, miten tutkimusaineisto on muodostunut, sekä miten aineisto on analysoitu.

4.1 Tutkimuksen suunnittelu

Tämän tutkimuksen suunnittelu aloitettiin helmikuussa 2016 opinnäytetyön ohjaajan kehotuksesta. Vuoden 2016 helmikuun tapaamisessa päätettiin tutkimuksen aihe, metodi ja laajuus. Itse käytännön tutkimus on suunniteltu käyttäen apuna Okolin ja Schabramin (2010) ohjeita.

4.1.1 Valittujen artikkeleiden kriteeristö

Aineiston seulontaan käytettävät kriteerit riippuvat tutkimuksen tutkimuskysymyksestä. Lähiluvussa artikkeleista luettiin tiivistelmät, joiden perusteella artikkelit valittiin tutkimukseen mukaan. Myös muut seikat, kuten käytännölliset rajoitteet, esimerkiksi tutkimuksen luonne, aika ja rahalliset vaikuttimet vaikuttavat aineiston seulontaan (Aveyard, 2014). Jotta tutkimusaineistoa voitaisiin rajata mielekkäästi, on käytettävä sisäänottokriteereitä, joilla käsiteltävä yksittäinen artikkeli otetaan mukaan aineistoon tai rajataan pois (Aveyard, 2014). Selkeä kriteeristö artikkelien valinnalle mahdollisti selkeän kuvan muodostamisen ja helpotti tutkimuskysymykseen vastaamista (Aveyard, 2014).

Informaatioteknologian alalta ei löydy vielä kattavaa listausta erilaisista tavoista luoda tietoturvapolitiikka. Järjestelmällisesti ja huolellisesti tehdyn systemaattisen kirjallisuuskatsauksen voidaan katsoa antavan uuden ja kattavahkon listauksen tavoista, joilla luoda tietoturvapolitiikka organisaatioon. Jotta työkuormitus ei kasvaisi liiallisen suureksi, tarkastellaan tässä tutkimuksessa aineistoa vasta vuoden 1999 jälkeen julkaistuista artikkeleista. Tämän lisäksi myös vertaisarvioimattomat artikkelit ja kirjat suljetaan otoksen ulkopuolelle, sillä niiden voidaan katsoa mahdollisesti vievän tutkimusta väärään suuntaan (Rousseau, Manning ja Denyer, 2008) Artikkelien valintakriteeristö on esitetty alla olevassa taulukossa (taulukko 1).

TAULUKKO 1 Kriteeristö artikkeleiden hyväksymiselle ja hylkäykselle

Hyväksytään	**Hylätään**
Akateeminen tutkimus, joka on julkaistu vertaisarvioidussa julkaisussa	Tutkimus ei ole vertaisarvioitu
Artikkeli julkaistu välillä 1999-2016	Tutkimus julkaistu ennen vuotta 1999
Tutkimus on julkaistu tieteellisessä julkaisussa	Blogikirjoitus, sanomalehtikirjoitus tai muu vastaava
Suomen- tai englanninkielinen julkaisu	Julkaisu muulla kuin suomen tai englanninkielellä
Aiheena tietoturvapolitiikan luominen ja vaikutukset	Tietoturvapolitiikka sivuosassa
Tutkimusten kontekstina yritykset tai julkinen sektori	Yhteisöjen, yhdistysten ja valtioiden tietoturvapolitiikka
Tutkimukset ovat maksuttomasti saavutettavissa	Tutkimukset eivät ole maksutta saavutettavissa
ICT- ja/tai tietojärjestelmätieteen alan tutkimuksia	Artikkelit muilta aloilta kuin ICT- ja tietojärjestelmätiede

4.1.2 Aineiston etsintä

Kirjallisuuskatsauksen aineiston keruuseen valittiin kymmenen eri lehteä ja tietokantaa. Tällä varmistettiin, että saatu aineisto on riittävän kattava. Katsaukseen hyväksyttiin vain kirjoittajalle ilmaiset suomen- ja englanninkieliset julkaisut. Hakusanoina aineiston hakemiseen käytettiin termejä “information security policy”, “cyber security policy”, “information security”, “security governance” ja “tietoturvapolitiikka”. Julkaisujen määrää rajattiin valitsemalla vain artikkeleita, jotka ovat julkaistu vuoden 1999 jälkeen. Tällöin hakulausekkeeksi muodostui “information security policy” AND "security governance" OR “Cyber security policy” AND "security governance". Aineiston keräämiseen käytettiin seuraavia tietokantoja: Google Scholar, SCOPUS ja ACM. Löydettyjen artikkeleiden määrät ja hakupäivämäärät on esitelty alla olevassa taulukossa (taulukko 2).

TAULUKKO 2 Tutkimuksen aineiston keräämiseen käytetyt tietokannat

Tietokanta	Hakupäivämäärä	Kappalemäärä
Google Scholar	28.7.2016	49
SCOPUS	28.7.2016	69
ACM	27.7.2016	6

27.6.2016 etsittiin valitulla hakulausekkeella artikkeleita ACM-tietokannasta ja kuusi löydettyä artikkelia otettiin mukaan tutkimukseen. Lisäksi haku samoilla hakusanoilla osoitettiin SCOPUS-tietokantaan, josta artikkeleita tuli tuloksena 69 kappaletta. Tämän lisäksi artikkeleita etsittiin Google Scholar -hakukoneella, joka hakee useasta tietokannasta yhtäaikaisesti. Lopputuloksena hakulausekkeella saatiin 124 artikkelin aineisto.

4.1.3 Aineiston lähiluku

Aineiston lähilukuun saatiin 124 artikkelin aineisto. Kaikki artikkelit luettiin kertaalleen, jonka pohjalta tehtyjen arviointien perusteella aineiston ulkopuolelle rajattiin artikkelit, jotka eivät käsitelleet tietoturvapolitiikan luomista. Ulkopuolelle jääneitä artikkeleita oli 112 kappaletta. Tämän jälkeen siirryttiin aineiston erotteluun, joissa jäljelle jääneet 12 artikkelia luettiin uudestaan ja niiden laatu arvioitiin sekä niiden keskeisimmät löydökset kirjattiin ylös.

4.2 Aineiston erottelu

Aineiston erottelu sisälsi laadun vaalimisen ja aineiston erottelun vaiheet. Tässä kappaleessa esiteltiin aineiston erottelun sekä laadun vaalimisen kannalta olennaiset yksityiskohdat.

4.2.1 Artikkelien laadun vaalinta

Laadun vaalimisen tarkoituksena on seuloa tutkimukseen artikkelit, jotka vastaavat tutkimuskysymykseen sisällöltään. Edellisessä vaiheessa aineistoon seulottiin artikkeleita, jotka nopealla tarkastelulla ja johdannon perusteella sopivat tutkimukseen. Artikkelien laadun vaalinnan vaiheessa aineisto seulottiin tiheämmällä kammalla, jotta aineistoon ei eksyisi turhia tai epäsopivia artikkeleita. (Okoli ja Schabram, 2010.) Erityisesti huomiota kiinnitettiin tutkimusten laatuun (Aveyard, 2010). Tässä tutkimuksessa käytetään Okolin ja Schabramin (2010) suosittelemia lähestymistapoja sekä laadullisen että määrällisen tutkimuksen tuottaman aineiston laadun arviointiin.

Artikkelien laadun vaalinnan alussa artikkeleita oli valikoitunut tutkimusaineistoon 22 kappaletta, joista kymmenen jouduttiin poistamaan laadun

säilyttämiseksi. Tässä vaiheessa artikkelit luettiin ensimmäisen kerran alusta loppuun ja ne arvioitiin. Tällöin kymmenen artikkelin havaittiin olevan laadultaan tai tutkimusasetelmaltaan vääränlaisia, tai ne eivät vastanneet tämän tutkimuksen kysymysasetteluun. Niitä ei voitu sisällyttää tämän kirjallisuuskatsauksen aineistoon. Hylätyt artikkelit hylkäyssyineen olivat seuraavat:

- Kuusi artikkelia ei käsitellyt tietoturvapolitiikan luomista, vaan sen arviointia tai sen elinkaarta. Nämä artikkelit olivat: Grobler ja Von Solms (2004), Hsu, J. S. C., Shih, S. P., Hung, Y. W., ja Lowry, P. B. (2015), Hu, Q., Xu, Z., Dinev, T., ja Ling, H. (2011), Knapp, K. J., Morris, R. F., Marshall, T. E., ja Byrd, T. A. (2009), Pathari, V., ja Sonar, R. (2012) ja Safa, N. S., Von Solms, R., ja Furnell, S. (2016).
- Yksi artikkeli Horcasilta, Pinmtolta, Fuentekselta ja Montes de Ocalta (2016) hylättiin, sillä se käsittelee ohjelmistojen tietoturvapolitiikkaa eikä organisaatioiden tietoturvapolitiikkaa.
- Yksi Asain ja Hakizaberan (2010) aretikkeli ei käsitellyt lainkaan tietoturvapolitiikkaa tai sen luomista.
- Yksi Sommestadin, Hallbergin, Lundholmin ja Bengtssonin (2014) artikkeli hylättiin, sillä sen havaittiin olevan kirjallisuuskatsaus.

Liitteeseen 2 on listattu arviointikysymykset, jotka on luotu Okolin ja Schabramin (2010) artikkelin ohjeiden mukaisesti. Okoli ja Schabram (2010) viittaavat artikkelissaan Myersin (2008) esittelemään laadullisen tutkimuksen aineiston arviointiin, ja siksi tässä tutkimuksessa käytetään Myersin esittämiä laadullisen aineiston arviointityökaluja. Esimerkkejä Myersin (2008) kysymyksistä ovat: Kuinka hyvin tutkimus vastaa esitettyyn tutkimusongelmaan? Onko aineisto riittävän laadukasta? Kuinka hyvin tutkimustulokset ovat yleistettävissä? Laadullisen aineiston arviointiin käytetään myös Popen, Maysin ja Popayn (2007) viittaaman Spencerin, Ritchien, Lewisin ja Dillonin (2003) kirjoittaman artikkelin pohjautuvia arviointikysymyksiä, jotka ovat hyvin linjassa Myersin (2008) ehdottamien arviointikriteerien kanssa.

