Tietoturvakäyttäytyminen organisaatioissa

Oulun Yliopisto
Tieto- ja sähkötekniikan tiedekunta
Tietojenkäsittelytieteiden koulutusohjelma
Kandidaatin tutkielma
Arttu Kruuti
4.4.2018

Tiivistelmä

Tietoturvakäyttäytyminen on tutkimusala, jota on lähdetty kehittämään, kun useat tutkimukset ovat huomanneet käyttäjien oleva suurin riski organisaatioiden tietoturvalle. Aiemmin huomio on keskittynyt enemmän teknisiin tietoturvaratkaisuihin, jotka ovat välttämättömiä, mutta niistä ei ole apua, kun organisaation omat työntekijät altistavat järjestelmän uhille, joita vastaan ratkaisuja ei ole suunniteltu. Tutkimusta on teknisten ratkaisujen sijaan alettu kohdistamaan asioihin kuten tietoturvapolitiikat ja niiden noudattaminen, sekä muihin ihmisläheisempiin aiheisiin. Näiden tutkimusten avulla yritetään löytää keinoja parantaa työntekijöiden tietoturvaohjeiden noudattamista ja kehittää niitä edelleen niin, että käyttäjät haluavat itse toimia turvallisemmin, eivätkä koe tietoturvaan liittyviä toimenpiteitä ylimääräisenä työnä ja ymmärtävät niiden tärkeyden.

Tämän kirjallisuuskatsauksen tarkoituksena on esitellä organisaatioiden työntekijöiden tietoturvakäyttäytymisen tutkimuksen osa-alueita, jotka kertovat käyttäjien toiminnasta ja siihen vaikuttavista tekijöistä heidän työympäristössään. Tutkimuksen pohjalta tuodaan esiin myös jatkotutkimuskohteita.

Tutkimuksen tulokset kokoavat yhteen eri ominaisuuksia ja alueita, joita olisi hyvä ottaa huomioon, kun kehitetään tietoturvapolitiikkoja ja –koulutusta organisaatioissa. Näiden löydöksien avulla organisaatiot voisivat paremmin suunnitella politiikkansa ja muut ohjeensa vastaamaan eri rooleissa toimivien työntekijöiden tarpeita. Tuloksista löytyy myös huomioita siihen, miten käyttäjien ympäristö tulisi ottaa huomioon.

Avainsanat
Tietoturva, tietoturvakäyttäytyminen, tietoturvapolitiikka

Ohjaaja
FT, tutkijatohtori Mari Karjalainen

Sisällysluettelo

Tiivistelmä 2
Sisällysluettelo 3
1. Johdanto 4
2. Keskeiset käsitteet 5
    2.1 Mitä on tietoturva? 5
    2.2 Mitä tarkoitetaan tietoturvapolitiikoilla? 6
    2.3 Mitä on tietoturvakäyttäytyminen? 7
3. Tutkimusmenetelmä 10
4. Tulokset 11
5. Pohdinta 16
6. Yhteenveto 20
Lähdeluettelo 22

1. Johdanto

Tietoturva on Crosslerin (2013) mukaan monipuolinen ala, johon kuuluu esimerkiksi teknisiä, ihmisen käyttäytymiseen ja johtamiseen liittyviä osa-alueita, jotka tulee huomioida organisaation tietoturvan hallinnassa. Yleensä tutkimus on lähinnä keskittynyt uusien teknisten tietoturvakeinojen suunnitteluun ja toteutukseen. Yksittäisen käyttäjän vaikutuksen tutkiminen tietoturvallisuuden toteuttamisessa on sen sijaan jäänyt teknistä osa-aluetta vähäisemmäksi, vaikka on arvioitu, että jopa puolet tietoturvarikkomuksista tapahtuu organisaation henkilöstöstä johtuvista syistä. (Crossler et al., 2013.) Tietoturvakäyttäytymisen alueella tutkimusta onkin alettu kohdistamaan myös ihmisläheisiin aiheisiin, kuten tietoturvapolitiikkojen noudattamiseen (Bauer, Bernroider, & Chudzikowski, 2017) ja miten organisaation sisäinen kulttuuri vaikuttaa myös tietoturvaan (Tang, Li, & Zhang, 2016). Tutkimusta on jopa tehty niinkin yksityiskohtaisista asioista, että kuinka käyttäjät kokevat ja vastaavat tietoturvavaroituksiin silmien liikkeitä seuraavaa teknologiaa hyödyntämällä (Anderson, Vance, Kirwan, Eargle, & Jenkins, 2016). Tutkimuksella pyritään parantamaan työntekijöiden tietoturvaohjeiden noudattamista sekä kehittämään niitä edelleen niin, että käyttäjät haluavat itse toimia turvallisemmin, eivätkä koe tietoturvaan liittyviä toimenpiteitä ylimääräisenä työnä ja ymmärtävät niiden tärkeyden (Albrechtsen, 2007).

