Tiia Maria Tammela

HENKILÖSTÖN TIETOTURVAKÄYTTÄYTYMINEN YRITYSKONTEKSTISSA

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2016

TIIVISTELMÄ

Tammela, Tiia Maria
Henkilöstön tietoturvakäyttäytyminen yrityskontekstissa
Jyväskylä: Jyväskylän yliopisto, 2016, 31 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja(t): Moilanen, Panu

Tämä tutkielma on toteutettu kirjallisuuskatsauksena, jonka lähteinä on käytetty pääasiassa akateemisten julkaisujen artikkeleita. Tutkielman tarkoitus oli selvittää mitä on tietoturvakäyttäytyminen, tekijät jotka vaikuttavat henkilöstön tietoturvakäyttäytymiseen ja miten henkilöstön käyttäytymistä voitaisiin parantaa, tietoturvan säilyttämiseksi. Kirjallisuuden perusteella onnistuttiin löytämään kattava lista erilaisia käyttäytymisen vaikuttavia tekijöitä ja henkilöstön motivoinnin keinoja. Näistä tekijöistä ja keinoista muodostettiin kontribuutiona havainnollistava kuva, sekä konkreettinen tehtävälista.

Asiasanat: tietoturva, tietoturvapolitiikka, henkilöstö, käyttäytyminen, motivaatio

ABSTRACT

Tammela, Tiia Maria
Information security behavior of the personnel in business context
Jyväskylä: University of Jyväskylä, 2016, 31 s.
Information systems science, bachelors degree
Ohjaaja(t): Moilanen, Panu

This thesis is a literature review based mainly on academic publications. Meaning of this study was to figure out what is information security behavior, factors that affect the information security behavior of the personnel and how could that behavior be improved for maintaining information security. A number of factors affecting security behavior and also several ways of motivating personnel were found based on the literature. As contribution for this study an explanatory picture and a concrete task list were formed, based on the results.

Keywords: information security, information security policy, personnel, behavior, motivation

KUVIOT

SISÄLLYS

1 JOHDANTO

Tässä johdantoluvussa pyritään kuvaamaan tarkasti tutkielman aihe ja tutkielman merkitys yrityksille. Lisäksi esitellään käytetyt tutkimusmenetelmät ja tutkimuksen tavoitteet. Johdannossa esitellään myös saavutetut tulokset ja niiden merkitys, sekä lyhyesti tutkielman rakenne.

Tämä tutkimus on tarpeellinen, koska henkilöstö muodostaa merkittävän tietoturvariskin yrityksille (Hu, Dinev, Hart & Cooke, 2012; Bulgurcu, Cavusoglu & Benbasat, 2010). Tämä on laajalti tunnustettu tosiasia ja tutkielman tarkoitus onkin koota aiemmasta kirjallisuudesta kirjallisuuskatsauksen menetelmin kattava kuva tutkimuskentästä ja niistä keinoista, joita aiempi tutkimus on löytänyt henkilöstön tietoturvakäyttäytymisen motivoimiseksi. Henkilöstön käyttäytymiseen vaikuttamista lähdettiin tutkimaan selvittämällä ensin mitä on tietoturvakäyttäytyminen ja sen jälkeen niitä tekijöitä, joilla on vaikutus yksilön sisäiseen tai ulkoiseen motivaatioon tietoturvakäyttäytymistä kohtaan. Seuraavaksi selvitettiin miten näitä tekijöitä voidaan käyttää työntekijän motivoimiseksi haluttuun käyttäytymiseen. Tässä tutkielmassa pyrittiin siis selvittämään vastaus kolmeen tutkimuskysymykseen:

- Mitä on tietoturvakäyttäytyminen?
- Mitkä tekijät vaikuttavat henkilöstön tietoturvakäyttäytymiseen?
- Millaisilla keinoilla henkilöstön tietoturvakäyttäytymistä voitaisi parantaa?

Tutkielmassa onnistuttiin vastaamaan tutkimuskysymyksiin ja löydettiin sekä henkilöstön turvallisuuskäyttäytymiseen vaikuttavia tekijöitä, että henkilöstöä parempaan tietoturvakäyttäytymiseen motivoivia keinoja. Henkilöstön tietoturvakäyttäytymiseen vaikuttaa muun muassa halu noudattaa määräyksiä ja tietoisuus tietoturvasta, myös esimerkiksi teknisellä osaamisella, palkinnoilla ja rangaistuksilla huomattiin olevan vaikutusta. Tietoturvakäyttäytymisen parantamista voi lähestyä esimerkiksi lisäämällä työntekijöiden tietoisuutta, laatimal-

la hyvän tietoturvapolitiikan tai varmistamalla johdon sitoutumisen politiikkojen noudattamiseen. Kaikkia näitä ja muutamia muita tekijöitä käsitellään tarkemmin tulevissa luvuissa. Tutkielma tarjoaa kaiken kaikkiaan hyvän katsauksen akateemiseen kirjallisuuteen, joka on tutkinut henkilöstön tietoturvakäyttäytymistä yrityskontekstissa.

Tutkielma toteutettiin kirjallisuuskatsauksena, joten lähteiden valintaprosessilla on suuri merkitys tutkimuksen luotettavuudelle. Seuraavaksi kuvataan lähteidenhakuprosessia sellaisella tarkkuudella, että lukija pystyy hahmottamaan mistä ja miten tutkielman materiaali on kerätty.

Tutkielman lähdemateriaalina käytettyjä artikkeleita arvioitiin kirjoitusprosessin aikana muun muassa julkaisun tunnettuuden ja luotettavuuden perusteella, aiempien viittausten määrän ja lähteiden laadun mukaan sekä kirjoittajan, tai kirjoittajien, ja kirjoitusajankohdan mukaan. Hyvinä lähteinä pidettiin erityisesti julkaisufoorumilla korkean luokituksen saaneissa julkaisuissa julkaistuja, tunnettujen tutkijoiden kirjoittamia ja suhteellisen tuoreita julkaisuja. Lisäksi tärkeä tekijä luotettavuuden arvioinnissa oli aiempien viittauksien määrä. Tutkielman aiheen rajauksen mukaan lähdemateriaali valittiin sellaiseksi, että se käsitteli työntekijöiden käytöstä erityisesti yrityskontekstissa, eikä esimerkiksi kotikäyttäjiä. Näin toimimalla haluttiin varmistaa lähteiden vertailtavuus keskenään.

Lähteiden etsimiseen tietokannoista käytettiin muun muassa seuraavia hakusanoja: employee, security behavior, information security, IT security, personnel, motivation, policy ja myös näiden ja muiden hakusanojen yhdistelmiä. Lisäksi lähteitä etsittiin jo luotettaviksi havaittujen lähteiden lähdeluetteloista ja hyväksi käytettiin myös joidenkin tietokantojen, esimerkiksi Emerald Insight- ja ScienseDirect-tietokantojen suosittelutoimintoja. Kyseinen toiminto suosittelee artikkelin avaajalle vastaavaan aiheeseen liittyviä muita artikkeleita.

Tutkielman toinen luku käsittelee tietoturvan käsitettä ja henkilöstöä yrityksen tietoturvan osatekijänä. Luvun tarkoitus on määritellä olennaiset käsitteet tietoturva, tietoturvakäyttäytyminen ja tietoturvapolitiikka, sekä tarjota perusteluja tutkimusaiheen tärkeydelle. Kolmannessa luvussa käsitellään ensimmäistä tutkimuskysymystä, eli henkilöstön tietoturvakäyttäytymiseen vaikuttavia keinoja. Neljännessä luvussa vastataan toiseen tutkimuskysymykseen ja eritellään niitä tapoja, joilla voidaan ohjata henkilöstöä parempaan tietoturvakäyttäytymiseen. Tutkielman viimeisessä luvussa kerätään yhteen tutkimuksen tulokset ja havainnollistetaan niitä kuvan ja konkreettisen tehtävälistan avulla. Lisäksi pohditaan tutkimuksen rajoitteita ja esitetään jatkotutkimusehdotuksia.

2 YRITYKSEN TIETOTURVA JA HENKILÖSTÖ

Tässä luvussa käsitellään tutkielman kannalta olennaisia käsitteitä, sekä pyritään tarjoamaan niille määritelmiä. Löydetyt määritelmät antavat puitteet käsitteiden käytölle ja tutkielman johtopäätöksille, samoin kuin mahdollisille tutkimuskysymyksiin löydetyille vastauksille. Kaikki käsitteet pyritään määrittelemään nimenomaan koskien yrityskontekstia ja yrityksen tietoturvaa, jotta määritelmät olisivat mahdollisimman osuvia, huomioon ottaen käsitteiden käyttötarkoituksen tutkielmassa. Lisäksi tässä luvussa pohditaan henkilöstöä yrityksen tietoturvan tekijänä ja henkilöstön käyttäytymisen mahdollisia seuraamuksia yrityksille.

Yritykset ovat tyypillisesti huolestuneita ulkoisista uhista yrityksen tietoturvalle, vaikka todellisuudessa huomattava osa vahingoista aiheutuu organisaation sisäisistä toimista (Stanton, Stam, Mastrangelo & Jolton, 2005). Arviot sisäisen toiminnan aiheuttamista tietoturvariskeistä vaihtelevat lähteittäin, mutta yhdistävää kaikille näille arvioille on se, että ne pitävät sisäistä toimintaa on huomattavana tietoturvariskinä. Esimerkiksi Ernest ja Young LPP (2002) tekemän arvion mukaan yli kolme neljäsosaa tietomurroista olisi seurausta sisäisestä toiminnasta. Gordon, Loeb, Lucyshyn ja Richardson (2004) puolestaan ovat arvioineet noin puolien yritysten tietoturvavahingoista aiheutuvan sisäisestä toiminnasta. Totuus löytyy varmastikin jostain näiden arvioiden väliltä. Arviot ovat kuitenkin merkittävän suuria, eikä niitä pitäisi ohittaa reagoimatta. Nämä tekijät huomioon ottaen on tarpeellista tutkia henkilöstön tietoturvakäyttäytymistä yrityskontekstissa ja selvittää paremman toiminnan edellytyksiä. Luotettava tietoturvahan on yrityksille elintärkeä ominaisuus, ei pelkästään tuotekehittelyn ja varsinaisen tuotannon toimivuuden kannalta, vaan myös brändin, markkina-arvon sekä asiakkaiden luottamuksen takia.