Määrällisen tutkimuksen aineiston arviointiin käytettiin kysymyksiä Okolin ja Schabramin (2010) viittaamasta Finkin (2005) artikkelista: Onko tutkimuksessa käytetty hyväksyttyjä ja yleisiä tilastollisia tutkimusmenetelmiä? Onko tutkimuksessa käytetty luotettavia ja oikeita riippuvia ja riippumattomia muuttujia? Minkälaisia asteikkoja tutkimuksessa on käytetty ja ovatko asteikot valittu oikein? Liitteen 2 mukaiset kysymykset asetettiin jokaiselle aineiston artikkelille. Jotta artikkeli voitaisiin ottaa mukaan tutkimukseen, on sen saavutettava vähintään seitsemän kahdestatoista pisteestä. Laadun arvioinnin tulokset, eli artikkelikohtaiset vastaukset on eroteltu liitteessä 3. Liitteessä myös perustellaan, miksi artikkeli on otettu mukaan tutkimukseen. Jos artikkeli ei läpäissyt seulaa, se

rajattiin pois tutkimusaineistosta. Pisteytyksen perusteella karsittiin vielä yksi artikkeli, joka oli Waltonin (2002) teksti.
Seuraavaan vaiheeseen aineiston syvemmästä tarkastelusta selvisi viisi artikkelia. Näistä viidestä artikkelista luotiin analyysit ja ne otettiin mukaan tutkimuksen tuloksena syntyvään synteesiin.

4.2.2 Aineiston louhinta

Aineiston louhinnan tarkoituksena on järjestelmällisesti erotella jäljelle jääneestä aineistosta tutkimuskysymyksen kannalta olennaiset asiat. Tarkoituksena on tuottaa materiaalia, "raaka-ainetta", josta seuraavassa vaiheessa voidaan muodostaa synteesi yhdessä edeltävistä aineiston karsinnan vaiheista saatujen tietojen kanssa. (Okoli ja Schabram, 2010.). Itse louhinta tapahtuu ennen synteesin muodostamista. Louhintaan liittyvät yksityiskohdat on sisällytetty liitteeseen 4.
Aveyard (2010) ohjeistaa artikkelissaan kohdistamaan tutkimusaineistoon kolme kysymystä, joiden avulla voidaan varmistua siitä, onko aineisto riittävän hyvälaatuista sen mukaan ottamiseksi. Kysymykset ovat:

1. Liittyykö tämä tutkimus kirjallisuuskatsaukseen?
2. Vastaako tutkimus kirjallisuuskatsauksen tutkimuskysymykseen?
3. Onko tutkimus tarpeeksi hyvälaatuista, jotta se voidaan sisällyttää kirjallisuuskatsaukseen?

Ensimmäisellä kysymyksellä Aveyard (2010) tarkoittaa, että tutkimus voi vaikuttaa ensisilmäyksellä tutkimuskysymyksen kannalta kannattavalta, mutta tarkemmin luettuna tutkimus osoittautuu vain välillisesti liittyvän kirjallisuuskatsaukseen tai tutkimusta ei voida pitää tarpeeksi luotettavana. Tällöin käsiteltävä aineisto on rajattava pois kirjallisuuskatsauksen aineistosta.

Toisella kysymyksellä Aveyard (2010) tähtää selvittämään, onko aineistona oleva tutkimus olennainen asetetun tutkimuskysymyksen kanssa. Tällä tarkoitetaan sitä, sisältääkö tarkasteltava tutkimus kirjallisuuskatsauksen tutkimuskysymyksen kannalta olennaisia asioita. Tämän kirjallisuuskatsauksen kannalta tutkittavassa aineistossa on olennaista, että siinä käsitellään tietoturvapolitiikan luomista.

Kolmannella kysymyksellä pyritään Aveyardin (2010) mukaan arvioimaan, kuinka luotettavasti ja laadukkaasti tutkittavan aineiston tutkimus on tehty ja sitä, kuinka suuri painoarvo tarkasteltavalle aineistolle tulisi antaa. Aveyard (2010) painottaa, että tätä nimenomaista kysymystä tulisi käyttää erityisen aineiston kriittisessä arvioinnissa.

Aineiston erottelun jälkeen jäljelle jääneeseen aineistoon kohdistettiin edellä mainitut kolme kysymystä aineiston hyödyllisyyden ja laadun takaamiseksi. Aineisto luettiin kahdesti uudestaan alusta loppuun, jotta ymmärrys aineiston sisällöstä ja laadusta saavutettaisiin. Samalla aineistosta kerättiin olennaiset ja tärkeät tiedot, jotta tutkimusaineiston kuvaaminen sujuisi järjestelmällisesti. Tämän

jälkeen synteesin tekeminen aineiston pohjalta mahdollistui. Seuraavassa luvussa kuvataan tässä luvussa kuvatulla tavalla syntynyt ja siivilöity tutkimusaineisto.

5 TUTKIMUSAINEISTON KUVAUS

Tässä luvussa esitellään seulottu tutkimusaineisto, jotta lukijan on helpompi hahmottaa, mitkä artikkelit muodostavat aineiston, missä ja milloin artikkelit on julkaistu ja minkälaisia artikkeleita tutkimusaineisto sisältää, sekä millä tavoin artikkelien aineisto on kerätty ja niiden sisältämä on tehty.

5.1 Aineiston tutkimusmetodit, maat ja viitekehykset

Jotta systemaattinen kirjallisuuskatsaus olisi läpinäkyvä, on tarpeen kuvata aineistoon valikoituneet artikkelit tarkasti. Tässä kappaleessa esitellään aineistoon valikoituneiden artikkeleiden tutkimustyypit, tutkimusmaat ja tutkimusmetodit. Tällöin lukijan on helpompi hahmottaa, mistä aineisto koostuu.

5.1.1 Aineiston tutkimustyyppi

Yleisin tutkimustyyppi aineistoon valikoituneissa artikkeleissa oli selkeästi suunnittelu- ja toimintateoria (engl. *Theory for Design and Action)* (Gregor, 2006). Tätä tutkimustyyppiä esiintyi seitsemässä aineistoon valikoituneessa tutkimuksessa, Corpuz ja Barnes (2010), Flowerday ja Tuyikeze (2016), Grobler ja Solms (2004), Jirasek (2012), Knapp, Morris, Marshall ja Byrd (2009), Kadam (2007) ja Palmer ym. (2001). Kahdessa aineistoon valikoituneessa artikkelissa, Hong ym., 2006 ja Ruighaver, Maynard ja Warren (2010) oli tutkimustyyppinä selittävän tutkimuksen teoria.

5.1.2 Aineiston tutkimusmaat

Neljässä aineistoon valikoituneessa tutkimuksessa aineiston keräämiseen käytetyt maantieteelliset sijainnit oli ilmoitettu. Nämä kyseiset sijainnit olivat Amerikan Yhdysvallat ja Yhdistynyt kuningaskunta (200 vastaajaa molemmissa, Floweday ja Tuyikeze, 2016), Taiwan (165 vastaajaa, Hong ym., 2006). Knapp ym. (2009) oli 220 vastaajaa ja tutkimuksessa vastaajien maat olivat Yhdysvallat (72 % vastaajista), Kanada (5 %), Intia (4 %), Hong Kong (3 %), Yhdistynyt Kuningaskunta (3 %), Uusi-Seelanti (3 %) sekä Ranska, Japani ja Meksiko (vastaajia alle 2 %). Kahdessa tutkimuksessa, Kadamin (2007) ja Palmerin ym. (2001) tutkimuksissa, ei tutkittu maantieteellistä merkitystä sisältävää aihealuetta.

5.1.3 Aineiston tutkimusmetodit

Viidessä aineiston tutkimuksessa tutkimusmetodina oli kyselytutkimus. Nämä artikkelit olivat Flowerdayn ja Tuyikezen (2016), Hongin ym. (2006), Knapp ym.

(2009) ja Palmerin ym. (2001) tutkimukset. Kuitenkin poikkeuksena Palmerin ym. (2001) tutkimus, jonka aineisto oli kerätty aikaisemmin toiseen tutkimukseen, ja heidän artikkelissaan he hyödynsivät samaa dataa. Groblerin ja von Solmsin (2004), Kadamin (2007), Jirasekin (2012) ja Ruighaverin ym. (2010) tutkimusmetodina oli kirjallisuuskatsaus samalla tavalla kuin Corpuzin ja Barnesin (2010) tutkimuksessa.

5.2 Tietoturvapolitiikan luomisen tavat

Ensin esitellään tietoturvapolitiikan luominen riskienhallintaa hyödyntämällä, jonka jälkeen esitellään nykytilanalyysin (GAP-analyysi) sekä tarkastuslistan hyödyntämistä tietoturvapolitiikan luomisessa. Kolmantena esitellään GRC- ja (hyvä hallintotapa, riskienhallinta ja vaatimustenmukaisuus) ja Initial Policy -viitekehyksien käyttö tietoturvapolitiikan luomisessa ja jonka jälkeen esitellään tietoturvapolitiikan luominen hyväksikäyttäen kohdistuvien vaikutusten analyysia. Sitten esitellään avainprosessien sekä ulkoisten ja sisäisten vaikuttimien analysoinnin hyväksikäyttö tietoturvapolitiikan luomisessa ja viimeisenä esitellään eettisten seurausten tarkastelun hyödyntäminen tietoturvapolitiikan luonnissa.