Tämän tutkielman tarkoituksena on esitellä organisaatioiden työntekijöiden tietoturvakäyttäytymisestä, toiminnasta ja siihen liittyvistä tekijöistä tehtyä tutkimusta. Tarkoituksena on tarkastella työntekijöiden toimintaan liittyviä tekijöitä, joiden on havaittu vaikuttavan organisaation tietoturvaan. Tässä tutkielmassa pohditaan sitä, mitkä työntekijän ominaisuudet vaikuttavat tietoturvakäyttäytymiseen ja mitkä asiat työympäristössä vaikuttavat käyttäjien asenteisiin ja toimintaan. Tutkimusmenetelmänä hyödynnetään kirjallisuuskatsausta, joka kohdistuu tietoturvakulttuurin, -käyttäytymisen ja –ohjeistuksen tutkimuksiin. Kirjallisuuskatsauksen avulla kartoitetaan tutkimuksissa esiintyviä tekijöitä, jotka vaikuttavat työntekijöiden asenteeseen ja toimintaan tietoturvan suhteen. Löydöksenä esitetään tutkimusten tulokset kootusti ja annetaan yksittäisiä tutkimuksia laajempi kuvaus siitä, mitä organisaatioiden tulisi ottaa huomioon, kun he suunnittelevat omia tietoturvakoulutuksia ja -ohjeita.

Alussa esittelen tutkielmassa esiintyviä keskeisiä tietoturvakäyttäytymiseen liittyviä peruskäsitteitä. Sen jälkeen kuvaan tutkimusmenetelmää, jolla kirjallisuuden haku ja rajaus on toteutettu. Tutkimuksen tulosluvussa kuvaan kirjallisuuden pohjalta tietoturvakäyttäytymistä, siihen vaikuttavia tekijöitä ja vaikuttamiskeinoja. Tuon esille sekä tiettyjen käyttäjäryhmien jakamia piirteitä että yksittäisiä ominaisuuksia, kuten ohjeiden seuraamista ja käyttäjien osallistumista. Pohdintaluvussa kokoan yhteen esittelemiäni ominaisuuksia luokittelemalla tietoturvakäyttäytymistä selittävät tekijät neljään kategoriaan: käyttäjien, ohjeiden ja ympäristön ominaisuuksia, sekä johdon toiminta. Lisäksi annan ehdotuksia siitä, miten näitä löydöksiä voitaisiin hyödyntää käytännössä. Yhteenvetoluvussa esittelen, miten tätä aihetta voitaisiin tutkia tulevaisuudessa erityisesti kvalitatiivista tutkimusta hyödyntämällä.

2. Keskeiset käsitteet

Tässä kappaleessa esitellään tutkimuksen kannalta tärkeitä termejä. Tietoturva, tietoturvapolitiikat ja -käyttäytyminen ovat merkittävästi esillä tässä tutkimuksessa, mutta ne eivät ole yksiselitteisiä termejä, joten on tärkeää avata sitä, mitä niillä tässä tutkimuksessa tarkoitetaan.