2.1 Tietoturva ja tietoturvapolitiikka käsitteinä

Tietoturva on laajalti käytetty käsite, josta kuulee mitä erilaisimmissa yhteyksissä, mediasta tieteellisiin artikkeleihin. Aihe puhuttaa paljon ja on ollut pinnalla jo useita vuosia, eikä yritysten mielenkiinto aihetta kohtaan osoita hiipumisen merkkejä. Se on luonnollista, sillä esimerkiksi tietoturvahyökkäysten riski näyttää kasvavan jatkuvasti (Liginlal, Sim & Khansa, 2009; Boss, Kirsch, Angermeier, Shingler & Boss, 2009). Näin ollen on loogista aloittaa tutkielman aiheen lähestyminen määrittelemällä tämä keskeinen käsite, tietoturva. Kirjallisuudesta on löydettävissä muun muassa seuraavia määritelmiä:

> Asiantunteva varmuuden tunne siitä, että tietoturvariskit ja niiden hallinta ovat tasapainossa keskenään (Anderson, 310, 2003).

> Tietoturva, tietovarantojen luottamuksellisuuden, eheyden ja saatavuuden suojaamiseksi niin säilytyksen, käytön kuin siirronkin aikana. Se voidaan saavuttaa politiikkojen, koulutuksen, harjoittelun, tietoisuuden ja teknologioiden soveltamisen ja parantamisen kautta. (Whitman & Mattord, 8–9, 2012.)

> Tietojärjestelmien suojaamista luvatonta käsiksi pääsemistä tai muokkaamista vastaan, niin säilytyksen, käytön kuin siirtämisenkin aikana, mukaan lukien tarvittavat toimet uhkien havaitsemiseksi, dokumentoimiseksi ja niihin vastaamiseksi. Sekä vastatoimia palvelujen estämiselle luvallisilta käyttäjiltä. (NSTISSC, 30, 2000.)

Tietoturva tarkoittaa siis niitä tekoja ja käytäntöjä joiden tehtävänä on suojata informaatiota joutumasta vääriin käsiin. Sen tarkoitus on luoda suojaa yritykselle, tuotteille, asiakkaille ja muille sidosryhmille. Yrityksien tietoturva liittyy tiedon ja sen käyttöoikeuksien hallitsemiseen, sekä tietojen käytön seurantaan. Samoin voidaan katsoa tietoturvan käsitteen piiriin kuuluvaksi mahdollisten uhkien määrittely ja niihin varautuminen.

Yrityskontekstissa tietoturvan käsitteeseen, ja erityisesti sen soveltamiseen käytännössä, liittyy saumattomasti tietoturvapolitiikan käsite. Höne ja Eloff (2002) määrittelevät artikkelissaan tietoturvapolitiikan tärkeimmäksi yksittäiseksi tekijäksi, jolla kontrolloidaan ja mitataan yrityksen tietoturvaa. Artikkelissa yrityksen tietoturvapolitiikka kuvataan ohjeistavaksi dokumentiksi, joka osoittaa johdon antamaa tukea ja sitoutumista tietoturvaa kohtaan, samoin kuin tietoturvan merkityksen organisaation vision ja tavoitteiden saavuttamisessa. Artikkeli huomauttaa myös, että tietoturvakäytänteet suunnataan laajalle yleisölle, joista osalle tietoturva voi olla vieras käsite. Tästä syystä tietoturvapolitiikan olisi hyvä sisältää myös tietoturvan määritelmä ymmärrettävässä muodossa.

Tietoturvapolitiikkaa voidaan siis pitää tietoturvaan liittyvän toimimisen, ja päätöksenteon ohjeena ja välineenä, niin johto- kuin toimihenkilötasollakin. Yritykset pyrkivät määritellyn tietoturvapolitiikan avulla selittämään tietoturvan merkityksen kaikille yrityksen tietoihin käsiksi pääseville työntekijöille (Höne & Eloff, 2002). Näin pyritään varmistamaan, että jokainen yrityksen tietojen kanssa tekemisissä oleva osaa käyttäytyä toivotulla tavalla, eikä altista yri-

tystä tietovuodoille tai muille epämieluisille sattumuksille. Voidaan myös todeta, että tietoturvapolitiikka kertoo mitä on sallittua tehdä ja mitä ei (Bishop, 2003) ja lisäksi siinä usein määritellään myös mahdollisten rikkeiden seuraukset (Guo, Yuan, Archer & Connelly, 2011).

2.2 Henkilöstö yrityksen tietoturvan tekijänä

Henkilöstöä pidetään merkittävimpänä yksittäisenä riskitekijänä yrityksen tietoturvan kannalta (Hu, Dinev, Hart & Cooke, 2012), mutta samalla se voi olla valttikortti tietoturvan parantamisessa (Bulgurcu, Cavusoglu & Benbasat, 2010). Aikaisempi tietoturvatutkimus on kuitenkin rajautunut voimakkaasti tietoturvan teknisiin tekijöihin, kuten palomuureihin ja viruksentorjuntaohjelmistoihin (Crossler, Johnston, Lowry, Hu, Warkentin & Baskerville, 2013; Herath & Rao, 2009). Nykyään tietoturvan inhimillistä tekijää pidetään merkittävänä tutkimushaarana teknologian ja prosessien ohella ja työntekijöiden käyttäytymisen tutkimista on lisätty (Herath & Rao, 2009). Esimerkiksi Siponen (2000) nosti artikkelissaan esiin motivoinnin merkityksen henkilöstön tietoturvakäyttäytymisen perustana jo vuonna 2000.

Kehittyvät teknologiat ja käytännöt kuten asioiden internet (eng. IoT) ja omien laitteiden käyttö työympäristössä (eng. byod) luovat muuttuvia riskejä ja tutkimuskohteita siihen, kuinka henkilöstön toiminta vaikuttaa yrityksen tietoturvaan. Esimerkiksi on todettu, että kaikki ohjelmistopohjaiset laitteet voidaan manipuloida tekemään asioita, joita niiden luojat eivät ole suunnitelleet. Lisäksi kaikki jollain tavalla verkkoon kytketyt laitteet ovat ulkoisen osapuolen vaarannettavissa. (Fenz, Heurix, Neubauer & Pechstein, 2014.) Tämä tarkoittaa asioiden internetin yleistyessä yhä suurempaa osaa kaikista laitteista, esimerkiksi sitä ”kuuluisaa” salakuuntelevaa jääkaappia (Osisanwo, Shade & Awodele, 2015). Nämä esimerkit liittyvät henkilöstöön yrityksen tietoturvan tekijänä muun muassa siten, että henkilöstöltä vaaditaan aiempaa korkeampaa tieto- ja taitotasoa, kuten myös kiinnostusta, jotta kyetään hallitsemaan uusien teknologioiden aiheuttamia riskejä.

Henkilöstön huolimattoman tai pahantahtoisen käyttäytymisen tiedetään aiheuttaneen monia ongelmia ja vahinkoja paitsi yrityksille, myös asiakkaille. Yksi tapa kategorisoida aiheutuneita vahinkoja on jakaa ne todellisiin menetyksiin, esimerkiksi kadotettu data, laitevauriot jne., niihin menetyksiin jotka aiheutuvat markkina-arvon laskusta luottamuksen katoamisen seurauksena ja asiakkaille koituneisiin menetyksiin. (Liginlal, Sim & Khansa, 2009.) Tuore tutkimus osoittaa, että tietomurron keskimääräinen ”hinta” yritykselle vaihtelee huomattavasti maittain, ja se on Yhdysvaltojen dollareissa ilmaistuna esimerkiksi:

- Yhdysvalloissa 6,5 milj.
- Saksassa 4,9 milj.

- Brasiliassa 1,8 milj.
- Intiassa 1,5 milj. (Ponemon Institute, 2015).

Huolimatta keskimääräisen hinnan vaihtelusta maittain on selvää, että yksittäiselle yritykselle se on liian korkea maksettavaksi.

Työntekijöiden huolimattomuudesta tai pahantahtoisuudesta aiheutuvat kustannukset voivatkin olla yrityksille kohtalokkaita. Esimerkiksi tapaustutkimus vuodelta 2001, koskien Barings-pankkia ja Nicholas Leesonin tietoturvarikkeitä luotetun työntekijän asemassa, kuvaa kuinka Leeson käytti hyväkseen yrityksen huonosti suunniteltuja tietoturvajärjestelmiä ja aiheutti lopulta yrityksen joutumisen oikeuteen ja konkurssiin. Keskeinen ongelma pankin järjestelmissä oli kunnollisen valvonnan puute, joka salli Leesonin salata tekemänsä satojen miljoonien puntien tappiot, luomansa tilin ja heikosti suunniteltujen kirjanpitojärjestelmien avulla. (Dhillon, 2001.)