5.2.1 Riskienhallinnan hyödyntäminen

Tutkimusaineistoon valikoitunut artikkeli Corpuzilta ja Barnesilta (2010) ehdotti tietoturvapolitiikan luomista yrityksen riskienhallintasuunnitelman viitekehyksen avulla. Tällä he tarkoittivat sitä, että organisaation IT-osasto ei ole ainut taho, joka luo tietoturvapolitiikan, vaan mukana kirjoittamisessa ja suunnittelussa olisi myös organisaation riskienhallinnasta vastaava taho. Toisin sanoen, he ehdottavat, että perinteistä yrityksen riskienhallintaviitekehystä (CRP) hyödynnettäisiin yrityksen tietoturvapolitiikan luomiseen ja hallinnointiin. Tällöin heidän mukaansa tietoturvapolitiikan hallinnointi olisivat linjassa organisaation riskienhallintapolitiikan kanssa. (Corpuz ja Barnes, 2010)

Toinen riskienhallintaa hyödyntävä ratkaisu oli Flowerdayn ja Tuikezen (2016) artikkelissa: Tietoturvapolitiikan kehityksen elämänkaari (engl. Information Security Policy Development Life Cycle, ISPDLC), jossa kaaren eri kohdista (riskiarviointi, politiikan luominen, politiikan käyttöönotto, politiikan noudattaminen ja politiikan noudattamisen seuranta) kaikkein tärkeimmäksi nousi riskiarviointi. Täten toimivan tietoturvapolitiikan luomisen tähden on tärkeää lähteä rakentamaan politiikkaa riskiarvioinnin pohjalta, sillä tällöin organisaatio voi tunnistaa mahdolliset uhat ja haavoittuvuudet, jotka organisaation tulee minimoida ja poistaa tietoturvapolitiikan avulla. (Flowerday ja Tuikeze, 2016)

5.2.2 Nykytila-analyysin hyödyntäminen

Palmer ym. (2007) esittävät tutkimuksessaan yksityiskohtaisen tietoturvapolitiikkaviitekehyksen. Tämän mukaan tietoturvapolitiikka tulisi luoda käyttäen

hyväksi jo olemassa olevan tietoturvapolitiikan nykytilanalyysia (GAP). Tällöin mahdolliset ongelmakohdat ja puutteet nykyisessä tietoturvapolitiikkaviitekehyksessä huomataan ja voidaan korjata. (Palmer ym., 2007) Toisenlaisen näkökulmaan nykytilan tarkasteluun esitetään Groblerin ja Von Solmsin (2004) artikkelissa, jossa organisaation nykytilanne selvitetään tarkastuslistan avulla. Tällöin heidän mukaansa organisaatio kykenee selvittämään mitä asioita tällä hetkellä tehdään turvallisesti, missä on parantamisen varaa, mitä ei ole lainkaan suojattu politiikan keinoin tai mikä ei ole organisaatiolle olennaista. Samalla listalla myös priorisoidaan kyseiset toimet ja osa-alueet, jolloin jokaiselle kohdalle saadaan kaksi arvoa, joiden painokkuuden mukaan voidaan aloittaa tietoturvapolitiikan luominen. Tällöin organisaatio kykenee tunnistamaan kipupisteensä ja tietoturvapolitiikan keinoin puuttumaan ongelmiin, pienentämään niitä ja mahdollisesti poistamaan kyseiset ongelmat. (Grobler ja Von Solms, 2004).

5.2.3 GRC (hyvä hallintotapa, riskienhallinta ja vaatimustenmukaisuus*)*

Jirasek (2012) esittelee artikkelissaan tietoturvapolitiikan luomista GRC-viitekehyksen avulla. GRC-mallilla tarkoitetaan tässä tapauksessa sellaista tietoturvan viitekehystä, joka jakautuu kolmeen pääkohtaan: tietoturvan eteenpäin vievään voimaan, riskienhallintaan sekä vaatimustenmukaisuuteen. Näiden kohtien perusteella kirjoitetaan tietoturvapolitiikka, joka luo kokonaisvaltaisesti ylätason raamit organisaation toiminnalle tietoturvan näkökulmasta. (Jirasek, 2012)

Tietoturvan eteenpäin ajavilla voimilla tarkoitetaan lakeja ja säädöksiä, jotka vaikuttavat organisaation toimialaan säätelemällä toimintaa. Näistä poikkeamalla ja rikkomalla organisaatio joutuu kohtamaan sanktioita, kuten sakkoja. Toinen turvallisuuden alla oleva eteenpäin ajava voima on liiketoiminnan tavoitteet, joilla tarkoitetaan niitä tavoitteita, joihin organisaatio pyrkii tuottaakseen voittoa. Tietoturvan tehtävä tässä tapauksessa on suojata järjestelmiä ja tietoa, jota käytetään tavoitteiden saavuttamiseen (Jirasek, 2012). Kolmas tietoturvaa eteenpäin ajava seikka ovat eri uhkat. Uhkat voivat vaarantaa organisaation laillisen toiminnan sekä liiketoiminnan tavoitteiden saavuttamisen (Jirasek, 2012).

Toisena GRC-viitekehyksen keskeisenä kohtana on riskien hallinta. Tällä turvallisuuden hallinnalla tarkoitetaan politiikan, prosessien ja turvallisuuden mittaamisen viitekehyksiä. Politiikan viitekehys sisältää esimerkiksi tietoturvapolitiikan sen hallinnointeineen ja luomisineen, standardien ylläpidon ja seuraamisen sekä artefaktit. (Jirasek, 2012) Prosessiviitekehyksellä tarkoitetaan niitä toimia ja toimintoja, joilla politiikan viitekehyksen sisältämät asiat hahmotetaan prosesseina ja ne otetaan osaksi organisaation toimintaa. Kolmannella viitekehyksellä, turvallisuuden mittaamisella tarkoitetaan palautteen keräämistä ja seuraamista eri turvamekanismien ja politikoiden toiminnasta. (Jirasek, 2012) Tällöin voidaan Jirasekin (2012) mukaan havainnoida miten tietoturvaprosessit toimivat ja onnistuvat, sekä tarvitseeko niitä muuttaa.

Kolmas GRC-viitekehyksen keskeinen kohta on vaatimusten mukaisuus. Tällä tarkoitetaan sitä, että organisaation tietoturvallisuus ja sen hallinta eivät ole

ristiriidassa eri sidosryhmien, kuten osakkeenomistajien toiveiden kanssa. Tällöin organisaation tietoturvasta vastaava taho voi osoittaa toimittamalla luvatut kontrollit ja asiat, että turvallisuus kykenee luomaan arvoa organisaatiolle ja sen prosesseille. (Jirasek, 2012)

5.2.4 Initial Policy -viitekehyksen hyödyntäminen

Hongin, Chin, Chaon ja Tangin (2006) Tutkimuksen tarkoituksena oli kartoittaa pääsyitä, joiden takia organisaatio luo tietoturvapolitiikan hyväksikäyttäen ISO/IEC 17799, 2000 -standardin kriteeristöjä. Tietoturvapolitiikan tulee olla suunniteltu tukemaan organisaation keskeisiä tehtäviä ja arvoja. Tämän vuoksi nämä edellä mainitut tehtävät ja arvot tulee olla kartoitettuna, jotta tietoturvapolitiikka voidaan luoda. Kartoituksen jälkeen politiikka voidaan luoda hyväksikäyttäen ISO/IEC 17799, 2000 -standardin kriteeristöä. (Hong, ym., 2006)

5.2.5 Kohdistuvien vaikutusten analyysin hyödyntäminen

Kadam (2007) esittelee tutkimuksessaan tietoturvapolitiikan luomisen metodiksi kohdistuvien vaikutusten analyysin, joka pohjautuu kuuteen kysymyssanaan. Tällä tarkoitetaan sitä, että organisaatiolle tulee esittää kysymykset pohjautuen kysymyssanoihin mitä, miksi, miten, kuka, missä ja milloin (engl. *what*, *why*, *how*, *who*, *where* ja *when*). Näistä kysymyssanoista voidaan Kadamin (2007) mukaan muodostaa olennaisia kysymyksiä, kuten ”mitä arvoa tiedolla on organisaatiolle”, ”kuka on vastuussa tiedon turvaamisesta” ja ”milloin tiedetään, että ovatko turvaamistoimet onnistuneet”. Näihin kysymyksiin vastaamalla voidaan luoda kohdistuvien vaikutusten analyysi (engl. *Business Impact Analysis, BIA*). Analyysin avulla organisaatio voi tunnistaa ne vaikutukset, jotka tietoturvapolitiikan kautta voitaisiin estää, rajoittaa tai hyväksyä. Kadamin (2007) mukaan tällöin tietoturvapolitiikka tulee kirjoittaa tämän analyysin pohjalta, jotta se on tosiasiallisesti vaikuttava positiivisesti niihin toimintoihin, jotka ovat tunnistettu kriittisiksi ja tulevat täten suojata tietoturvapolitiikalla.

5.2.6 Avainprosessit sekä sisäiset ja ulkoiset vaikuttimet

Knapp ym. (2009) esittävät tutkimuksessaan, että tietoturvapolitiikka kannattaa luoda avainprosessien ja sisäisten sekä ulkoisten vaikutusten avulla. Sisäisillä vaikutuksella Knapp ym. (2009) tarkoittavat suosituksia, parhaita käytäntöjä sekä alan vakioituneita standardeja. Ulkoisilla vaikutuksilla he viittaavat organisaation toimialasta johtuviin erityistä huomiota vaativiin tietoturvakysymyksiin (hoito- ja rahoitusala), teknologian tuomiin etuihin, jolla he tarkoittavat teknologian kehittymisen ja muutoksen seuraamista sekä vallalla oleviin säädöksiin ja lakeihin, jotka valtiot säätävät. (Knapp ym., 2009)

5.2.7 Eettisten seurausten tarkastelun hyödyntäminen

Ruighaver ym. esittävät vuoden 2010 artikkelissaan tietoturvapolitiikan luomistavaksi erilaista lähestymistapaa, käyttäjien tekojen eettisten seurausten tarkastelun hyödyntämistä. Tällöin Tietoturvapolitiikka tulee kirjoittaa seurausten etiikkaa tarkastelemalla, jossa tietoturvapolitiikan kirjoittajien tulee teknisten lähtökohtien sijasta asettua tavallisen työntekijän saappaisiin. (Ruighaver ym. 2010) Tällöin tietoturvapolitiikka on lähempänä tavallista käyttäjää ja se keskittyy ja pakottaa käyttäjänsä ajattelemaan tekojensa seurauksia (Ruighaver ym. 2010). Parhaimmillaan eettisiin seurauksiin pohjautuva tietoturvapolitiikka onnistuu ohjaamaan käyttäjiään turvallisempaan toimintaan antamalla heille ilmi, että heidän teoillaan on merkitystä myös organisaation mahdollisille asiakkailla. Tietoturvapolitiikka selittää milloin ja missä olosuhteissa tietyt toiminnot ovat sallittuja ja milloin eivät. (Ruighaver ym. 2010)