2.1 Mitä on tietoturva?

Tietototurvaa on perinteisesti pidetty käsitteenä, joka kattaa vain tekniset tietoturvaratkaisut, kuten esimerkiksi haittaohjelmien aikaisen havaitsemisen (Zou, Gong, Towsley, & Gao, 2005) tai palvelunestohyökkäyksiltä puolustautumisen (Mirkovic & Reiher, 2004). Tietoturva on viime vuosien aikana noussut yhä tärkeämmäksi käsitteeksi, kun tietoturvahyökkäyksien määrä ja riippuvaisuus tekniikasta on kasvanut (Boss, Kirsch, Angermeier, Shingler, & Boss, 2009). Tietoturva on esimerkiksi määritelty toiminnaksi, joka suojelee tietoa ja sitä säilyttäviä ja käsitteleviä järjestelmiä (Johnson, 2014). Tietoa täytyy suojata ihmisten tekemiltä tahallisilta ja tahattomilta teoilta, mutta myös esimerkiksi luonnonkatastrofeilta, jotka voivat molemmat aiheuttaa suuria vahinkoja, joiden vaikutusta voidaan kuitenkin lieventää, kun tietoturva on hyvin toteutettu (Baskerville, Straub, & Goodman, 2008). On kuitenkin huomattu, että jos halutaan parantaa järjestelmien turvallisuutta, tulee kiinnittää huomiota myös ihmisläheisempiin tekijöihin ja luoda niistä saatujen tietojen avulla uusia tietoturvapolitiikkoja, sekä selvittää, miten saadaan yksittäiset käyttäjät seuraamaan niitä (Boss et al., 2009).

Kun tietoturvatutkimus perinteisesti keskittyy organisaatiokontekstiin, Lin ja Siposen (2011) mukaan tietoturvaa on myös lähdetty vasta myöhemmin tutkimaan enemmän kotikontekstissa, koska tietokoneiden käytön määrä kotona kasvaa nopeammin kuin koskaan. Vaikka kotikäyttöön tarvittava tietoturva jakaa paljon piirteitä organisaatioympäristön kanssa, niissä on myös eroja, jotka olisivat tarpeen ymmärtää ja niiden tutkimukseen tulisi kiinnittää enemmän huomiota. Kotikäytössä käyttäjä saa valita, miten hän hoitaa tietoturvansa ja koska tämä toiminta on vapaaehtoista, se voi erota siitä, miten sama henkilö toimii työympäristössä. Yhtenä esimerkkinä toimii esimerkiksi salasanan valinta, johon työpaikalla voi olla tarkat ohjeet, jotta salasanoista saadaan mahdollisimman turvallisia. Kotona käyttäjän ei kuitenkaan tarvitse seurata samoja ohjeita. Työpaikalla on myös usein saatavilla tukea asiantuntijoilta, joita ei kotiympäristössä ole. (Li & Siponen, 2011.)

Tietoturvan yksi perinteisimmistä määrittelytavoista on Whitmanin ja Mattordin (2009) mukaan C.I.A. -kolmio, joka jakaa tietoturvan kolmeen osaan, jotka ovat arvokkaita organisaatioille: confidentiality, integrity ja availability, eli luottamuksellisuus, eheys ja saatavuus. Luottamuksellisuus tarkoittaa sitä, että tietoon pääsee käsiksi vain sellaiset henkilöt ja järjestelmät, joilla on oikeus siihen. Se on erittäin tärkeä silloin, kun käsitellään esimerkiksi henkilötietoja. Luottamuksellisuuden parantamiseksi käytetään keinoja kuten informaation luokittelu, jolloin vain oikean luokittelun omaava henkilö pääsee siihen käsiksi. Informaation turvallinen säilytys on myös tärkeää, koska luottamuksellisuus voi rikkoutua myös vahingossa, jos esimerkiksi työntekijä jättää tietylle tasolle luokitellun dokumentin näkyviin omalle työpöydälleen tai heittää sen roskiin ilman, että hän esimerkiksi silppuaisi sen. Eheys tarkoittaa sitä, että tieto on alkuperäistä ja siihen ei ole tehty oikeudettomia muutoksia. Sen pitää pysyä turvassa