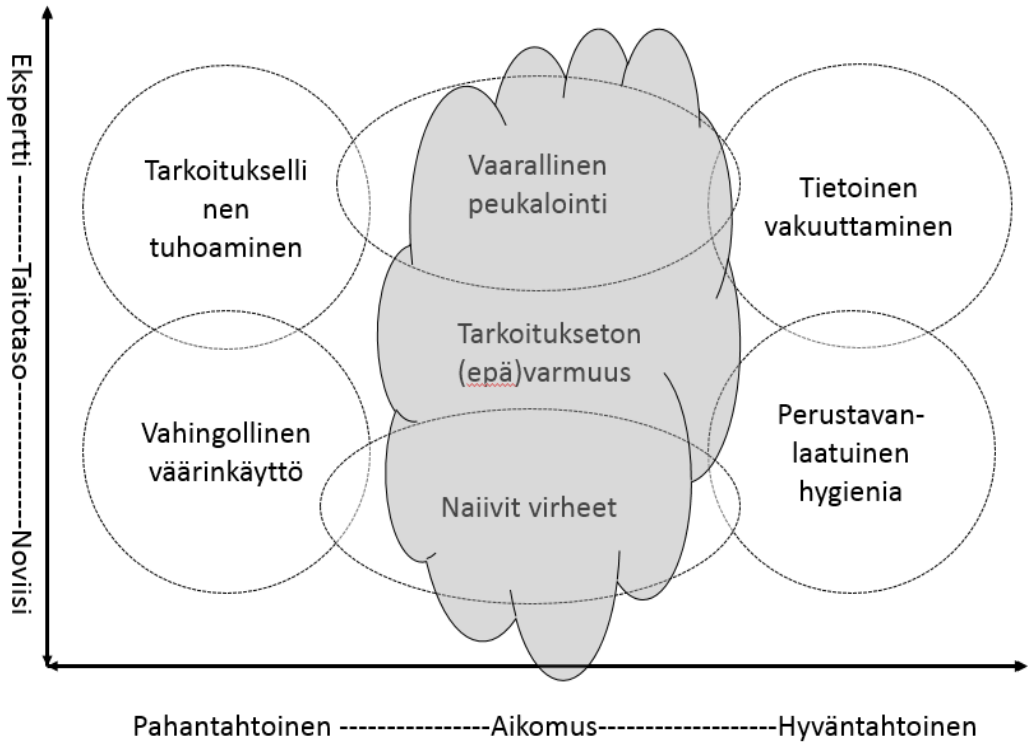
Edellä mainitun kaltaisten tapahtumien välttämiseksi on olennaisen tärkeää tuntea henkilöstön käyttäytymistä ajavat tekijät ja pohtia keinoja tietoturvaa parantavan käyttäytymisen kannustamiseksi. Todellisuutta kuitenkin on, että tietoturvateknologioita ja käytänteitä voidaan käyttää tai tulkita väärin, tai jättää jopa kokonaan käyttämättä, jolloin niistä ei ole todellisuudessa mitään hyötyä (Siponen, 2000).

2.3 Henkilöstön tietoturvakäyttäytyminen

Henkilöstön suoria tai epäsuoria uhkia yritykselle aiheuttava tietoturvakäyttäytyminen voidaan jakaa kahteen kategoriaan sen mukaan, onko toiminta tarkoituksellista vai tahatonta. Tarkoituksellisena käytöksenä voidaan pitää muun muassa varkauksia, sabotaasia ja vakoilua. (Crossler ym., 2013.) Tahattomia tietoturvan vaarantavia toimia sen sijaan ovat esimerkiksi liian yksinkertaisen salasanan valitseminen, muilla kuin työhön liittyvillä verkkosivuilla vierailut tai tuntemattomien sähköpostien ja niiden liitteiden huolimaton availu. Näiden kategorioiden erottelu olisi tärkeää, sillä tarkoituksellisten ja tarkoituksettomien toimien motiivit ja syyt ovat todennäköisesti hyvin erilaiset. (Crossler ym. 2013.) Toiminnan syiden eroista huolimatta molemmat käytösmallit voivat olla yhtä haitallisia yritykselle: tahallinen toiminta voi aiheuttaa suoria tuoton menetyksiä, kun taas erilaiset huolimattomuudet altistavat yrityksen epäsuorasti hyökkäyksille (Crossler ym. 2013). Tässä tutkielmassa tahallisia ja tahattomia rikkeitä ei ole näkyvästi eroteltu tutkielman suppeuden takia ja siitä syystä, että myöskään kaikki kirjallisuuskatsauksen lähdemateriaali ei ole tuota eroa maininnut. Eroista mainitaan kuitenkin muutaman kerran, kun se lähteen referoinnin kannalta on relevanttia.

Toisen näkökulman käyttäjien turvallisuuskäyttäytymiseen tarjoaa Stantonin, Stamin, Mastrangelon ja Joltonin (2005) artikkeli, jossa erotellaan kuusi käyttäytymismallia. Nämä mallit on esitetty havainnollisesti kuviossa 1. Tutkijoiden löytämät ja testaamat kategoriat ovat suomennettuina: tahallinen

tuhoaminen, vahingollinen väärinkäyttö, vaarallinen peukalointi, naivit virheet, tietoinen vakuuttaminen sekä perustavanlaatuinen hygienia. Näistä kategorioista kaksi ensimmäistä kuvaa pahantahtoista käyttäytymistä, kaksi seuraavaa neutraalia käyttäytymistä ja kaksi viimeistä kuvaavat yritystä kohtaan hyödyllistä käyttäytymistä. Malli myös määrittelee tietoteknisen taitotason, joka vaaditaan näiden käyttäytymismallien toteuttamiseksi. Esimerkiksi tahallinen tuhoaminen, kuten murtautuminen suojattuihin tiedostoihin, vaatii korkeaa teknistä osaamista. Vastaavasti taas naiivit virheet kuten huonon salasanan valitseminen eivät vaadi erityisosaamista. (Stanton ym., 2005.)



KUVIO 1 Kahden tekijän luokittelu loppukäyttäjien tietoturvakäyttäytymisestä (Stanton ym., 127, 2005; suomennettu Tammela, 2016)

Edellä esitettyjen mallien perusteella voidaan päätellä, että muun muassa teknisellä osaamisella on vaikutusta työntekijän tietoturvakäyttäytymiseen. Muitakin henkilöstön tietoturvakäyttäytymiseen vaikuttavia tekijöitä on lukuisia. Tässä tutkielmassa niitä eritellään tarkemmin luvussa kolme. Henkilöstön tietoturvakäyttäytymisen parantamiseen tähtääviä toimia ja käytänteitä pyritään avaamaan luvussa neljä.

Tietoturvakäyttäytymistä on edellä esitetyn lähdemateriaalin perusteella kaikki sellainen toiminta, joka millään tavalla vaikuttaa yrityksen tietoturvaan. Tällainen vaikutus voi olla positiivinen, esimerkiksi tietoturva-aukon huomaaminen ja korjaaminen, tai negatiivinen kuten suojattujen tiedostojen murtaminen ja myyminen. Toiminta voi lisäksi olla tahatonta tai tahallista ja käyttäytymisen toteuttamiseen vaikuttavat henkilön motivaatio, tekninen osaaminen, tietoisuus ja monet muut tekijät, joita selvitetään seuraavassa luvussa.

3 HENKILÖSTÖN TIETOTURVAKÄYTTÄYTYMISEEN VAIKUTTAVAT TEKIJÄT

Tässä luvussa pyritään vastaamaan toiseen tutkimuskysymykseen, eli erittelemään niitä syitä, jotka vaikuttavat henkilöstön tietoturvakäyttäytymiseen. Luvussa eritellään siis sellaisia käytäntöjä ja motivaatiotekijöitä, jotka saattavat johtaa henkilöstön epätoivottavaan käyttäytymiseen. Erilaisia vaikuttimia on kerätty lukuisista artikkeleista ja ne on pyritty jaottelemaan sisäisesti motivoiviin tekijöihin ja ulkoisesti motivoiviin tekijöihin. Tämä jako perustuu psykologiassa paljon tutkittuun ulkoisen ja sisäisen motivaation teoriaan. Informaatioteknologian alalla teoriaa ovat soveltaneet esimerkiksi Herath ja Rao (2009).

Sana motivaatio tulee latinan kielen sanasta movere, joka tarkoittaa vapaasti suomennettuna syy liikkua tai liikuttaa (eng. to move) (Ryan & Deci, 2000). Motivaatio on siis tekijä joka liikuttaa ihmisiä. Samalla logiikalla voidaan ajatella sen olevan tekijä, joka saa henkilöstön toimimaan tietyllä tavalla, kuten tämän tutkielman tapauksessa hyvin tai huonosti tietoturvan suhteen.

Sisäisen motivaation ajamaa käyttäytymistä toteutetaan kiinnostuksesta ja siitä tyydytyksestä, jonka se tuo synnynnäiselle pätevyyden ja itsenäisyyden tarpeelle. Ulkoisen motivaation aiheuttaman käytöksen taas kuvataan johtuvan erillisistä seuraamuksista, joita teon toteuttamiseen tai toteuttamatta jättämiseen liittyy. (Ryan & Deci, 2000.) Motivaatiolla on lukuisia muitakin ulottuvuuksia, kuten motivaation taso ja suuntautuminen. Esimerkiksi opiskelija voi olla motivoitunut uuden taidon oppimisesta koska ymmärtää sen merkityksen ja arvon, tai vaihtoehtoisesti koska opiskelija haluaa hyvän arvosanan ja sen positiiviset seuraukset. (Ryan & Deci, 2000.) Näissä tapauksissa motivaation suuntautuminen eroaa toisistaan.

Tutkielman laajuuden puitteissa pyritään tarjoamaan perusteluja valituille jaotteluille, mutta absoluuttista jakoa sisäisen motivaation ajamaan käytökseen ja ulkoisesti motivoituun käytökseen lienee mahdotonta tehdä, sillä osa tekijöistä kuuluu selkeästi myös molempiin kategorioihin. Jako on pyritty tekemään edellä kuvatulla periaatteella, eli onko toiminnan tai taidon lähde henkilön sisäinen kiinnostus ja inspiraatio, vaiko ulkoinen pakote. Tätä pohditaan tarkemmin tutkielman viimeisessä luvussa, rajoitteet-osiossa.

Huomattavaa on myös se, että sisäisesti motivoivat tekijät näyttävät olevan voimakkaampia käyttäytymisen aiheuttajia, kuin ulkoisesti motivoivat tekijät (Son, 2011). Esimerkiksi rangaistukset ja palkinnot, sekä koulutuksen määrä kuuluvat ulkoisiin motivaatiotekijöihin, kun esimerkiksi tietoisuus tietoturvasta on selkeästi sisäinen tekijä. Näin ollen tutkielmassa on eroteltu havaitut vaikuttavien tekijöiden tasot toisistaan.