6 ANALYYSI

Tässä luvussa esitellään tämän systemaattisen kirjallisuuskatsauksen aineiston teemat ja analyysi, jonka jälkeen seuraavassa luvussa esitellään analyysin pohjalta luodut johtopäätökset. Toisin sanoen, kuten edellä on viitattu, tämän luvun tarkoitus on jäsennetyn aineiston analysointi ja yhdistely joko laadullisen, määrällisen tai molempien metodien tavoin (Okoli ja Schabram, 2010).
Analyysi on olennainen osa systemaattisen kirjallisuuskatsauksen tekemistä itse kirjallisuuskatsauksen kirjoittamisen ohella. Systemaattisen kirjallisuuskatsauksen analyysissä, jota myös synteesiksi kutsutaan, ja tulosten kirjaamisessa on Okolin ja Schabramin (2010) mukaan luontevaa käyttää narratiivista synteesiä. Narratiivisessa synteesissä on etuna se, että sen avulla voidaan laadullisesti analysoida sekä laadullista että määrällistä tutkimusta. Tällöin käytetään apuna taulukointia visuaalisesti hahmottamaan aineiston eroavaisuuksia ja samankaltaisuuksia. (Petticrew ja Roberts, 2006). Tuomen ja Sarajärven (2009) ohjeiden mukaan aineisto kannattaa redusoida, eli pelkistään, jonka jälkeen pelkistetty data kannattaa ryhmitellä luettavuuden ja tulkittavuuden lisäämiseksi. Ryhmittelyn jälkeen muodostetaan tämän tutkimuksen synteesi, eli mitä erilaisia tapoja luoda tietoturvapolitiikka on olemassa. Synteesin muodostaminen aloitetaan palaamalla takaisin alkuperäisen tutkimuskysymyksen pariin, jonka jälkeen palataan lukemaan aineisto läpi ja luokittelemaan se. (Tuomi ja Sarajärvi, 2009).

6.1 Käytettävät metodit tietoturvapolitiikan luomisessa

Kahta artikkelia lukuun ottamatta jokaisessa aineiston artikkelissa esiteltiin erilainen tapa luoda tietoturvapolitiikka. Nämä tavat ovat listattuna seuraavanlaiset:

- Riskien hallinnan hyödyntäminen
- Nykytila-analyysin hyödyntäminen
- GRC-viitekehyksen käyttö
- Initial Policy -viitekehyksen käyttö
- Kohdistuvien vaikutusten analyysin hyödyntäminen
- Avainprosessien ja ulkoisten ja sisäisten vaikuttimien hyväksikäyttö
- Eettisten seurausten hyväksikäyttö

Näiden neljän erilaisen lähestymistavan sekä niiden taustalla olevien tutkimusten sisällön perusteella muodostettiin taulukko 3, jossa eritellään tarkemmin eri tapoja yhdistävät ja erottavat tekijät.

TAULUKKO 3 Tutkimusartikkeleiden teemat

Teemat	Tietoturvapolitiikan luomistapa
Riskien tunnistaminen ja hallinta	Tavallisen riskienhallintaviitekehyksen hyväksikäyttö Tietoturvapolitiikan elinkaaren riskienhallinta GRC-viitekehys
Yleiset analyysityökalut	Nykytila-analyysi Kohdistuvien vaikutusten analyysi
Organisaation keskeiset tehtävät ja arvot	Initial Policy -viitekehys Avainprosessien ja sisäistä ja ulkoisten vaikutusten havainnointi Käyttäjien toimien eettisten seurausten tarkastelu Organisaation prosessien, tarpeiden ja toimien arviointi

6.1.1 Riskien tunnistaminen ja hallinta

Riskien tunnistamiseen ja hallintaan sijoittui kolme artikkelia aineistosta. Artikkelit tarkastelivat tietoturvapolitiikan luomista riskienhallinnan näkökulmasta, sillä erotuksella, että yksi artikkeleista tarkasteli tietoturvapolitiikan luomista hyväksikäyttäen tietoturvapolitiikan elinkaarta, kun toinen artikkeli tarkasteli tietoturvapolitiikan luomista tavallisen riskienhallintaviitekehyksen kautta. Kolmas artikkeli käsitteli riskien kokonaisvaltaista hallintaa ja tunnistamista GRC-viitekehyksen kautta.
Riskienhallintasuunnitelman viitekehyksen avulla luodessa tietoturvapolitiikkaa noudatetaan samoja suuntaviivoja kuin riskienhallintapolitiikkaa luodessa. Tällöin tietoturvapolitiikkaa ei ole luomassa vain IT-osasto, vaan luomistyössä on mukana myös riskienhallinnasta vastaava taho. Itse tietoturvapolitiikan luomisen suurimmat askelmerkit ovat tällöin ympäristön riskien havainnointi, turvallisuusriskianalyysi ja turvallisuusriskiarviointi. Tällöin tunnistamalla yrityksen toiminnalle suurimmat riskit voidaan yhteistyössä riskeistä vastaavan tahon kanssa luoda kattava tietoturvapolitiikka, joka on sidottu konkreettisiin ja tunnistettuihin riskeihin sekä yrityksen riskienhallintapolitiikkaan. Samalla tavalla tietoturvapolitiikan elinkaaren riskiarviointia hyväksikäyttämällä voidaan saada toimiva ja konkreettisiin ongelmiin pureutuva tietoturvapolitiikka. Tällöin tietoturvapolitiikka keskittyy ohjaamaan organisaation tietoturvaa tukemaan liiketoiminnan tarpeita sekä vastaamaan ylätasolla tietoturvallisuuden tavoitteisiin.

Voidaan siis todeta, että on mahdollista riskienhallintaa hyödyntämällä luoda tehokas tietoturvapolitiikka, joka luodaan yhteistyössä muidenkin kuin IT-osaston asiantuntijoiden kanssa. Tietoturvapolitiikka huomioi tällöin organisaation toimintaympäristön, sen asettamat rajoitteet ja pakotteet sekä organisaation omat tarpeet.

6.1.2 Yleiset analyysityökalut

Kahdessa aineiston tutkimuksessa käsiteltiin tietoturvapolitiikan luomista yleisiä ja tunnettuja analyysityökaluja käyttäen. Nykytila-analyysia hyväksikäyttämällä on tarkoitus tarkastella organisaation nykytilannetta, jonka pohjalta voidaan luoda tietoturvapolitiikka. Tunnistamalla nykyhetken onnistumiset ja heikkoudet, sekä puutteet nykyisissä politiikoissa, standardeissa sekä prosesseissa voidaan tietoturvapolitiikkaa kirjoittaa kattamaan ja tukemaan myös organisaation heikkouksia. Voidaan siis katsoa, että tietoturvapolitiikka saadaan tällöin nykytila-analyysin kartoituksen avulla kattamaan paremmin myös vähemmän teknisten ongelmien tietoturvaongelmat.

Kohdistuvien vaikutusten analyysi tietoturvapolitiikan luomisen apuvälineenä voi tuottaa organisaatiolle sen liiketoimintaa ja ydinprosesseja tukevan tietoturvapolitiikan. Tällöin tietoturvapolitiikka on hieman enemmän riskiperusteisempi kuin nykytila-analyysiin perustuva tietoturvapolitiikka. Kuitenkin tässä tapauksessa tietoturvapolitiikka luodaan ydinprosessien ja liiketoiminnan suojaamiseen ja turvaamiseen niiden haavoittuvuuksien perusteella, niin, että tietoturvapolitiikka tukee toimintaa enemmän kuin rajoittaa sitä.

Näiden seikkojen valossa voitaisiin todeta, että luomalla tietoturvapolitiikka hyväksikäyttäen tunnettuja, yleisiä analyysityökaluja on tietoturvapolitiikka valmiina mahdollisesti lähellä organisaation ydintoimintaa. Tietoturvapolitiikkaa luodessa organisaatio myös joutuu tarkastelemaan ja tunnistamaan ydinprosessejaan ja mahdollisesti tunnistaa uusia kehitystarpeita tulevaisuuden varalle. Yleisten analyysityökalujen käytön eduksi voidaan lukea tunnettavuus sekä helppokäyttöisyys; organisaatiot ovat usein käyttäneet kyseisiä työkaluja jo aikaisemmin, eikä tällöin organisaation tarvitse ostaa tai oppia käyttämään mahdollisesti uutta työkalua tietoturvapolitiikan parantamisen tai luomisen takia.

6.1.3 Organisaation keskeiset tehtävät ja arvot

Organisaation keskeisiin tehtäviin ja arvoihin perustuva tietoturvapolitiikan luominen esiintyi neljässä aineiston artikkelissa. Keskisiin tehtäviin ja arvoihin perustuvassa tavassa luoda tietoturvapolitiikka suurin painoarvo sijoittuu itse organisaation sisäisiin tavoitteisiin ja tapoihin. Organisaation kulttuuri, prosessit ja luonne määrittelevät sen, minkälaisen tehokkaan tietoturvapolitiikan organisaatio voi luoda itselleen. Tämän takia organisaatioiden on ennen tietoturvapolitiikan luomista tunnistettava oman yhteisönsä keskiset tehtävät ja arvot, ja vasta sen jälkeen luoda tietoturvapolitiikka hyväksikäyttäen esimerkiksi ISO/IEC 17799, 2000 – tai 27001-standardia. Sisäisten arvojen, tehtävien ja tekojen eettisten seurausten sisällyttämisellä tietoturvapolitiikkaan voidaan tällöin luoda politiikka, joka tukee organisaation toimintaa ja sen arvoja. Tällöin organisaation on luonnollisempaa ottaa käyttöön ja noudattaa tietoturvapolitiikkaa.

7 TULOKSET

Tässä luvussa esitellään tämän tutkimuksen tulokset, niiden arviointi sekä pohdinta siitä, mitä tulokset kertovat tutkimusongelmasta. Luvussa arvioidaan ja pohditaan myös itse tutkimusprosessin sekä tutkimusmetodin onnistumista ja merkitystä.

7.1 Tulokset

Tutkimuksen tuloksien voidaan katsoa jääneen sangen laihoiksi johtuen tutkittavan aineiston ohuudesta. Tästä huolimatta, tulokset osoittavat, että tietoturvapolitiikan luomiselle on aikaisemmissa tutkimuksessa esitetty erilaisia vaihtoehtoisia tapoja. Tuloksena syntyi taulukko (taulukko 3), jossa luokiteltiin löydettyjen artikkeleiden pohjalta erilaiset tavat luoda tietoturvapolitiikka.