vahingoilta, jotka muuttavat sen alkuperäistä tilaa, joka voi tapahtua esimerkiksi tietoa siirrettäessä. Useat virukset ovat suunniteltu juuri tietojen korruptointia varten, mutta korruptoituminen ei tapahdu kuitenkaan aina tahallisen haittateon takia, vaan se voi myös tapahtua esimerkiksi siirtoprosessin aikana useista eri syistä. Saatavuus tarkoittaa sitä, että tieto on saatavilla niille, jotka sitä tarvitsevat silloin, kun he sitä tarvitsevat. Vaikka tieto pitää olla suojattu henkilöiltä, joilla ei ole siihen oikeutta, pitää myös varmistua siitä, että ne joilla on siihen oikeus, pääsevät siihen käsiksi silloin, kun he sitä tarvitsevat. (Whitman & Mattord, 2009.)

Whitman ja Mattord (2009) kuitenkin kertovat, että C.I.A. kolmio on kuitenkin jäänyt ympäristön kehittyessä hieman vajaaksi ja myös muita ominaisuuksia on noussut näiden kolmen rinnalle, jotta pystyttäisiin paremmin arvioimaan uudenlaisia ominaisuuksia ja uhkia tietoturvalle. Accuracy eli tarkkuus, tarkoittaa sitä, että tiedon pitää olla virheetöntä ja sen pitää vastata sitä, mitä käyttäjä odottaa. Autenttisuus, eli tiedon pitää olla aitoa. Tätä rikotaan, kun esimerkiksi lähetetään huijaussähköposteja, joissa huijari esiintyy valheellisesti organisaationa, kuten pankkina ja pyytää käyttäjältä hänen tietojaan. Utility, joka tarkoittaa tässä tapauksessa tiedon hyödyllisyyttä. Tiedon tulee olla muodossa, jossa käyttäjä pystyy käyttämään ja hyödyntämään sitä. Possession eli hallussapito, jolla tarkoitetaan sitä, että informaatio on sellaisen henkilön hallussa, jolla on oikeus siihen. Tämä rikkoutuu usein luottamuksellisuuden kanssa, mutta on myös tilanteita, joissa tieto voi olla väärän henkilön hallussa, mutta koska se on suojattu, luottamuksellisuutta ei ole rikottu. (Whitman & Mattord, 2009.)

2.2 Mitä tarkoitetaan tietoturvapolitiikoilla?

Tietoturvapolitiikka on Hönen ja Eloffin (2002) määritelmän mukaan ohjelinja tietoturvaan organisaation sisällä. Se sisältää paljon erilaista informaatiota ja ohjeita siihen, miten tietoturvaa hoidetaan organisaatiossa. Näitä ovat esimerkiksi periaatteet eli säännöt sille, miten käyttäjien tulisi toimia. Eri käyttäjien roolit ja mitä vastuita kuuluu yksittäiselle käyttäjälle. Siinä myös kerrottaan miten toimitaan, jos havaitaan käyttäjiä, jotka eivät noudata annettuja ohjeita. Siinä tulee myös olla kerrottu mikä on tietoturvan tavoite ja miksi sitä tarvitaan. (Höne & Eloff, 2002.)

Myös ISO/IEC27001 ja ISO/IEC 27002 standardit kuvaavat tietoturvapolitiikkojen sisältöä hyvin samansuuntaisesti. ISO/IEC27001 kuvaa politiikkoja ryhmänä tietoturvakäytäntöjä, jotka johdon tulee määritellä ja hyväksyä, sekä jakaa ja kommunikoida työntekijöille ja relevanteille ulkoisille osapuolille. ISO/IEC 27002 standardin mukaan politiikkojen tulisi kohdistaa organisaation lähestymistapa heidän tietoturvansa hallitsemiseen. (Niemimaa & Niemimaa, 2017.)