3.1 Sisäisesti motivoivat tekijät

Henkilöstön sisäinen motivaatio on merkittävässä roolissa tietoturvakäyttäytymisen kannalta (Herath & Rao, 2009). Sisäisiin henkilöstön tietoturvakäyttäytymiseen vaikuttaviin tekijöihin kuuluvat tutkitun materiaalin perusteella ainakin toiminnan koetut vaikutukset, henkilökohtainen osaaminen, halu noudattaa määräyksiä ja politiikkoja sekä tietoisuus määräyksistä ja politiikoista.

Esitellyt tekijät on valikoitu tähän kategoriaan sillä perusteella, että ne vaikuttavat työntekijän käyttäytymiseen niin sanotusti sisältä päin. Esimerkiksi henkilön halu noudattaa määräyksiä perustuu muun muassa siihen, kuinka tämä arvioi tekojensa seurauksia (Guo, Yuan, Archer & Connelly, 2011). Tällainen arvio voidaan ajatella muodostuvan jokaisen henkilökohtaisten kokemuksien perusteella. Vaikka tätä käsitystä voidaan oikaista esimerkiksi koulutuksella, joka on jaoteltu ulkoisiin tekijöihin, sen ollessa henkilöön ulkoapäin kohdistuva paine tehdä jotain tietyllä tavalla.

3.1.1 Toiminnan koetut seuraukset ja halu noudattaa määräyksiä

Henkilön kokemus toimintansa aiheuttamista seuraamuksista on merkittävä tekijä työntekijän tehdessä toimintapäätöstä, tällainen kokemus on esimerkiksi työntekijän havaitsema suhteellinen hyöty työsuoritukselleen, mikäli hän rikkoo tietoturvapolitiikkoja. (Herath & Rao, 2009). Nämä uskomukset rakentuvat politiikkojen noudattamisen hyödyistä ja hinnasta työntekijälle, sekä mahdollisen noudattamatta jättämisen hinnasta. Tietoisuus tietoturvapolitiikoista vaikuttaa positiivisesti sekä työntekijän asenteeseen, että siihen mitä tämä uskoo seuraavan tietyistä toimista. (Bulgurcu, Cavusoglu & Benbasat, 2010.) Tietoisuuden vaikutuksia käyttäytymiseen pohditaan tarkemmin seuraavassa alaluvussa.

Mikäli tietty teko auttaa henkilöä tekemään työnsä tehokkaammin, käyttäjä todennäköisesti tekee teon, vaikka se rikkoisi organisaation tietoturvapolitiikkaa. (Guo ym., 2011.) Tätä on selitetty esimerkiksi työssäsuoriutumisen näkökulmasta, jolloin hyvä suoriutuminen on tavoite, maali, johon pyritään kaikilla tarpeellisilla keinoilla (Guo ym., 2011).

Myös käyttäjän havaitsema tai kokema tietoturvariski on merkittävä tekijä toimintapäätöksen teossa. Mitä suuremman riskin työntekijä kokee toimintansa aiheuttavan, sitä epätodennäköisemmin hän etenee toiminnassaan. (Guo ym.,

2011.) Yritys voi pyrkiä vaikuttamaan työntekijöidensä käsityksiin esimerkiksi koulutuksella tai vaikkapa tietoturvariskeistä kertovilla julisteilla ja tietoiskuilla.

Työntekijän käyttäytymistä ohjaa myös hänen käsityksensä omasta identiteetistään työntekijänä. Mikäli hyvä tietoturvakäyttäytyminen ja politiikkojen noudattaminen kuuluu henkilön käsitykseen ammattimaisesta työntekijästä, noudattaa hän todennäköisemmin tietoturvamääräyksiä. (Guo ym., 2011.)

Käyttäjän halukkuus noudattaa hyväksyttyjä käytäntöjä vaikuttaa luonnollisesti hänen käyttäytymiseensä. Halukkuuteen vaikuttavat käyttäjän henkilökohtaiset arvot ja toiminnan standardit, käyttäjän psykologinen sitoutuneisuus työnantajaansa sekä tietoturvapolitiikan noudattamisen vaatiman vaivan ja noudattamatta jättämisen tuoman houkutuksen välinen suhde. (Leach, 2003.)

Kaikissa yllä mainituissa artikkeleissa on nähtävissä, että mikäli tietoturvapolitiikan noudattaminen haittaa tai häiritsee henkilön työskentelyä merkittävästi, ovat rikkeet todennäköisiä. Tätä puoltaa myös toteamus siitä, että työntekijöille pitäisi varata aikaa tietoturvavaatimusten noudattamiselle, jotta tietoturvapolitiikkojenmukainen toiminta ei kilpailisi varsinaisen työsuorituksen kanssa (Bulgurcu, Cavusoglu & Benbasat, 2010). Artikkeleista huomataan myös henkilön omakuvan ja arvojen vaikutus. Mikäli työntekijän arvot ovat yhtenevät yrityksen arvojen kanssa, on tietoturvapolitiikan noudattaminen todennäköisempää. Lisäksi nähdään, kuinka suuri merkitys tottelevaisuuteen on sillä, mitä työntekijä uskoo tapahtuvan tiettyjen toimien seurauksena. Näihin uskomuksiin vaikuttaa työntekijän tietoisuus tietoturvapolitiikoista, jota pohditaan seuraavaksi.

3.1.2 Tietoisuus tietoturvallisuudesta

Tietoisuus tietoturvasta tarkoittaa yksinkertaisesti sitä, että tietää jotain tietoturvallisuudesta. Tietoisuus voi syntyä elämänkokemusten perusteella tai se voi olla saavutettu ulkoisten lähteiden kuten artikkeleiden ja koulutusten avulla. (Bulgurcu, Cavusoglu & Benbasat, 2010). Tietoisuus tietoturvakäytännöistä ja ohjeista on merkittävä tekijä tietoturvan säilyttämisen kannalta. Kuitenkaan tyypillinen tapa esittää käytäntöjä vain faktoina ja fraasinomaisesti ei ole välttämättä hyvä, tai toimiva tapa saada työntekijät omistautumaan asialle. (Siponen, 2000.)

Sisäiseen motivaatioon, tietoisuuteen ja asenteeseen vaikuttavia tekijöitä ovat esimerkiksi toiminnan loogisuus ja ohjeiden järkiperäisyys, turvallisuuskäytäntöjen tunteisiin vetoavuus ja niiden pohjautuminen yleiseen moraaliin ja etiikkaan, tietoisuus siitä miten turvallisuuspolitiikat edesauttavat yksilön hyvinvointia ja niiden tuoma turvallisuuden tunne. Näillä tekijöillä on merkittävä vaikutus siihen, kuinka tietoinen yksilö on ja miten tämä omaksuu ja noudattaa tietoturvapolitiikkaa. (Siponen, 2000.) Tietoisuuden on todettu muodostuvan myös yleisestä tietoturvan ja tietoturvapolitiikkojen tiedostamisesta. Se kuinka työntekijä hahmottaa tietoturvaa ja politiikkoja, vaikuttavaa työntekijän asenteeseen noudattaa tietoturvapolitiikkoja sekä suoraan muuttamalla käyttäytymistä, että epäsuorasti muokkaamalla työntekijän tietoturvaan tai käyttäytymisen seurauksiin liittyviä uskomuksia. (Bulgurcu, Cavusoglu & Benbasat, 2010.)

Käyttäjän ymmärrys ja tietoisuus siitä, millaista käyttäytymistä häneltä odotetaan vaikuttaa hänen käyttäytymiseensä (Leach, 2003; Boss ym., 2009). Tällainen ymmärrys muodostuu kolmesta vaikuttavasta tekijästä: tietämyksen rungosta, johon kuuluvat muun muassa henkilökohtaiset arvot, tietoturvapolitiikat, standardit ja käytänteet, johdon ja kollegoiden esimerkillään osoittamista käyttäytymismalleista sekä käyttäjän turvallisuuteen liittyvästä maalaisjärjestä ja päätöksentekokyvystä (Leach, 2003). Toinen lähestymistapa yksilön tietoisuuteen ja ymmärrykseen tietoturvasta, on pakollisuuden näkökulma. Tässä näkökulmassa merkittävää on tietoturvapolitiikkojen määritteleminen selkeästi ja näin saavutettava tietoisuus sääntöjen noudattamisen pakollisuudesta ja mahdollisten rikkomusten seurauksista. (Boss ym., 2009.) Tässä huomataan tietoisuuden liittyvän läheisesti palkintojen ja rangaistusten olemassa oloon. Palkintoihin ja rangaistuksiin palataan tarkemmin ulkoisten motivaatiotekijöiden käsittelyn yhteydessä.

Esitellyt tutkimukset ja artikkelit osoittavat selvästi kuinka suuri vaikutus tietoisuudella on työntekijän tietoturvakäyttäytymiseen ja motivaatioon toimia tietoturvaa edistävällä tavalla. Työntekijän tulisi olla tietoinen tietoturvapolitiikasta ja sen noudattamisen tärkeydestä, sekä toimintansa aiheuttamista seurauksista itselleen ja yritykselle. Tietoisuuden lisäämistä ja muita käyttäytymiseen vaikuttamisen keinoja käsitellään tarkemmin luvussa neljä.

3.1.3 Henkilökohtainen osaaminen

Teknologinen osaaminen on merkittävimpiä henkilökohtaisen osaamisen muotoja tietoturvasta puhuttaessa. Teknologisen osaamisen taso määrittelee muun muassa sen, millaisiin tekoihin työntekijä pystyy. Tämä pätee niin hyviin, neutraaleihin, kuin pahantahtoisiinkin toimiin. (Stanton, Stam, Mastrangelo & Jolton, 2005).