Tuloksia tarkastelemalla voidaan huomata, että tietoturvapolitiikan luomiseen on käytettävissä erilaisia keinoja, jotka eivät kuitenkaan lopulta laajasti eroa toisistaan, sillä keinot tähtäävät samaan lopputulokseen, hyvin kirjoitettuun tietoturvapolitikkaan. Tavoissa oli kuitenkin eroavaisuuksia: Riskiarvioinnin kautta kirjoitettavien tietoturvapolitiikkametodien (Corpuz ja Barnes, 2010; Flowerday ja Tuyikeze, 2016, Jirasek, 2012) tuloksena syntyvä tietoturvapolitiikka nojaa organisaation jo valmiiseen riskienhallintaan ja sen metodiikkaan. Tällöin kyseisen metodin avulla luotavan tietoturvapolitiikan organisaation tulee olla riittävän kypsä ja omistaa jo olemassa oleva riskienhallintapolitiikka tai suunnitelma, jotta tietoturvapolitiikka voidaan luoda riskienhallinnan avulla.

Yleisten riskienhallintatyökalujen, kuten kohdistuvien vaikutusten analyysin ja nykytilanalyysin käyttö tietoturvapolitiikan laatimisen tukena vaatii tekijäorganisaatiolta kyseisten työkalujen käyttötaidon sekä tilaisuuden käyttää niitä. Tällä tarkoitetaan sitä, että organisaation tulee kyetä yleisiä analyysityökaluja hyödyntämällä tarkastelemaan omaa toimintaansa, heikkouksiaan ja vahvuuksiaan, jolloin saatujen tulosten pohjalta voidaan kirjoittaa organisaation tietoturvapolitiikka. Kyseisten työkalujen hyväksi voidaan lukea se tosiasia, että edellä mainitut työkalut ovat yleisesti tunnettuja sekä niiden saatavuuden ja käytön voidaan katsoa olevan helppoa. Yleisiä analyysityökaluja käyttämällä organisaatiot voivat myös saada muuta tietoa omasta toiminnastaan, kuten Kadam (2007) esitteli tutkimuksessaan kohdistuvien vaikutusten analyysiä: organisaation ydinprosessien kartoitus sekä niihin kohdistuvien uhkien arviointi voi auttaa organisaatiota parantamaan omaa toimintaansa myös tietoturvapolitiikkaan liittymättä. Palmer, Robinson, Patilla ja Moser (2001) esittelivät nykytila-analyysin käytössä vaatimuksen nykyisestä, jo olemassa olevasta tietoturvapolitiikasta, joka altistetaan nykytila-analyysille. Tällöin heidän mukaansa mahdolliset ongelmakohdat ja puutteet nykyisessä tietoturvapolitiikkaviitekehyksessä voidaan huomata sekä korjata.

Kolmannessa tämän tutkimuksen esitetyssä teemassa, Organisaation keskeiset tehtävät ja arvot, esiteltiin esimerkiksi Hongin ym., (2006) ehdottama Initial Policy -viitekehys, joka hyväksikäyttää organisaation keskeisiä tehtäviä ja arvoja. Tässä nimenomaisessa tavassa on suurammat eroavaisuudet edellä mainittuihin kahteen tietoturvapolitiikan luomisen tapaan. Hongin ym. (2006) esittämällä metodiikalla tietoturvapolitiikka luodaan tukemaan organisaation olemassaolon pääsyitä tunnistamalla organisaation eksistenssin kannalta olennaiset toiminnot ja tahot. Näitä vasten peilaten organisaation tulisi kirjoittaa tietoturvapolitiikka hyväksikäyttäen jo olemassa olevien standardeja, kuten ISO/IEC 17799, 2000 ja ISO 27001 -standardeja. Hongin ym. (2006) mukaan itse tietoturvapolitiikan kirjoittamista olennaisempaa organisaatiolle on ymmärtää mihin tarkoitukseen ja minkälaiselle organisaatiolle tietoturvapolitiikka kirjoitetaan, sillä hyvä ja tunnettu standardi on toissijaista verrattuna organisaation arvojen ja tehtävien tuntemiseen perusteellisesti. Toisin sanoen, Hongin ym., (2006) tekstin mukaan tärkeintä tietoturvapolitiikan luomisessa on tuntea sen tarvitseva organisaatio kuin se, miten itse politiikka kirjoitetaan. Tätä tukevat Knapp ym. (2009), Grobler ja Von Solms (2004), sillä he korostivat omissa artikkeleissaan myös organisaation itsetuntemuksen tärkeyttä: tietoturvapolitiikka kannattaa kirjoittaa noudattamaan organisaation ja ympäröivän maailman asettamia vaateita sekä tukemaan organisaation toimintaa. Erilaisen lähestymistavan organisaation keskeisiin tehtäviin ja arvoihin esittävät Ruighaver ym. (2010). He lähestyvät tietoturvapolitiikan tekemistä käyttäjien toimien eettisten seurausten näkökulmasta. Tässä tapauksessa myös organisaation oma toiminta ja sen tunteminen korostuvat, sillä käyttäjät ovat osa organisaatiota, ja täten heidän tuntemisensa voidaan laskea osaksi organisaation itsetuntemusta.

7.2 Tutkimuksen merkitys

Tämän tutkimuksen heikkous nousee esiin tässä luvussa: Aineiston vähyyden takia on suhtauduttava kriittisesti tämän tutkimuksen tuloksiin, sillä tämä tutkimus on kestänyt liian kauan aikaa, eikä näitä tuloksia voi pitää enää kovin yleistettävinä. Tutkimuksen tarkoitus oli kartoittaa mitä erilaisia tapoja on luoda tietoturvapolitiikka ja tutkimuksen oli määrä valmistua vuodessa, mutta tutkijan omien syitten takia tutkimus valmistui vasta kolme vuotta sen aloittamisen jälkeen, eikä sitä voida pitää luotettavuutta lisäävänä tekijänä systemaattisen kirjallisuuskatsauksen kannalta, vaikka tutkimus tehtiin noudattaen Okolin ja Schabramin (2010) ohjeita. Systemaattiselle kirjallisuuskatsaukselle tyypillisesti tämä tutkimus ei antanut laajaa ja uutta tietoa, vaan pyrki keräämään ja kasaamaan aikaisemman tutkimuksen tuloksia sekä tarkastelemaan niitä. Toisin sanoen, tämän tutkimuksen merkitys on vähäinen, vaikka se loi pienen ja lyhyen taulukon eri tavoista luoda tietoturvapolitiikka (taulukko 3).

7.3 Tutkimusmenetelmä

Tämän tutkimus rakentui Okolin ja Schabramin (2010) kirjoittaman systemaattisen kirjallisuuskatsauksen ohjeen pohjalle. Kuten he kirjoittivat artikkelissaan, on systemaattisessa kirjallisuuskatsauksessa tärkeää, että lukija pystyy seuraamaan tutkijan jalanjäljissä koko tutkimuksen matkan. Tämän tähden tässä tutkimuksessa pyrittiin huomioimaan ja dokumentoimaan mahdollisimman tarkasti tutkimuksen eri vaiheet. Okoli ja Schabram (2010) esittivät tekstissään, että systemaattisessa kirjallisuuskatsauksessa on tämän takia etsittävä ja valittava aineisto, seulottava aineistosta tutkimukselle merkitykselliset tutkimukset sekä vaalittava aineistossa tarvittavan korkeaa laatua.

Materiaalin haku suoritettiin kahdessa osassa, ja sen aikana havaittiin, että itse hakulausekkeen muodostaminen niin, että se tuottaa hyödyllisen määrän aineistoa on todella tärkeää ja hankalaa. Useamman yrityksen jälkeen hakulause saatiin tarpeeksi rajatuksi, jotta aineiston keruu voitiin aloittaa. Aineiston keruussa on huomattava tutkijan harjaantumattomuus, sillä aineiston koko kasvoi nopeasti suureksi, joka tuotti myöhemmin ylimääräistä työtä seuraavassa vaiheessa, kriittisessä arvioinnissa.

Tutkimuksen suurin ja raskain työ oli materiaalin hakua seuranneessa kriittisessä arvioinnissa. Tutkimuksen alussa määriteltiin tutkimukseen mukaan otettavan aineiston sisäänottokriteerit. On huomattava, että vaikka kriteeristö oli itsessään helppo luoda, oli niihin palattava jatkuvasti kriittisen arvioinnin aikana. Huomattava määrä aineistosta jouduttiin poistamaan, sillä ne eivät joko käsitelleet tutkimuksen aihetta, olivat tutkijan saavuttamattomissa maksumuurin takana tai olivat korruptoituneet eikä aineistoa voitu kyseisten artikkelien osalta palauttaa. Kriittisen arvioinnin aikana myös havaittiin muutama kaksoiskappale, jotka olivat päätyneet aineistoon. Kaksoiskappaleet poistettiin aineistosta.