Tietoturvapolitiikkoja on myös tutkittu eri näkökulmista, kuten esimerkiksi kuinka teoriassa toimivia ratkaisuja voidaan implementoida paremmin käytäntöön. Yhden kuvauksen mukaan politiikat tulee ikään kuin kääntää toiselle kielelle, kun kirjoitettu politiikka otetaan käyttöön. Tämän käännöksen tehtävä on sovittaa muualla hyväksi havaitut toimintatavat omalle organisaatiolle sopiviksi ja laittaa ne käytäntöön. (Niemimaa & Niemimaa, 2017.) Doherty ja Fulford (2005) tutkivat politiikkojen vaikutusta sen kannalta, onko organisaatiolla edes olemassa selkeät tietoturvapolitiikat, kuinka vanhoja ne ovat ja kuinka usein niihin tulee muutoksia. Huomioitavaa näissä tuloksissa oli se, että sillä oliko organisaatiolla käytössä selkeä tietoturvapolitiikka, ei havaittu olevan tilastollista yhteyttä tietomurtojen kanssa. He myös huomasivat sen, että organisaatioissa, joissa oli ollut tietoturvapolitiikka käytössä jo pitkään, eivät olleet sen

paremmin suojautuneita. Tähän syynä ainakin osaksi voisi olla se, että osa organisaatioista voi jäädä liian tyytyväiseksi itseensä politiikan käyttöönoton jälkeen ja kuvittelevat sen toimivan ilman jatkuvaa huomiota. Heidän tuloksista käy ilmi myös se, että organisaatioissa joissa tietoturvapolitiikkaa päivitettiin useammin, se myös toimi tehokkaammin. (Doherty & Fulford, 2005.)

Whitman ja Mattord (2009) määrittelevät tietoturvapolitiikkoja neljälle eri tasolle. Ensimmäinen taso on yleiset turvallisuuspolitiikat, jotka rajaavat organisaation strategisen tason lähestymistapaa tietoturvaan, sekä kertovat tietoturvan tärkeydestä organisaatiolle. Toisella tasolla ovat suunnitteludokumentit, jotka ovat ikään kuin pohjapiirros sille, kuinka turvallisuutta analysoidaan, suunnitellaan ja implementoidaan. Kolmas taso kattaa tarkemmin toteutukset ja sovellukset, joista käyttäjien tulisi olla tietoisia. Neljäs taso kertoo tarkasti sen, miten käyttäjien tulisi käyttää yksittäisiä järjestelmiä. Näihin voi lukeutua esimerkiksi asetuksien määrittely tai järjestelmän kirjautumiseen liittyvät ohjeet. (Whitman & Mattord, 2009.) Tässä tutkimuksessa tietoturvapolitiikoilla tarkoitetaan Hönen ja Eloffin (2002) mukaisesti organisaation sisäisiä ohjeita ja sääntöjä, joiden mukaan käyttäjien tulisi toimia ja sisältävät periaatteet, joiden mukaan organisaation toimii, kun niitä ohjeita ei seurata.

2.3 Mitä on tietoturvakäyttäytyminen?

Yksi tärkeimmistä tietoturvaan liittyvästä käyttäjien toiminnasta on tietoturvapolitiikkojen tai muiden vastaavanlaatuisten tietoturvaohjeiden seuraaminen. Ongelmana on kuitenkin se, että vaikka organisaatio olisi asettanut ohjeet käyttäjien toiminnalle, käyttäjät eivät usein seuraa niitä. (Pahnila, Siponen, & Mahmood, 2007.)

Käyttäjät tekevät virheitä, jotka eivät kuitenkaan ole aina tahallisia, vaan voivat johtua esimerkiksi tiedon puutteesta. Näitä virheitä olisi tarpeen korjata, koska nykyään hakkerit eivät kohdista iskujaan ainoastaan järjestelmiin vaan myös ihmisiin, joiden on huomattu olevan usein tietoturvan heikoin lenkki. (Safa, Solms, & Furnell, 2016.) Yksi tutkimus esimerkiksi ehdottaa tietoturvakäyttäytymisen luokitteluun kaksiakselista taulukkoa, joka on esitetty suomennettuna Kuvassa 1, jossa ohjeiden noudattaminen kasvaa vasemmalta oikealle ja tietoturvaan liittyvä osaaminen kasvaa alhaalta ylös. Se luokittelee tietoturvakäyttäytymisen neljään kategoriaan: 1) ohjeita huonosti seuraavat ja vähän tietävät ovat varomattomia (oblivious), 2) korkean tiedon omaavat, mutta silti ohjeita huonosti seuraavat ovat kapinallisia (rebellious), 3) ohjeita hyvin seuraavat, mutta vähän tietävät ovat tottelevaisia (obedient) ja 4) paljon tietävät ja myös hyvin ohjeita seuraavat ovat arvostelukykyisiä (discerning). (Ahmad, Norhashim, Song, & Hui, 2016.)