Aiemmin kuviossa 1 esitelty kahden tekijän loppukäyttäjän tietoturvakäyttäytymisten luokittelu, esittelee havainnollisesti teknisten taitojen vaikutuksen yksilön tietoturvakäyttäytymiseen. Käyttäytymismallit on luokittelussa jaoteltu matalan ja korkean teknisen vaativuuden mukaan, sekä toiminnan motiivin mukaan. Korkea tekninen osaaminen yhdessä hyväntahtoisuuden kanssa mahdollistaa tutkijoiden mukaan niin sanotun tietoisen vakuuttamisen (eng. aware assurance), joka tarkoittaa esimerkiksi mahdollisten haittaohjelmien etsimistä ja havaitsemista yrityksen järjestelmistä. Vastaavasti pahantahtoisella ja teknisesti taitavalla työntekijällä on mahdollisuus tarkoitukselliseen tuhoamiseen (eng. intentional destruction), joka voi käytännössä olla esimerkiksi tietomurron tekeminen ja arkaluontoisten tietojen varastaminen. (Stanton ym., 2005.) Toisaalta matala teknisen osaamisen taso yhdistettynä välinpitämättömyyteen, tai neutraaliin suhtautumiseen, voi johtaa naiveihin virheisiin (Stanton ym., 2005). Tällaisia virheitä ovat esimerkiksi huonon salasanan, kuten ”password”, valitsemisen tai roskapostien avaaminen työpaikan verkossa. Tällainen käytös altistaa yrityksen epäsuorasti riskeille, esimerkiksi helpottamalla ulkoisen tietomurron suorittamista.

Edellä esitetyistä esimerkeistä voidaan huomata kuinka suuri vaikutus on sillä, miten päteviä työntekijät ovat teknologiselta osaamiseltaan. Vaikka työntekijän tahtotila ei olisi pahantahtoinen, voi tämä silti aiheuttaa merkittävää haittaa yrityksen tietoturvalle jos tekninen ymmärrys ja osaaminen ovat liian heikolla pohjalla.

3.2 Ulkoisesti motivoivat tekijät

Ulkoinen motivaation käyttäytymiselle antavat sellaiset tekijät, joilla on seuraamuksia tekijälle tai muuten erotettavissa oleva lopputulos (Ryan & Deci, 2000). Seuraamukset voivat olla konkreettisia, kuten palkintoja tai rangaistuksia, mutta myös vaikeammin havaittavia kuten yhteisön hyväksyntä tai paheksunta ja muut normien ylläpitämät seuraukset. Ulkoisina henkilöstön tietoturvakäyttäytymiseen vaikuttavina tekijöinä voidaan pitää tietoturvapolitiikan olemassaoloa ja sen noudattamisen pakollisuutta, palkintoja ja rangaistuksia, työyhteisön normeja, tietoturvakoulutusta, yrityksen johdon sitoutuneisuutta sekä viestinnän ja palautteen laatua ja määrää.

3.2.1 Tietoturvapolitiikan olemassaolo ja noudattamisen pakollisuus

Tietoturvapolitiikka on yksi tärkeimmistä organisationaalisen tietoturvallisuuden hallinnan ja soveltamisen tehokkuuden varmistamisen keinoista (Höne & Eloff, 2002). Näin ollen määritellyn tietoturvapolitiikan puuttumista voidaan pitää suurena tietoturvariskinä yritykselle. Tietoturvapolitiikan määritteleminen vaikuttaa suoraan henkilöstön tietoisuuteen ja käsityksiin siitä mitä saa ja mitä ei saa tehdä, liittyen tietoturvaan ja teknologiaan (Bishop, 2003). Tietoisuuden ja seurausten vaikutusta käyttäytymiseen kuvattiin edellisissä luvuissa.

Tietoturvapolitiikkojen määritteleminen ja käyttäytymismallien arvioiminen ovat tehokkaita keinoja yksilöiden vakuuttamiseksi siitä, että politiikat ovat pakollisia noudattaa. Käsitys pakollisuudesta vaikuttaa voimakkaasti yksilön motivaatioon toimia tietoturvan edistämiseksi. (Boss ym., 2009.) Toisinsanoen on huomattu, että mikäli yksilöt uskovat johdon tarkkailevan, he tottelevat määräyksiä.

Tietoturvapolitiikan tulisi myös olla kokonaisuudessaan ymmärrettävä ja helposti sisäistettävä. Tietoisuutta politiikan olemassaolosta on lisättävä riittävällä mainostamisella yrityksissä esimerkiksi koulutuksin ja julistein. (Siponen & Vance, 2010.)

Mikäli tietoturvapolitiikan kirjoittavat esimerkiksi tietoturva-alan ammattilaiset on huolehdittava siitä, että ohjeet on kirjoitettu kansantajuisella kielellä ilman ammatillista slangia, tai ennakko-odotuksia käyttäjien ymmärryksestä. Yrityksellä tulisikin olla selkeästi määritelty tietoturvapolitiikka ja työntekijäiden tulisi olla tietoisia mahdollisesta valvonnasta ja toimintansa seurauksista. Yksilön käsitykseen tietoturvapolitiikan noudattamisen pakollisuudesta liitty-

vät läheisesti seuraavassa alaluvussa käsiteltävien palkintojen ja rangaistusten vaikutus motivoinnissa.

3.2.2 Säännöt, rangaistukset ja palkinnot

Rangaistuksien tarkoitus on pelottaa tai uhata toimijaa seuraamuksilla, mikäli tämä toimii vastoin sääntöjä, määräyksiä tai muita ohjeita. Rangaistukset vaikuttavat myös todellisuudessa yksilöiden käyttäytymiseen. Ne voivat yrityskontekstissa käsittää muun muassa tuomitsemista, sakkoja, irtisanomisen ja vankilaan joutumisen. (Herath & Rao, 2009.)

Peloteteorian, joka tarkoittaa käytännössä sitä, että teon seuraamukset ovat niin ”pelottavia”, ettei tekoa haluta suorittaa, perusteella on esitetty, että rangaistukset vaikuttavat yksilön käyttäytymiseen väistämättömyytensä ja vakavuutensa perusteella. Käytännössä tämä tarkoittaa sitä, että rangaistuksen väistämättömyyden ja vakavuuden kasvaessa, ei-sallitun käytöksen pitäisi vähentyä. (Herath & Rao, 2009.) Toisaalta vasta-argumenttina on esitetty, ettei rangaistuksen vakavuudella ole merkitystä rikkeen suorittamisen todennäköisyydelle (Siponen & Vance, 2010; Guo, Yuan, Archer & Connelly, 2011). Tutkimustieto tästä aiheesta on ristiriitaista, mikä osaltaan saattaa selittyä neutralointitekniikoilla, joilla työntekijä sallii itselleen virheellisen käyttäytymisen ja uskoo silti olevansa sääntöjä noudattava työntekijä. Neutralointitekniikat oikeuttavat työntekijälle hänen virheellisen tai ”laittoman” käyttäytymisensä ja näitä tekniikoita onkin tutkittu aiemmin lähinnä rikosteknisissä yhteyksissä. (Siponen & Vance, 2010.) Näitä tekniikoita ovat tarkemmin:

- vastuun kieltäminen
- vahingon kieltäminen
- välttämättömyydellä puolustautuminen
- arvostelijoiden tuomitseminen
- auktoriteetteihin vetoaminen
- hyvien ja pahojen tekojen tasapainottaminen. (Siponen & Vance, 2010.)

Tällaisten tekniikoiden avulla työntekijä siis oikeuttaa itselleen haluamansa käyttäytymisen ja näin ollen heikentää rangaistusten vaikuttavuutta käytöstä ohjaavana tekijänä, ellei neutraloinnin vastatoimiin ryhdytä. Tutkimuksissa esiintyvän, rangaistusten vaikutuksiin liittyvän ristiriidan tarkempi pohtiminen jää kuitenkin tämän tutkielman laajuuden ulkopuolelle.

Organisaation tulisi pystyä myös valvomaan rikkeiden tekemistä, muutoin rangaistuksien vaikutus jää mitättömäksi. Valvonta voi käsittää satunnaisia tarkastuskierroksia työpaikoilla, tietokoneen selaushistorian tarkkailua, verkkolokien seurantaa tai muita vastaavia toimia. (Herath & Rao, 2009.) Nämä käytännöt vaikuttavat työntekijöiden tietoisuuteen valvonnasta, joka aiemmin todettiin merkittäväksi motivoivaksi tekijäksi.

Siinä missä rangaistuksia ja peloteteoriaa on tutkittu paljon turvallisuuteen liittyen, näyttäisi palkitsemisen vaikutusten tutkimus olleen vähäisempää.

Esimerkiksi empiirisesti on huomattu palkintojen vaikuttavan merkittävästi työntekijän hinta-hyöty-arvioon, tämän punnitessa toimintansa kannattavuutta. Palkinnot itsessään eivät riitä saamaan työntekijöitä uskomaan, että tietoturvapolitiikan vaatimukset ovat pakollisia noudattaa, mutta niitä voidaan käyttää motivoimaan työntekijöiden toimintaa oikeaan suuntaan. (Bulgurcu, Cavusoglu & Benbasat, 2010.)

Eräänlaisena palkintona voidaan pitää myös seikkaa, jonka mukaan työntekijä noudattaa sääntöjä todennäköisemmin, mikäli hän uskoo teoillaan olevan merkitystä yleisen turvallisuuden kannalta (Herath & Rao, 2009). Tällöin palkinto ei ole aineellinen, esimerkiksi rahaa, vaan aineetonta tarpeellisuuden ja tärkeyden tunnetta.