Kriittisen arvioinnin jälkeen artikkelit luettiin vielä uudestaan. Tässä lähiluvussa huomio keskittyi aineiston laatuun, jonka takia artikkelit pisteytettiin. Apuna aineiston pisteytyksessä käytettiin sekä Aveyardin (2010), Myersin (2008), Popen ym., (2007) että Spencerin ym., (2003) ohjeita systemaattisen kirjallisuuskatsauksen kriittisen arvioinnin tekemiseen. Tämän vaiheen jälkeen tutkimuksen aineistoon hyväksyttäviä artikkeleita oli aineistossa jäljellä viisi kappaletta. Tässä vaiheessa on huomattava, että epäilys aineiston riittävyydestä nousi esiin. Pitkän epäilyn jälkeen tämän pro gradu -tutkielman ohjaajan kanssa sovittiin, että aineiston sisäänottokriteerejä kannattaa höllentää, vaikka mahdollisuus systemaattisen kirjallisuuskatsauksen vaatiman korkean tason laskemiseen korostuu. Myös Aveyardin (2014) ohjeistus tuki tätä ratkaisua: hänen mukaansa viiden hyvälaatuisen artikkelin mukaan kannattaa harkita otettavan mukaan heikommalla tasolla varustettuja tai vähemmän relevantteja tutkimuksia. Tämä asia tulee vain selostaa tutkimuksessa ja selittää että kirjoittaja on tietoinen niin sanotun heikomman aineksen olemassa olosta tutkimusaineistossa, sillä tarpeeksi korkealaatuista aineistoa ei osattu tai kyetty löytämään (Aveyard, 2014). On hyvin

todennäköistä, että aineistosta karsittiin tutkijan oman osaamattomuuden takia tutkimukseen kelpaavia artikkeleita, minkä voidaan katsoa johtaneen aineiston pienuuteen ja vaikuttaneen heikentävästi tämän tutkimuksen laatuun. Uusiksi ehdokkaiksi aineistoon otettiin seitsemän artikkelia, jotka arvioitiin uudestaan. Nämä kyseiset artikkelit ovat esitettynä alla olevassa listassa

- Chaudry, Chaudry ja Reese, 2012,
- Grobler ja Von Solms, 2004
- Pathari ja Sonar, 2012
- Jegede, Aimufua ja Salami, 2007
- Jirasek, 2012
- Knapp, Morris, Marshall ja Byrd, 2009
- Ruighaver, Maynard ja Warre, 2010
- Walton, 2002

Artikkeleista neljä todettiin laadultaan ja sisällöltään sellaisiksi, että ne voitiin ottaa mukaan tutkimukseen. Nämä artikkelit olivat Grobler ja Von Solms (2004), Jirasek (2012), Knapp ym. (2009). Täten lopulliseen kriteeristön höllentämisen jälkeen aineistoon saatiin yhdeksän artikkelia tutkittavaksi ja synteesin muodostamiseksi.

8 JOHTOPÄÄTÖKSET

Tämän tutkimuksen tarkoituksena oli kartoittaa aiemmin kirjallisuudessa esitetyt tavat luoda tietoturvapolitiikka. Tutkimuksen alussa esitetty tutkimuskysymys oli ”minkälaisia tapoja on tietoturvapolitiikan luomiseen?”.

Tämän teoreettisen pro gradu -tutkielman tuoma hyöty ei ole välttämättä suuri, mutta sen voidaan katsoa paljastavan sen seikan, että tutkittavaa tietoturvapolitiikan luomisen eri tavoissa ja niiden kehittämisessä on vielä edessä. Tutkimuksessa pyrittiin tarkastelemaan systemaattisen kirjallisuuskatsauksen keinoin, millä tavalla tietoturvapolitiikan luomista on käsitelty aiemmassa tieteellisessä kirjallisuudessa ja minkälaisia toimintatapoja tietoturvapolitiikan luomiselle on esitetty. Tutkimuksen tuloksena saatiin aikaan kolmiosainen teemoitus niistä tavoista, joilla tietoturvapolitiikka voidaan ylätasolla luoda.

Tutkimuksen tulokset esittävät, että tietoturvapolitiikan luomista on käsitelty aiemmassa tutkimuksessa suhteellisen vähänlaisesti, ja että teemoittain esitettynä tapoja luoda tietoturvapolitiikka on kolme. Tavoista kolme painottui riskeihin ja kolmas organisaation oman kulttuurin ja prosessien tuntemiseen. Voidaankin mieltään, että tietoturvapolitiikan luominen on yleisempää organisaation oman tekemisen ja prosessien itsetutkiskelun avulla. Riskienhallinnan ja tunnistamisen tärkeyttä edellä mainittuihin voidaan myös kuitenkin painottaa, ja sen voidaan katsoa myös olevan hyödyllistä tietoturvapolitiikan luomisen kannalta.

Empiirisen jatkotutkimuksen kannalta hedelmällisiä uusia tutkimusaiheet voisivat esimerkiksi liittyä yksittäisten tietoturvapolitiikkojen luomiseen ja niiden luomisprosessien tarkkailuun sekä vertailuun. Tämä tutkimus kartoitti artikkeleita tietoturvapolitiikan luomisesta vuosien 1999 – 2016 välillä, jolloin teoreettisen jatkotutkimuksen kannalta voisi olla hyödyllistä jatkaa tutkimusta vuoden 2016 jälkeen ilmestyneiden tutkimusten ja artikkeleiden joukosta. Pitkittäistutkimuksen kannalta voisi olla mielenkiintoista tarkkailla tietoturvapolitiikan elinkaaren kaikkia vaiheita sen luomisesta poistamiseen asti. Tällöin mielenkiinto voisi kohdistua siihen, kuinka paljon tietoturvapolitiikka mahdollisesti muuttuu elinkaarensa aikana, ja onko mahdollista luoda alusta alkaen tietoturvapolitiikka, jota ei tarvitsisi muuttaa.

Tämän tutkimuksen tekeminen oli tekijälleen suuri työ, ja se valitettavasti näkyy myös tutkimuksen laadussa sekä rajoittuneisuudessa. Tutkimusmetodina käytetty systemaattinen kirjallisuuskatsaus on työmäärältään laaja, ja vaatii käyttäjältään pikkutarkkaa sekä pitkäjänteistä työskentelytapaa. Tekijän omat taidot mahdollisesti rajoittivat liikaa aineiston laajuutta seulonnan liiallisella tarkkuudella, jolloin vakuuttavia yleistyksiä ja johtopäätöksiä tämän pro gradun tuloksista ei ole luultavasti suotavaa tehdä.

LÄHTEET

Atkinson, P. E. (1997). Creating Culture Change: Strategies for Success. Rushmere Wynne Limited.

Aveyard, H. (2014). Doing a literature review in health and social care: A practical guide. McGraw-Hill Education (UK).

Aveyard, H. (2010) Doing a Literature Review in Health and Social Care. A practical guide. Maidenhead: Open University Press.

Baskerville, R., & Siponen, M. (2002). An information security meta-policy for emergent organizations. Logistics Information Management, 15(5/6), 337-346. doi: 10.1108/09576050210447019

Calder, A., & Watkins, S. G. (2010). Information security risk management for ISO27001/ISO27002. It Governance Ltd.

Ernst & Young Global Limited (2015). Creating trust in the digital world EY's Global Information Security Survey. Viitattu 10.6.2016 at: http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2015/$FILE/ey-global-information-security-survey-2015.pdf

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. Information Systems Journal, 11(2), 127-153. doi: 10.1046/j.1365-2575.2001.00099.x

Fink, A. (2013). Conducting research literature reviews: from the Internet to Paper. Sage Publications.

Fink, A. (2005). Conducting research literature reviews: from the Internet to paper. Sage Publications.

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. computers & security, 31(8), 983-988. doi: 10.1016/j.cose.2012.08.004

Gregor, S. (2006). The nature of theory in information systems. MIS quarterly, 611-642. doi: 10.2307/25148742

Hart, C. (1998). Doing a literature review: Releasing the social science research imagination. Sage. Cengage Learning. doi:

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), 106-125. doi: 10.1057/ejis.2009.6

Höne, K., & Eloff, J. H. P. (2002). Information security policy—what do international information security standards say?. Computers & Security, 21(5), 402-409. doi: 10.1016/S0167-4048(02)00504-7

Joint Information Systems Committee (JISC). 16 March 2001. Developing an Information SecurityPolicy. Viitattu 3.6.2016 http://www.jisc.ac.uk/pub01/security_policy.htm doi: 10.1016/S0167-4048(02)00504-7

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information systems security policies: a contextual perspective. Computers & Security, 24(3), 246-260. doi: 10.1016/j.cose.2004.08.011

Kekäle, T., de Weerd-Nederhof, P., Cervai, S., & Borelli, M. (2009). The "dos and don'ts" of writing a journal article. Journal of Workplace Learning, 21(1), 71-80. doi: 10.1108/13665620910924925

Kotimaisten kielten keskus (2016). Kielitoimiston sanakirja. Viitattu 24.5.2016. http://www.kielitoimistonsanakirja.fi/netmot.exe?motportal=80

Myers, P. M. D. (2008). Qualitative Research in Business & Management (kuvitettu painos.). Sage Publications Ltd.

Okoli, C., & Schabram, K. (2010). A guide to conducting a systematic literature review of information systems research. Sprouts Work. Pap. Inf. Syst, 10, 26. doi: :10.2139/ssrn.1954824

Petticrew, M., & Roberts, H. (2006). Systematic reviews in the social sciences: A practical guide. Blackwell Pub. doi: 10.1002/9780470754887

Pope, C., Mays, N., & Popay, J. (2007). Synthesising qualitative and quantitative health evidence: A guide to methods: A guide to methods. McGraw-Hill Education (UK).

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. Mis Quarterly, 757-778. doi: 10.2307/25750704

Raggad, B. G. (2010). Information security management: Concepts and practice. CRC Press. doi: 10.1201/9781439882634

Rousseau, D. M., Manning, J., & Denyer, D. (2008). 11 Evidence in Management and Organizational Science: Assembling the Field's Full Weight of Scientific Knowledge Through Syntheses. The academy of management annals, 2(1), 475-515. doi: 10.5465/19416520802211651

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. Information & management, 51(2), 217-224. doi:

Spencer, L., Ritchie, J., Lewis, J., & Dillon, L. (2003). Quality in qualitative evaluation: a framework for assessing research evidence.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. MIS quarterly, 441-469 doi: 10.2307/249551

Straub, D. W., Goodman, S. E., & Baskerville, R. (2008). Information security: policy, processes, and practices. ME Sharpe. doi: 10.4324/9781315288697

Thomson, K. L., & Von Solms, R. (2005). Information security obedience: a definition. Computers & Security, 24(1), 69-75. doi: 10.1016/j.cose.2004.10.005

Tuomi, J., & Sarajärvi, A. (2009). Laadullinen tutkimus ja sisällönanalyysi. Tammi.

Von Solms, R., & Von Solms, B. (2004a). From policies to culture. Computers & security, 23(4), 275-279. A doi: 10.1016/j.cose.2004.01.013

Von Solms, B., & Von Solms, R. (2004b). The 10 deadly sins of information security management. Computers & Security, 23(5), 371-376. doi: 10.1016/j.cose.2004.05.002

Whitman, M. E., & Mattord, H. J. (2011). Principles of information security. doi:

LIITE 1 TUTKIMUSAINEISTO

Corpuz, M., & Barnes, P. H. (2010). Integrating information security policy management with corporate risk management for strategic alignment. In Proceedings of the 14th World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2010). doi:

Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. computers & security, 61, 169-183. doi: 10.1016/j.cose.2016.06.002

Grobler, T., & Von Solms, S. (2004). Assessing the policy dimension. Johannesburg, South Africa: Technikon Witwatersrand.