Kuva 1. Tietoturvakäyttäytymisen typologia (Ahmad et al., 2016)

Organisaatiot eivät kuitenkaan saa täysin sivuuttaa sitä näkökulmaa, että käyttäjät voivat toimia myös tahallisesti väärin, esimerkiksi henkilökohtaisen taloudellisen hyödyn saavuttamiseksi. Tätä ilmiötä kutsutaan kirjallisuudessa tietotekniikan väärinkäytöksi tai tietokonerikollisuudeksi (computer misuse, computer abuse tai computer crime). Tämä näkökulma on tärkeä ottaa huomioon, sillä useat tutkimukset ovat todenneet, että suurimmat uhat ovat usein organisaation sisäisiä. Työntekijöillä saattaa myös kehittyä motivaatiota organisaatiolle haitalliseen toimintaan johtuen esimerkiksi erimielisyyksistä työpaikalla. Työntekijän on mahdollista käyttää väärin asemaansa organisaatiossa tavalla, joka ei ole ulkopuoliselle mahdollista. Tämän vuoksi jo yhden työntekijän haitallinen toiminta voi olla erittäin haitallista organisaatiolle. Työntekijät saattavat myös käyttää asemaansa väärin tilanteissa, joissa he kokevat itsensä väärin kohdelluksi ja yrittävät vain korjata tilannetta, mihin he kokevat olevansa oikeutettuja. Esimerkkinä tästä voisi olla tilanne, jossa toinen työntekijä saa tietää kollegansa saavan enemmän palkkaa, vaikka hän kokee, että heidän panostuksensa työhön on sama. Tällöin heidän tarkoituksena ei välttämättä ole suoranaisesti aiheuttaa vahinkoa organisaatiolle ja he voivat esimerkiksi vakuuttaa itsensä siitä, että organisaatio ansaitsi tämän teon. (Willison & Warkentin, 2013.) Näistä syistä tutkijat ovat myös etsineet keinoja soveltaa perinteisten rikosten tutkimukseen käytettyjä menetelmiä IT ympäristössä. Vaikka erilaisia turvakeinoja sisäisen haittateon estämiseksi on myös tutkittu, nämä menetelmät voisivat avata tutkijoille uusia näkökulmia tähän ongelmaan ja näin auttaa kehittämään uusia ratkaisuja vähentämään sisäisiä uhkia ja niiden potentiaalista vaikutusta. (Willison, 2006.)

Tärkeä osa tietoturvakäyttäytymisen parantamista on tietoturvatietoisuuden parantaminen, koska tietoturvaratkaisut eivät auta, jos ihmiset eivät käytä niitä. Suositeltuja tietoturvaratkaisuja voidaan myös tulkita ja käyttää väärin, joka voi poistaa niistä saadun hyödyn. Tietoisuuden parantamisella pyritään minimoimaan käyttäjälähtöisiä ongelmia ja samalla saada suurin mahdollinen hyöty irti teknisistä tietoturvaratkaisuista. Tätä varten tulisi luoda tietoturvatietoisuuden parantamiseen keskittyvä ohjelma, jonka tehtävä on parantaa tietoturvatietoisuutta suunnitelmallisesti organisaatiotasolla. Ohjelmaa tulisi lisäksi kehittää jatkuvasti keräämällä palautetta ja mittaamalla ohjelman vaikutusta. Tietoisuuden parantamiseen liittyy kaksi tärkeää kategoriaa: kehys ja sisältö. Kehyskategoria kattaa järjestelmällisen puolen tietoisuuden parantamiseen ja sen pystyy pohjustamaan tehtyyn tutkimukseen ja hyviksi todettuihin ratkaisuihin. Sitä kuvataan ”insinöörillisten periaatteiden” kategoriana, jota voidaan kehittää olemassa olevien standardien ja ”parhaiden käytäntöjen” pohjalta. Sisältökategorian kehittämiseen on organisaatioissa panostettu vähemmän ja sen kehittäminen onkin haastavaa, koska sisällön suunnitteluun ei välttämättä voida löytää suoraa ratkaisua aikaisemmasta tutkimuksesta. Sisältöön kuuluu esimerkiksi sen määrittely, kuinka motivoidaan työntekijät seuraamaan annettuja ohjeita. Sisällön määrittely on tärkeää, koska ilman sitä kehysosiossa määritellyt ratkaisut eivät välttämättä toteudu ollenkaan. Jos käyttäjiä ei saada seuraamaan ohjeita, niin niiden kehitykseen käytetyt resurssit ovat menneet hukkaan. (Siponen, 2000.)