Palkinnoilla ja rangaistuksilla on edellä esitettyjen esimerkkien perusteella suuri merkitys työntekijän tietoturvakäyttäytymiseen. Ne vaikuttavat työntekijän arvioon siitä, miten hänen toimintansa vaikuttaa yleiseen ja tapauskohtaiseen turvallisuuteen. Vaikka rangaistusten tehokkuudesta on vaihtelevaa tutkimustietoa, ovat ne varmasti yksi perinteisimpiä tietoturvan kohentamisen keinoja. Rangaistusten ohella myös palkinnot ovat tehokkaita motivaattoreita niin aineellisina, kuin aineettominakin hyötyinä.

3.2.3 Työyhteisön normit ja johdon sitoutuneisuus

Työyhteisön normeilla tarkoitetaan kirjoittamattomia sääntöjä ja käyttäytymismalleja, joita työyhteisössä on ja joiden rikkomisesta aiheutuu seuraamuksia kuten paheksuntaa tai ilmiantoja, tai jotka vaihtoehtoisesti ovat tyypillisiä käytäntöjä virallisten ohjeiden noudattamisen sijaan. Esimerkiksi on huomattu heikommat tietoturvataidot omaavien työntekijöiden tyypillisesti sekä kysyvän neuvoa, että vierittävän vastuun tietoturva-asioista esimiehilleen, tai paremmin asiat hallitseville työtovereilleen. (Guo ym., 2011.) Normit vaikuttavat työntekijöiden käyttäytymiseen sekä suorasti, että epäsuorasti. Epäsuoran vaikutuksen aiheuttavat työyhteisön sanattomasti hyväksymät tai hylkimät käytösmallit, jolloin normien noudattaminen tai noudattamatta jättäminen aiheuttaa seuraamuksia. Suora vaikutus sen sijaan ilmenee, mikäli yksilölle on tärkeää vain toimia samoin kuin muutkin, riippumatta siitä, onko toiminta oikein vai väärin. (Guo ym., 2011.)

Työyhteisön normeihin liittyen on tutkittu myös roolien vaikutusta tietoturvakäyttäytymiseen. Työroolin ulkopuolisella (eng. extra-role) käyttäytymisellä ja sosiaalisella kontrollilla on huomattu olevan huomattava vaikutus työntekijöiden tietoturvakäyttäytymiseen. Työroolin ulkopuolinen käyttäytyminen tarkoittaa sellaista käyttäytymistä, jota tietoturvapolitiikka ei määrittele ja joka on näin ollen palkintojen ja rangaistuksien vaikutuksen ulkopuolella (Hsu, Shih, Hung & Lowry, 2015). Erityisesti sosiaalinen kontrolli liittyy läheisesti työyhteisön normeihin, sillä se tarkoittaa tutkijoiden mukaan työyhteisön sosiaalisen kanssakäymisen tilanteita ja sosiaalista ilmapiiriä, joihin vaikuttavat normit ja sosiaaliset suhteet. Sosiaalisen kontrollin on huomattu olevan yhtä tärkeää kuin muodollisen kontrollin, puhuttaessa työroolikäyttäytymisestä. Toinen merkittävä havainto on, että sosiaalinen kontrolli on paljon olennaisempaa kuin muo-

dollinen kontrolli, kun puhutaan työroolin ulkopuolisesta käyttäytymisestä. (Hsu ym., 2015.)

Johdon sitoutuneisuus tietoturvapolitiikan noudattamiseen vaikuttaa myös työntekijöiden suhtautumiseen ja käyttäytymiseen. Johdon tehtävä on korostaa turvallisuuden merkitystä ja jakaa tietoa aiheesta. Johdon sitoutuneisuus tietoturvaa kohtaan heijastuu suoraan alaspäin hierarkiassa ja organisaation alemmat tasot vaativat johdolta ymmärrystä, kiinnostusta ja toimia tietoturvan parantamiseksi. (Kraemer & Carayon, 2005.) Johdon osallistuminen tietoturva-aloitteisiin vaikuttaa suorasti ja epäsuorasti työntekijöiden asenteisiin tietoturvapolitiikkaa kohtaan (Hu, Dinev, Hart ja Cooke, 2012). Suora vaikutus ilmenee esimerkiksi uusina toimintaohjeina ja määräyksinä ja epäsuorana vaikutuksena puolestaan voidaan pitää esimerkiksi johdon vaikutusta organisaatiokulttuurin ja yhteisön normien muuttumiselle kohti tietoturvallisempaa työyhteisöä.

Työyhteisön normit ja yrityksen johdon suhtautuminen vaikuttavat siis selvästi työntekijöiden tietoturvakäyttäytymiseen ja asenteeseen tietoturvapolitiikkaa kohtaan. Johdon käyttäytyminen vaikuttaa suoraan työntekijöihin, mutta myös välillisesti organisaatiokulttuurin ja normien kautta. Johdon toiminnan vaikutus työntekijöiden suhtautumiseen ilmenee hyvin tyypillisestä ajattelumallista: ”jos muutkaan eivät noudata sääntöjä, miksi minun pitäisi?”, tällainen vaikutus näkyy erityisen selvästi työntekijän asenteessa tietoturvaa kohtaan silloin, kun johto ei noudata omia ohjeitaan.

3.2.4 Muut tekijät

Muina merkittävinä tietoturvakäyttäytymiseen vaikuttavina tekijöinä voidaan lähdekirjallisuuden perusteella pitää koulutuksen määrää ja laatua, palautteen antamisen mahdollisuutta, teknologian kehittymistä ja kulttuurin muuttumista. Tässä alaluvussa käsitellään lyhyesti kutakin näistä tekijöistä.

Työntekijöiden tietoturvaosaamiseen ja tekniseen kyvykkyyteen vaikuttaa koulutuksen määrä, merkityksellistä organisaation tietoturvakultuurin kannalta on sekä yleinen että aihekohtainen koulutus (Kraemer & Carayon, 2005). Olisi olennaista, että yleisen tietoturvapolitiikkaan perehdyttämisen lisäksi työntekijöille tarjottaisiin heidän henkilökohtaiseen työnkuvaansa liittyvää tietoturvakoulutusta. Esimerkiksi yrityksen johtoa kannattaisi ohjeistaa teknologian suojaamiseksi varkauksilta, jotta arkaluontoista materiaalia ei häviäisi. (Kraemer & Carayon, 2005.) Esiin on nostettu myös viestinnän ja palautteen antamisen merkitys tietoturvakulttuurin parantamisessa. Työntekijät kokivat esimerkiksi yrityksen intranetissä olevan tietoturvapolitiikan kommentoimis- ja kyseenalaistamismahdollisuuden tärkeäksi viestinnän osa-alueeksi. (Kraemer & Carayon, 2005.) Viestinnän tärkeyden voi huomata myös viestintäteknologioiden soluttautumisesta ihmisten jokapäiväiseen elämään. Viimeaikaisessa uutisoinnissa on jopa puhuttu paljon riippuvuudesta erilaisia medioita kohtaan ja aihetta on käsitelty myös tieteellisissä julkaisuissa (Bright, Graun & Kleiser, 2015).

Teknologian jatkuvan vauhdikkaan kehityksen myötä myös yritykset omaksuvat uusia teknologioita käyttöönsä. Uudet mobiili- ja viestintäteknologiat, joita on aiemmin käytetty vain kotioloissa, saattavat saada työntekijät vaatimaan enemmän vapautta laitteiden ja teknologioiden käytössä (Colwill, 2009). Tähän liittyy myös yleistymässä oleva ”bring your own device” eli byod-ilmiö (Song, 2014). Tällainen kehitys asettaa luonnollisesti enemmän vaatimuksia yrityksen tietoturvatoimille, koulutukselle ja muille resursseille, sillä vaihtelevilla laitteilla voi olla toisistaan eroavia vaatimuksia turvallisuuden ja teknologisen osaamisen suhteen.

Erityisesti pienille ja keskisuurille yrityksille (PK-yritykset) varautuminen tällaisiin vaatimuksiin voi olla resurssien puolesta mahdotonta. PK-yrityksille jääkin siis harkittavaksi niin sanotun liikkuvan liiketoimintastrategian edistäminen, jolloin on joustettava turvallisuudesta, tai liikkuvan liiketoimintastrategian hylkääminen tietoturvan säilyttämiseksi ja pitäytyminen perinteisemmissä työskentelymenetelmissä. (Harris & Patten, 2014.)

4 HENKILÖSTÖN TIETOTURVAKÄYTTÄYTYMISEN PARANTAMINEN

Tässä luvussa siirrytään henkilöstön tietoturvakäyttäytymiseen vaikuttavien tekijöiden erittelystä, käyttäytymisen parantamisen keinoihin. Edellisessä luvussa esitelty motivaatio on merkittävä tekijä jokaisen esitellyn keinon takana, joten tässä luvussa ei koettu tarpeelliseksi järjestellä alalukuja sen mukaan onko motivaatio sisäistä vai ulkoista. Tämän luvun tarkoitus on pikemminkin tarjota konkreettisia keinoja, joilla on mahdollista parantaa henkilöstön sitoutuneisuutta ja motivaatiota tietoturvaa ja politiikkojen noudattamista kohtaan.

4.1 Tietoisuuden lisääminen

Ensimmäisenä tietoturvakäyttäytymisen parantamisen menetelmänä käsitellään tietoisuuden lisäämistä, sillä se on yksi merkittävimpiä keinoja, joilla yritys voi parantaa tietoturvaansa henkilöstönsä kautta. Useissa lähteissä käsitellään työntekijän tietoisuuden merkitystä käyttäytymisen aiheuttajana (Siponen, 2000; Bulgurcu, Cavusoglu & Benbasat, 2010; Leach, 2003; Boss ym., 2009). Tietoisuus tietoturvasta tarkoittaa sitä, että yrityksen työntekijät tiedostavat ja ovat sitoutuneita yrityksen turvallisuuspyrkimyksiin. On olemassa lukuisia käytännön lähestymistapoja työntekijöiden tietoisuuden lisäämiseksi. Näitä ovat esimerkiksi:

- materiaalin, koulutuksen ja toiminnan loogisuus ja järkevyys,
- tunteisiin, moraaliin ja etiikkaan vetoaminen,
- mahdollinen uhka yksilön hyvinvoinnille ja turvallisuuden tunteelle. (Siponen, 2000.)