Hong, K. S., Chi, Y. P., Chao, L. R., & Tang, J. H. (2006). An empirical study of information security policy on information security elevation in Taiwan. Information Management & Computer Security, 14(2), 104-115. doi: 10.1108/09685220610655861

Jirasek, V. (2012). Practical application of information security models. Information security technical report, 17(1-2), 1-8. doi: 10.1016/j.istr.2011.12.004

Kadam, A. W. (2007). Information security policy development and implementation. Information Systems Security, 16(5), 246-256. doi: 10.1080/10658980701744861

Knapp, K. J., Morris Jr, R. F., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. computers & security, 28(7), 493-508. doi: 10.1016/j.cose.2009.07.001

Ruighaver, A. B., Maynard, S. B., & Warren, M. (2010). Ethical decision making: Improving the quality of acceptable use policies. Computers & Security, 29(7), 731-736. doi: 10.1016/j.cose.2010.05.004

Palmer, M. E., Robinson, C., Patilla, J. C., & Moser, E. P. (2001). Information security policy framework: best practices for security policy in the e-commerce age. Information Systems Security, 10(2), 1-15. doi: 10.1201/1086/43314.10.2.20010506/31399.4

LIITE 2 LAADUN ARVIOINTIKRITEERISTÖ

Artikkeli	Kyllä	Ei	Pisteet
Aikaisemman tutkimuksen esittely			
Tutkimuksen tarkoitus selitetty selkeästi			
Aineiston muodostuminen selostettu			
Tutkimusjoukon esittely			
Tulosten selkeä esittely			
Tulosten vertailu aikaisempiin tutkimuksiin			
Tulosten merkitysten arviointi			
Tutkimuksen kontekstin esittely			
Tutkimuksen luotettavuuden arviointi			
Tutkimusetiikan arviointi			
Hyväksyttyjen ja yleisten tilastollisten tutkimusmenetelmien käyttö			
Luotettavien ja oikeiden riippuvien ja riippumattomien muuttujien käyttö			
Oikeanlaisten asteikoiden käyttö ja valinta			
Kuinka hyvin tutkimus vastaa esitettyyn tutkimusongelmaan			
Onko aineisto riittävän laadukasta			
Kuinka hyvin tutkimustulokset ovat yleistettävissä			
Lopputulos			

LIITE 3 KRIITTINEN ARVIONTI

Tutkimusartikkeli	Laatumääritykset	Pistey-tys
Corpuz, M., & Barnes, P. H. (2010). Integrating information security policy management with corporate risk management for strategic alignment. In *Proceedings of the 14th World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2010)*.	-Aikaisempaa tutkimusta on esitelty -Tutkimuksen tarkoitus on kerrottu selkeästi -Aineiston muodostuminen on selostettu -Tutkimusjoukko on esitelty -Tutkimus vastaa esitettyyn tutkimusongelmaan -Aineisto on riittävän laadukasta -Tutkimuksen tulokset ovat yleistettävissä -Tulokset ovat esitelty selkeästi -Tulosten merkitys on arvioitu -Tulosten konteksti on esitelty -Tutkimuksen luotettavuutta ei arvioitu -Tuloksia ei ole vertailtu aikaisempiin tutkimuksiin -Tutkimusetiikkaa ei ole arvioitu	10/13
Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *computers & security*, *61*, 169-183.	-Aikaisempaa tutkimusta on esitelty -Tutkimuksen tarkoitus on kerrottu selkeästi -Aineiston muodostuminen on selostettu -Tutkimusjoukko on esitelty -Tutkimus vastaa esitettyyn tutkimusongelmaan -Aineisto on riittävän laadukasta -Tutkimustulokset ovat yleistettävissä -Tulokset ovat esitelty selkeästi -Tulosten merkitystä on arvioitu -Tutkimuksen konteksti on esitelty -Tutkimuksen luotettavuus on arvioitu -Tutkimusetiikkaa ei ole arvioitu -Tuloksia ei ole vertailtu aikaisempiin tutkimuksiin	11/13
Grobler, T., & Von Solms, S. (2004). Assessing the policy dimension. *Johannesburg, South Africa: Technikon Witwatersrand*.	-Aikaisempaa tutkimusta on esitelty -Tutkimuksen tarkoitus on kerrottu selkeästi -Tutkimus vastaa esitettyyn tutkimusongelmaan -Tutkimustulokset ovat yleistettävissä -Tulokset ovat selkeästi esitetty -Tulosten merkitystä on arvioitu -Tutkimuksen konteksti on esitelty -Tutkimuksen luotettavuutta ei ole arvioitu -Tutkimuksen aineiston muodostumista ei ole selitetty -Tutkimusjoukkoa ei ole esitelty -Tutkimusetiikkaa ei ole arvioitu	7/13

	-Aineiston laadukkuutta ei ole arvioitu -Tuloksia ei ole verrattu aikaisempiin tutkimuksiin	
Hong, K. S., Chi, Y. P., Chao, L. R., & Tang, J. H. (2006). An empirical study of information security policy on information security elevation in Taiwan. *Information Management & Computer Security*, *14*(2), 104-115.	-Aikaisempaa tutkimusta on esitelty -Tutkimuksen tarkoitus on kerrottu selkeästi -Aineiston muodostuminen on selostettu -Tutkimusjoukko on esitelty -Tutkimus vastaa esitettyyn tutkimusongelmaan -Tutkimustulokset ovat yleistettävissä -Tulokset ovat esitelty selkeästi -Tulosten merkitystä on arvioitu -Tutkimuksen konteksti on esitelty -Tutkimuksen luotettavuutta on arvioitu -Tutkimusetiikkaa ei ole arvioitu -Aineiston laadukkuutta ei ole arvioitu -Tuloksia ei ole verrattu aikaisempiin tutkimuksiin	10/13
Jegede, A. J., Aimufua, G. I. O., & Salami, H. O. (2007). Information Security Policy: Relevance, Creation and Enforcement. *International Journal of Soft Computing, 2(3), 408-410.*	-Tutkimus vastaa esitettyyn tutkimusongelmaan -Tutkimustulokset ovat yleistettävissä -Tulokset ovat esitelty selkeästi -Tulosten merkitystä on arvioitu -Tutkimuksen konteksti on esitelty -Aikaisempaa tutkimusta ei ole esitelty -Tutkimuksen tarkoitus ei ole kerrottu selkeästi -Aineiston muodostumista ei esitelty -Tutkimusjoukkoa ei ole esitelty -Tutkimusetiikkaa ei ole arvioitu -Aineiston laadukkuutta ei ole arvioitu -Tuloksia ei vertailtu aikaisempiin tutkimuksiin -Tutkimuksen luotettavuutta ei ole arvioiti	5/13
Jirasek, V. (2012). Practical application of information security models. *Information security technical report*, *17*(1-2), 1-8.	-Aineiston muodostuminen on selostettu -Tutkimus vastaa esitettyyn tutkimusongelmaan -Aineisto on riittävän laadukasta -Tutkimustulokset ovat yleistettävissä -Tulokset ovat esitelty selkeästi -Tulosten merkitystä on arvioitu -Tutkimuksen konteksti on esitelty -Aikaisempaa tutkimusta ei ole esitelty	5/13

	-Aineiston muodostumista ei esitelty -Tutkimusjoukkoa ei ole esitelty -Tutkimusetiikkaa ei ole arvioitu -Tuloksia ei vertailtu aikaisempiin tutkimuksiin -Tutkimuksen luotettavuutta ei ole arvioitu	
Kadam, A. W. (2007). Information security policy development and implementation. *Information Systems Security, 16*(5), 246-256.	-Tutkimuksen tarkoitus on kerrottu selkeästi -Tutkimus vastaa esitettyyn tutkimusongelmaan -Tulokset ovat esitelty selkeästi -Tulosten merkitystä on arvioitu -Tutkimuksen konteksti on arvioitu -Aikaisempaa tutkimusta ei ole esitelty -Aineiston muodostumista ei esitelty -Tutkimusjoukkoa ei ole esitelty -Tutkimusetiikkaa ei ole arvioitu -Aineiston laadukkuutta ei ole arvioitu -Tuloksia ei vertailtu aikaisempiin tutkimuksiin -Tutkimuksen luotettavuutta ei ole arvioitu	5/13
Knapp, K. J., Morris Jr, R. F., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. *computers & security*, *28*(7), 493-508.	-Aikaisempaa tutkimusta on esitelty -Tutkimuksen tarkoitus on kerrottu selkeästi -Aineiston muodostuminen on selostettu -Tutkimusjoukko on esitelty -Tutkimusetiikkaa on arvioitu -Tutkimus vastaa esitettyyn tutkimusongelmaan -Aineisto on riittävän laadukasta -Tutkimustulokset ovat yleistettävissä -Tulokset ovat esitelty selkeästi -Tulosten merkitystä on arvioitu -Tutkimuksen konteksti on esitelty -Tutkimuksen luotettavuus on arvioitu -Tulosten merkitystä on arvioitu -Tutkimuksen konteksti on arvioitu -Tutkimuksen luotettavuutta on arvioitu	13/13
Palmer, M. E., Robinson, C., Patilla, J. C., & Moser, E. P. (2001). Information security policy framework: best practices for security policy in the e-commerce age. *Information Systems Security*, *10*(2), 1-15.	-Aikaisempaa tutkimusta on esitelty -Tutkimuksen tarkoitus on kerrottu selkeästi -Tutkimustulokset ovat hyvin yleistettävissä -Tulokset ovat esitelty selkeästi -Tulosten merkitystä on arvioitu -Tutkimuksen konteksti on arvioitu -Aineiston muodostumista ei esitelty -Tutkimusjoukkoa ole ei esitelty -Tutkimusetiikkaa ei ole arvioitu	6/13