Kaikkien tekojen joilla pyritään tehokkaasti vaikuttamaan käyttäjän toimintaan, tulisi noudattaa käyttäytymisteorioiden periaatteita. Lisäksi käyttäjille tulisi

selittää tai havainnollistaa, miksi turvallisuuspolitiikkojen noudattaminen on niin tärkeää. (Siponen, 2000.)

On huomattu myös, että tietoisuudella, SETA-ohjelmilla (turvallisuus, koulutus, harjoittelu, tietoisuus) ja tietokoneiden tarkkailulla on vaikutusta tietoturvavirheiden ja -rikkeiden ehkäisyssä. Tietoisuus paitsi olemassa olevista säännöistä, myös suoritetusta valvonnasta vähentää riskejä. Esimerkiksi tietoturvakäytäntöjen määrittely on olennainen tekijä vakuutettaessa käyttäjää käytäntöjen noudattamisen pakollisuudesta. Mikäli käyttäjä siis uskoo johdon tarkkailevan hänen toimintaansa, hän noudattaa todennäköisemmin tietoturvakäytäntöjä. (Boss ym., 2009.)

Työntekijän on olennaista myös tunnistaa yritykseen kohdistuvat tietoturvauhkat ja riskit. Työntekijälle tulee korostaa yrityksen altistumista riskeille, mikäli jokainen ei noudata annettuja määräyksiä ja ohjeita vakavasti, ja mukaile käytöksellään tietoturvapolitiikkaa. Työntekijän tulee kokea, että tietoturvapolitiikan noudattaminen on osa hänen työnkuvaansa ja vastuutaan. (Vance, Siponen & Pahnila, 2012.)

4.2 Hyvä tietoturvapolitiikka

Kuten jo aiemmissa luvuissa todettiin, tietoturvapolitiikka on yrityksen tärkein konkreettinen työkalu matkalla kohti parempaa tietoturvaa (Höne & Eloff, 2002a). Tietoturvapolitiikan tulisi sisältää ohjeet tietoturvan kanssa toimimiseen, eli käytännössä mitä saa tehdä ja miten ei pidä toimia (Bishop, 2003). Hyvässä tietoturvapolitiikassa määritellään myös seuraamukset mahdollisesti suoritetuille rikkeille (Guo ym., 2011). Tällä tavoin koostettu tietoturvapolitiikka toimii niin työntekijän kuin johtotasonkin ohjeena ja päätöksenteon välineenä.

Tietoturvapolitiikalla on suuri vaikutus edellä käsiteltyyn työntekijöiden tietoisuuteen tietoturvasta. Määritellyn tietoturvapolitiikan avulla selvitetään tietoturvan merkitys kaikille turvallisuuden säilyttämisen kannalta olennaisille henkilöille. Huomioon ottaen laajan yleisön jolle politiikka suunnataan, esimerkiksi koko kansainvälisen organisaation henkilöstö, on olennaista että se sisältää myös ymmärrettävän tietoturvan määritelmän. (Höne & Eloff, 2002a.)

Tehokas tietoturvapolitiikka sisältää selkeät ohjeet ja käytännöt, jotka selittävät työntekijälle mitä tältä odotetaan tietoresurssien käytön suhteen. Vielä tietoturvapolitiikan oikeaa sisältöäkin tärkeämpää on se tapa, jolla asiat ilmaistaan dokumentissa ja miten ne kommunikoidaan käyttäjille. (Höne & Eloff, 2002b.)

4.3 Työntekijän oikeasta toiminnasta kokeman hyödyn lisääminen

Lukuisissa tutkimuksissa on huomattu työntekijän henkilökohtaisen arvion tekojensa seurauksista vaikuttavan merkittävästi päätökseen toimia tietoturvapolitiikan mukaan, tai jättää toimimatta (Bulgurcu ym., 2010; Herath & Rao, 2009; Guo ym., 2011). Sitä miten tällainen henkilökohtainen riskiarvio muodostuu, tutkittiin luvussa kolme. Tässä luvussa keskitytään siihen, kuinka työntekijä saadaan kokemaan tietoturvapolitiikan noudattaminen tarpeelliseksi ja hyödylliseksi sekä itselleen, että yritykselle.

Tietoturvakoulutukset ja -perehdytykset tulisi suunnitella niin, että työntekijöiden kokema sisäinen hinta, hyöty, turvallisuus ja haavoittuvaisuus ovat korostettuina. Tietoisuuden lisääminen vähentää työntekijöiden käsitystä siitä, että tietoturvakäytäntöjen noudattaminen haittaa varsinaisten työtehtävien suorittamista. Tällöin tietoisuus tietoturvasta vaikuttaa suoraan ja epäsuorasti työntekijöiden arvioon ohjeiden noudattamisen kannattavuudesta. (Bulgurcu ym., 2010.)

Työntekijöiden kokema kiinnijäämisen riskin suuruus vaikuttaa merkittävästi sääntöjen rikkomisen todennäköisyyteen ja on jopa epäilty, että seurantamekanismien olemassa olo ja näkyvyys ovat olennaisempia oikean toiminnan motivaattoreita, kuin mahdollisten rangaistusten vakavuus. (Herath & Rao, 2009.) Sen lisäksi, että työntekijälle havainnollistetaan kiinnijäämisen riski ja politiikkojen noudattamisen hyöty tai noudattamatta jättämisen haitat, on tärkeää suunnitella tietoturvakäytännöt niin, ettei niiden noudattaminen vie paljoa aikaa tai resursseja. Työntekijöiden ei tulisi kokea tietoturvakäytäntöjen noudattamisen haittaavan työskentelyä tai olevan pois muusta työpanoksesta (Bulgurcu ym., 2010). Työnantajan olisi siis varattava työntekijälle myös aikaa noudattaa politiikkoja.

On myös esitetty sisäisesti motivoivien tekijöiden korostamista, rangaistuksiin keskittymisen sijaan tietoturvakäytännöissä. Tällainen työntekijän sisäinen motivaatio voidaan saada aikaan, kun sidotaan tiukasti yhteen työntekijöiden arvot ja tietoturvapolitiikan pyrkimykset. (Son, 2011.) Työntekijän tulisi pystyä näkemään tekojensa vaikutus tietoturvaan, sillä se motivoi oikeaan toimintaan (Son, 2011; Herath & Rao, 2011).

4.4 Johdon sitoutuminen ja tietoturvallinen organisaatiokulttuuri

Työntekijöiden käyttäytymiseen vaikuttaa huomattavasti se, mitä he uskovat johdon odottavan. Toinen merkittäväksi havaittu tekijä on muiden kollegoiden käyttäytyminen tietoturvan suhteen. Näistä tekijöistä voidaan päätellä, että yrityksen johto voi parantaa turvallisuuskäytäntöjen noudattamista parantamalla

sopivaa turvallisuusilmapiiriä organisaatiossa. Kaikenkaikkiaan on olennaista, että johto tekee parhaansa vakuuttaakseen työntekijät tietoturvan tärkeydestä organisaatiolle. (Herath & Rao, 2009.) Johtajuutta voidaankin pitää yhtenä tärkeimmistä henkilöstön motivointikeinoista tietoturvakäyttäytymisen suhteen ja mikäli johto omalla toiminnallaan tukee esitettyjä käytäntöja näin osoittaen niiden merkityksen yritykselle, seuraa henkilöstö todennäköisesti esimerkkiä (Leach, 2003). Samoin käynee myös siinä tilanteessa, että johto ei ole kiinnostunut tai ei noudata sääntöjä.

Yrityksen johdon on mahdollista toimia ennakoivassa roolissa työntekijöiden sääntöjen myötäilykäyttäytymisen muodostumisessa. Eräässä tutkimuksessa johdon osallistuminen oli jopa tärkein ulkoinen tekijä, jonka on mahdollista vaikuttaa työntekijöiden käyttäytymiseen. (Hu ym., 2012.) Johdolle on tyypillistä delegoida vastuuta tietoturvasta yrityksen informaatioteknologiaan erikoistuneille alemman johdon henkilöille. Näin ei kuitenkaan pitäisi toimia, vaan olisi ensisijaisen tärkeää, että etenkin ylin johto ottaa aktiivisen ja näkyvän roolin yrityksen tietoturvan kehittämisessä. Tällä on vaikutus niin organisaatiokulttuuriin, kuin suoraan työntekijöiden päätöksentekoonkin. (Hu ym., 2012).

Organisaatiokulttuuri jossa tavoitteet, säännöt ja politiikat ovat selvästi määritellyt ja kunnioitetut, jossa työntekijöitä arvioidaan tavoitteiden saavuttamisen ja sääntöjen noudattamisen perusteella ja jossa sääntöjen noudattamisesta palkitaan ja rikkomisesta rangaistaan, vaikuttaa positiivisesti työntekijöiden aikeisiin ja käyttäytymiseen tietoturvapolitiikan noudattamiseen liittyen. (Hu ym., 2012.) Turvallisuustietoisen organisaatiokulttuurin luominen parantaa tietoturvaa ja yritysten tulisikin järjestää koulutuksia ja muita tietoisuuden lisäämiseen tähtääviä ohjelmia (Bulgurcu ym., 2010).

4.5 Muut tekijät

Tekijöitä jotka eivät mahtuneet edellisiin kategorioihin ovat esimerkiksi koulutus, joka vaikuttaa työntekijän tietoturvaosaamiseen ja teknisiin taitoihin sekä viestintä ja palautteen antaminen, joilla on merkitystä politiikkojen ymmärtämisen ja merkittävyyden kannalta yksilölle (Kraemer & Carayon, 2005). Näiden konkreettisten vaikuttimien lisäksi kehittyvä viestintäkulttuuri, uudet teknologiat ja mediat tuovat mukanaan uudenlaisia riskejä yrityksille, mutta samalla kehittymismahdollisuuksia. Yritysten täytyy arvioida tarkasti uusien teknologioiden omaksumista ja niiden asettamia tietoturva- ja muita vaatimuksia. (Colwill, 2009; Harris & Patten, 2014).

5 YHTEENVETO JA LOPPUPÄÄTELMÄT

Tutkielmassa selvitettiin kirjallisuuskatsauksen keinoin henkilöstön tietoturvakäyttäytymiseen vaikuttavia tekijöitä ja mahdollisia keinoja noiden käyttäytymismallien parantamiseksi. Laajasta lähdemateriaalista pyrittiin valitsemaan luotettavimmat ja tulokset jaettiin johdantoon, kolmeen sisältölukuun ja yhteenvetoon. Ensimmäisessä sisältöluvussa määriteltiin olennaiset käsitteet: tietoturva ja tietoturvapolitiikka, sekä huomattiin henkilöstön merkittävyys tietoturvantekijänä (Hu ym., 2012). Lisäksi pyrittiin vastaamaan ensimmäiseen tutkimuskysymykseen: mitä on tietoturvakäyttäytyminen? Tietoturvakäyttäytymisen käsitettä valotettiin esimerkiksi kuvion 1 avulla ja todettiin, että sen piiriin kuuluvat kaikki ne toimet, jotka vaikuttavat tietoturvaan suorasti tai epäsuorasti.

Toinen luku omistettiin henkilöstön käyttäytymiseen vaikuttavien tekijöiden erittelylle. Samalla vastattiin toiseen tutkimuskysymykseen: Mitkä tekijät vaikuttavat henkilöstön tietoturvakäyttäytymiseen? Tekijät jaettiin sisäisesti motivoiviin ja ulkoisesti motivoiviin, psykologian ja informaatioteknologian lähteiden perusteella (Ryan & Deci, 2000; Son, 2011). Sisäisesti motivoivia tekijöitä huomattiin olevan toiminnan koetut seuraamukset ja halu noudattaa määräyksiä, tietoisuus tietoturvallisuudesta ja henkilökohtainen osaaminen. Ulkoisesti motivoivia tekijöitä puolestaan ovat tietoturvapolitiikan olemassaolo ja noudattamisen pakollisuus, säännöt, rangaistukset ja palkinnot sekä Työyhteisön normit ja johdon sitoutuneisuus. Jokaista mainittua tekijää kannattivat useammat lähteet ja ne todettiin riittävän luotettaviksi, jotta nämä tekijät voitiin sisällyttää tutkielmaan. Tutkimuksen tuloksia on pyritty havainnollistamaan kuviossa 2.

KUVIO 2 Tutkielman saavutusten havainnollistus

Tutkielman neljännessä luvussa pyrittiin vastaamaan kolmanteen tutkimuskysymykseen, joka oli: miten työntekijöiden tietoturvakäyttäytymistä voitaisi parantaa? Luvussa kerättiin lähteiden perusteella keinoja henkilöstön tietoturvakäyttäytymisen parantamiseksi. Työnantajan tulisi lähteiden perusteella huolehtia ainakin seuraavista tekijöistä:

- Työntekijöiden tietoisuuden ja vastuullisuuden lisääminen
- Selkeästi määritelty tietoturvapolitiikka ja käytännöt
- Valvonnasta huolehtiminen ja sen näkyvyyden lisääminen
- Toiminnan seurauksien havainnollistaminen, vetoaminen tunteisiin ja moraaliin
- Tietoturvapolitiikan noudattamisen integroiminen osaksi normaalia työntekoa
- Johdon sitoutuneisuudesta ja kiinnostuneisuudesta huolehtiminen
- Tietoturvaa tukevan organisaatiokulttuurin vahvistaminen
- Tilanteeseen sopivista, ennalta tunnetuista palkinnoista ja rangaistuksista huolehtiminen

Tutkimuksen rajoitteiden pohtiminen on aloitettava toteamalla, että tutkielma on kirjallisuuskatsaus. Tästä seuraa se, ettei väitteitä ja tuloksia ole saavutettu tai testattu käytännössä, niitä muutamaa lähdettä lukuunottamatta joiden taus-

talla oli empiirinen tutkimus. Lisäksi tutkielman laajuus on melko suppea, mikä rajoittaa näkökulmien punnitsemista ja lähteiden vertailua.

Tähän liittyen tutkielmaa kirjoitettaessa oli välttämätöntä sivuuttaa esimerkiksi lähteistä löytynyt ristiriita rangaistusten vaikutuksesta käyttäytymiseen. Osa lähteistä piti rangaistusten todennäköisyyttä merkittävimpänä tekijänä, osa niiden vakavuutta ja muutama tutkimus ei pitänyt rangaistuksia lainkaan merkittävänä tekijänä henkilöstön motivoinnin kannalta. Tässä olisi kiinnostava mahdollisuus empiiriselle ja muulle jatkotutkimukselle, jossa voitaisi selvittää miksi ristiriitoja esiintyy.

Tutkielman laajuus vaikuttaa myös siihen, että vaikka saatiinkin aikaiseksi kattava lista käyttäytymiseen vaikuttavista tekijöistä, jäi jotain varmasti myös uupumaan. Esimerkiksi tietoista pahantahtoisuutta ei käsitelty erillisenä tekijänä, eikä sen motivaatiotekijöihin ollut mahdollista syventyä. Tällainen rikollisuus ja tietoinen tuhoaminen ovat kuitenkin todellisuutta ja niiden tutkimuksessa olisi toinen mielenkiintoinen jatkotutkimuskohde.

Muita rajoitteita tutkimuksen suorittamiselle ovat kirjoittajan puutteellinen psykologian ja käyttäytymisteorioiden tuntemus, mikä saattaa vaikuttaa esimerkiksi tutkielman rakenteeseen, valittuihin lähteisiin ja argumentaatioon. Lisäksi tutkielma on kirjoittajan ensimmäinen akateeminen tutkimus ja tarkoitettu osaltaan harjoitukseksi tulevaisuutta varten, mikä voi vaikuttaa argumentaation ja havaintojen luotettavuuteen.

Jokin edellämainituista tutkimuskohteista voisi olla kiinnostava pro gradu -tutkielman aiheeksi. Samoin jonkin edellä mainitun, tai muun näkökulman tutkiminen tietyn yrityksen osalta tapaustutkimustyyppisesti, olisi varmasti antoisa tutkielman aihe.

LÄHTEET

Anderson, J. M. (2003). Why we need a new definition of information security. *Computers & Security, 22*(4), 308-313.

Bishop, M. (2003). What is computer security? *Security & Privacy, IEEE, 1*(1), 67-69.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems, 18*(2), 151-164.

Bright, L., Grau, S. L. & Kleiser, S. B. (2015). Thumbs down to facebook? Exploring social media addiction among millenials using the consumption continuum framework. *American Academy of Advertising. Conference. Proceedings (Online)*, 170-171. Lubbock: American Academy of Advertising.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly, 34*(3), 523-548.

Colwill, C. (2009). Human factors in information security: The insider threat – Who can you trust these days? *Information Security Technical Report, 14*(4), 186-196.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*(2), 90-101.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research, 20*(1), 79-98.

Dhillon, G. (2001). Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns. *Computers & Security, 20*(2), 165-172.

Ernest & Young LPP. (2002). *Global information security survey 2002.* UK: Presentation Services.

Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk managementnull. *Info Mngmnt & Comp Security, 22*(5), 410-430.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2004). *2004 CSI/FBI Computer Crime and Security Survey.* Manhasset: CMP Media.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. *Journal of Management Information Systems, 28*(2), 203-236.

Harris, M. A., & Patten, K. P. (2014). Mobile device security considerations for small- and medium-sized enterprise business mobility. *Information Management & Computer Security, 22*(1), 97-114.

Herath, T., & Rao, H. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165.

Hsu, J. S.-C., Shih, S.-P., Hung, Y. W., & Lowry, P. B. (2015). The Role of Extra-Role Behaviors and Social Controls in Information Security Policy Effectiveness. *Information Systems Research, 26*(2), 282-300.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture*. *Decision Sciences, 43*(4), 615-660.

Höne, K., & Eloff, J. (2002a). Information security policy — what do international information security standards say? *Computers & Security, 21*(5), 402-409.

Höne, K., & Eloff, J. (2002b). What Makes an Effective Information Security Policy? *Network Security, 2002*(6), 14-16.

Kraemer, S., & Carayon, P. (2005). Computer and Information Security Culture: Findings from two Studies. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 49*(16), 1483-1488.

Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied Ergonomics, 38*(2), 143-154.

Leach, J. (2003). Improving user security behaviour. *Computers & Security, 22*(8), 685-692.

Liginlal, D., Sim, I., & Khansa, L. (2009). How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Computers & Security, 28*(3-4), 215-228.

NSTISSC. (2000). *National Information Systems Security (INFOSEC) Glossary.* Ft.Meade: National Security Agency.

Osisanwo, F., Shade Kuyoro, S., & Awodele, O. (2015). Internet Refrigerator –A typical Internet of. *3rd International Conference on Advances in Engineering Sciences & Applied Mathematics (ICAESAM'2015*, (pp. 59-63). London.

Ponemon Institute. (2015). *2015 Cost of Data Breach Study: Global Analysis.* Traverse City: Ponemon Institute.

Ryan, R. M., & Deci, E. L. (2000). Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions. *Contemporary educational psychology, 25*(1), 54-67.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awarenessnull. *Info Mngmnt & Comp Security, 8*(1), 31-41.

Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS quarterly, 34*(3), 487-515.

Son, J.-Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management, 48*(7), 296-302.

Song, Y. (2014). "Bring Your Own Device (BYOD)" for seamless science inquiry in a primary school. *Computers & Education, 74*(5), 50-60.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security, 24*(2), 124-133.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management, 49*(3-4), 190-198.

Whitman, M. E., & Mattord, H. J. (2012). *Principles of Information Security.* Boston, United States of America: Course technology, Cengage learning.