	-Tutkimus ei vastaa esitettyyn tutkimusongelmaan selkeästi -Aineiston laadukkuutta ei ole arvioitu -Tuloksia ei vertailtu aikaisempiin tutkimuksiin -Tutkimuksen luotettavuutta ei ole arvioitu	
Ruighaver, A. B., Maynard, S. B., & Warren, M. (2010). Ethical decision making: Improving the quality of acceptable use policies. *Computers & Security*, *29*(7), 731-736.	-Aikaisempaa tutkimusta on esitelty -Tutkimuksen tarkoitus on kerrottu selkeästi -Aineiston muodostuminen on selostettu -Tutkimus vastaa esitettyyn tutkimusongelmaan -Aineisto on riittävän laadukasta -Tutkimustulokset ovat yleistettävissä -Tulokset ovat esitelty selkeästi -Tulosten merkitystä on arvioitu -Tutkimuksen konteksti on esitelty -Tutkimusjoukkoa ei ole esitelty -Tutkimusetiikkaa ei ole arvioitu -Tuloksia ei ole vertailtu aikaisempiin tutkimuksiin -Tutkimuksen luotettavuutta ei ole arvioitu	9/13
Walton, J. P. (2002, November). Developing an enterprise information security policy. In *Proceedings of the 30th annual ACM SIGUCCS conference on User services* (pp. 153-156). ACM.	-Tutkimuksen tarkoitus on kerrottu selkeästi -Aineiston muodostuminen on selostettu -Tutkimuksen konteksti on esitelty -Aikaisempaa tutkimusta ei ole esitelty -Tutkimusjoukkoa ei ole esitelty -Tutkimusetiikkaa ei ole arvioitu -Tutkimus ei vastaa esitettyyn tutkimusongelmaan selkeästi -Aineiston laadukkuutta ei ole arvioitu -Tutkimustulosten yleistettävyyttä ei ole arvioitu -Tuloksia ei ole selkeästi esitelty -Tuloksia ei ole vertailtu aikaisempiin tutkimuksiin -Tulosten merkitystä ei ole arvioitu -Tutkimuksen luotettavuutta ei ole arvioitu	3/13

LIITE 4 AINEISTOON VALIKOITUNEIDEN TUTKIMUSTEN TEEMAT JA KESKEISET LÖYDÖKSET

Tutkimuksen tiedot	Tutkimuksen tarkoitus	Keskeisimmät löydökset	Pisteytys
Corpuz, M., & Barnes, P. H. (2010). Integrating information security policy management with corporate risk management for strategic alignment. In Proceedings of the 14th World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2010).	Tutkimus esittää lähestymistavan, jossa perinteistä yrityksen riskienhallintaviitekehystä käytetään yrityksen tietoturvapolitiikan luomiseen ja hallinnointiin. Tällöin kehitys ja hallinnointi olisivat linjassa yrityksen riskienhallintapolitiikan kanssa.	ISP-CRP -tapa, eli yrityksen riskienhallintasuunnitelman viitekehyksellä luodaan tietoturvapolitiikka käyttäen samoja askelmerkkejä kuin riskienhallintapolitiikan luomisessa. Tällöin tietoturvapolitiikkaa ei pelkästään sysätä IT-osaston luotavaksi, vaan mukana luomisessa on myös riskienhallinnasta vastaava taho. Pääkohdat luomiselle ovat: 1. Ympäristön riskien havainnointi 2. Turvallisuusriskianalyysi 3. Turvallisuusriskiarviointi	10/13
Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *computers & security*, *61*, 169-183.	Tutkimuksen tarkoituksena on luoda viitekehys (sisältäen Tietoturvapolitiikan kehityksen elinkaaren), joka varmistaisi varteenotettavan strukturoidun metodologian tietoturvapolitiikan tehokkaalle luomiselle ja käyttöönotolle.	Tietoturvapolitiikan kehityksen elinkaaren kohdista kaikkein tärkeimmäksi nousi riskiarviointi. Täten toimivan tietoturvapolitiikan luomisen tähden on tärkeää lähteä rakentamaan politiikkaa riskiarvioinnin pohjalta. Tällöin organisaatio tunnistaa mahdolliset uhat ja haavoittuvuudet, jotka tulee minimoida.	13/16
Grobler, T., & Von Solms, S. (2004). Assessing the policy dimension. Johannesburg, South Africa: Technikon Witwatersrand.	Tutkimuksen tarkoituksena on luoda arviointijärjestelmä tietoturvapolitiikan valmiudelle ja tarpeiden kartoittamiselle.	Tietoturvapolitiikka luodaan noudattamaan ISO17799-standardia. Politiikka luodaan arvioimalla olemassa olevaa politiikkaa tai nykytilaa, ja tarkastelemalla organisaation tarpeita eri osa-alueilla tietoturvan näkökulmasta. Tällöin samalla arvioidaan myös politiikan riittävyyttä ja kattavuutta.	7/13
Hong, K. S., Chi, Y. P., Chao, L. R., & Tang, J. H. (2006). An empirical study of information security policy on information security elevation in Taiwan. *Information Management & Computer Security*, *14*(2), 104-115.	Tutkimuksen tarkoituksena on kartoittaa pääsyitä, joiden takia organisaatio luo tietoturvapolitiikan hyväksikäyttäen ISO/IEC 17799, 2000.	Tietoturvapolitiikan tulee olla suunniteltu tukemaan organisaation keskeisiä tehtäviä ja arvoja. Täten nämä tehtävät ja arvot tulee olla kartoitettuna, jotta tietoturvapolitiikka voidaan luoda. Tämän jälkeen politiikka luodaan hyväksikäyttäen ISO/IEC 17799, 2000	12/16
Jegede, A. J., Aimufua, G. I. O., & Salami, H. O. (2007). Information Security Policy: Relevance, Creation and Enforcement. International Journal of Soft Computing, 2(3), 408-410.	Tutkimuksen tarkoituksena on esitellä, että organisaation tietoturvapolitiikka tulee vain tarkasti muokata jo valmiista tietoturvapolitiikoista itselleen sopiva yhdistelemällä niitä sekä sovittamalla ne omalle organisaatiolle ja ympäristölle sopivaksi.	Organisaation prosessit, toimintatavat ja ympäristö tulee olla tarkasteltuna ja analysoituna, jotta tietoturvapolitiikka voidaan kirjoittaa jo olemassa olevien ja tunnistettujen tietoturvapolitiikoiden pohjalta. Politiikan tulee tasapainoilla oikeuksien ja vastuiden välillä, ja sen tulee myös määrittää yksinkertaisesti se, mikä on sallittua ja mikä ei.	5/13
Jirasek, V. (2012). Practical application of information security models. Information security technical report, 17(1-2), 1-8.	Tutkimuksen tarkoituksena on esitellä tietoturvallisuuden GRC -malli ja sen toiminta.	Tietoturvapolitiikka ymmärretään osana GRC-mallia, jolloin ympäröivä maailma (lait ja säädökset, liiketoiminnan tavoitteet ja tietoturvauhat) otetaan huomattavasti enemmän huomioon, kuin pelkästään keskittymällä yksittäisiin riskeihin tai	7/13

		tietoturvauhkiin sekä liiketoiminnan tarpeisiin.	
Kadam, A. W. (2007). Information security policy development and implementation. *Information Systems Security*, *16*(5), 246-256.	Tutkimus esittelee lähestymistavan, jolla tietoturvapolitiikan luomisessa kyetään huomioonottamaan liiketoiminnan tarpeet mahdollisimman hyvin. Kohdistuvien vaikutusten analyysi.	Kuusi kysymystä (what, why, how, who, where, ja when), joiden pohjalta luodaan kohdistuvien vaikutusten analyysi (engl. BIA, Business Impact Analysis) liiketoimintaprosesseille niin uhkien kuin haavoittuvuuksien näkökulmasta, jonka pohjalta luodaan tietoturvapolitiikka.	5/13
Knapp, K. J., Morris Jr, R. F., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. computers & security, 28(7), 493-508.	Tutkimuksen tarkoitus on kehittää ja esitellä organisaatiomalli kuvaamaan kattavaa tietoturvapolitiikkaprosessia.	Tietoturvapolitiikka tulisi luoda avainprosessien sekä sisäisten (esim. parhaat käytännöt ja ulkoisten vaikutusten (esim. toimialakohtainen säätely) huomioonottamisen avulla.	13/13
Ruighaver, A. B., Maynard, S. B., & Warren, M. (2010). Ethical decision making: Improving the quality of acceptable use policies. Computers & Security, 29(7), 731-736.	Tutkimuksen tarkoituksena on kartoittaa käytännön sovellutus tietoturvapolitiikan käytön ja omaksunnan parantamiseksi etiikan avulla.	Tietoturvapolitiikka tulee kirjoittaa tekojen seurausten eettisyyttä tarkastelemalla, jossa tietoturvapolitiikan kirjoittajien tulee teknisten lähtökohtien sijasta asettua tavallisen työntekijän saappaisiin.	9/13
Palmer, M. E., Robinson, C., Patilla, J. C., & Moser, E. P. (2001). Information security policy framework: best practices for security policy in the e-commerce age. *Information Systems Security*, *10*(2), 1-15.	Tutkimus esittelee yksityiskohtaisen tietoturvapolitiikkaviitekehyksen. Nykytilanalyysin (GAP) hyväksikäyttö.	Tietoturvapolitiikka tulisi luoda käyttäen hyväksi tietoturvapolitiikan nykytilanalyysia (GAP), jolloin mahdolliset ongelmakohdat ja puutteet nykyisessä tietoturvapolitiikkaviitekehyksessä huomataan ja voidaan korjata.	6/13
Walton, J. P. (2002, November). Developing an enterprise information security policy. In Proceedings of the 30th annual ACM SIGUCCS conference on User services (pp. 153-156). ACM.	Tutkimuksen tarkoituksena on esitellä tietoturvapolitiikan kirjoittamisen apuna tarvittavia prosesseja, joilla tunnistetaan tietoturvaongelmia sekä sisällytetään parhaita käytänteitä sisältävä tietoturvasuunnitelma.	Tietoturvapolitiikka on luotava yhteistyössä sen organisaation eri jäsenten kanssa, jotka tulevat käyttämään tietoturvapolitiikkaa ja valvomaan sen käyttöä. Tietoturvapolitiikan luomisen apuna toimii 18-kohtaisen lista.	3/13