Tämä tutkimus on rajattu käsittelemään tietoturvaan ja tietoturvapolitiikkojen noudattamiseen liittyvää käyttäjien toimintaa ja ominaisuuksia organisaatioissa. Aiemmin mainitun typologian pohjalta (Ahmad et al., 2016) keskitytään kahden tyyppisen tietoturvakäyttäytymisen selittämiseen ja parantamiseen. Tutkielmassa yritetään löytää vastauksia sille, miten tottelevaisuutta ja osaamista voitaisiin parantaa. Käsitelty materiaali keskittyy käyttäjien toimintaan ja asenteisiin sekä siihen, miten niihin vaikuttavat esimerkiksi annetut ohjeet, koulutus ja ympäristö. Tutkielmassa ei kiinnitetä

huomiota teknisiin tietoturvaratkaisuihin, kotikäyttöön ja tietotekniikan tahalliseen väärinkäyttöön keskittyviin tutkimuksiin.

3. Tutkimusmenetelmä

Materiaalia kirjallisuuskatsaukseen etsiessä pääpaino oli organisaatioiden työntekijöiden käyttäytymisessä tietoturvan suhteen. Haun ulkopuolelle rajattiin tekniset tietoturvaratkaisut, kuten organisaatioissa käytettävät salaus- ja todennusmenetelmät, koska vaikka ne vaikuttavat työntekijöiden käyttäytymiseen, ne eivät ole lähtöisin heistä itsestään. Kirjallisuuden rajaamisessa keskityttiin siihen, miten erilaisten työntekijöiden käyttäytyminen eroaa toisistaan ja mitkä tekijät luovat nämä erot. Haku aloitettiin yksittäisellä fraasilla ”information security behaviour”, jonka avulla löydettiin yksittäisiä termejä kuten, policy, awareness ja compliance, joita kaikkia löytyy eri tavalla käytettyinä tietoturvakäyttäytymisestä tehdystä tutkimuksesta. Tässä vaiheessa otettiin mukaan tarkennus organisaatioihin, koska tutkimusta on tehty myös kotikäyttäjistä. Lisäksi tuloksia rajattiin etsimällä empiiristä tutkimusta, jota haettiin hakusanoilla kuten ”qualitative” ja ”empiric”. Suurin osa tuloksista löydettiin Scopus tietokannasta, joka oli erityisen hyvä, kun etsi käyttäytymiseen liittyvää materiaalia tietoturvasta. Myös IEEE Xplore Digital Librarya käytettiin, mutta sen käyttöliittymä ja usein liian teknisiin asioihin keskittyvä materiaali jätti sen käytön vähäisemmäksi.

4. Tulokset

Koska tietojärjestelmien määrä kasvaa jatkuvasti ja organisaatiot luottavat niihin yhä enemmän, on noussut tarve keksiä parempia suojauskeinoja tietoturvariskien vähentämiseksi (Dang-Pham, Pittayachawan, & Bruno, 2017a). Useat tutkimukset ovat todenneet, että käyttäjät ovat suurin riskin kohde organisaatioiden tietoturvallisuudessa, jota on pyritty parantamaan useilla eri keinoilla, kuten tietoturvatietoisuuden (information security awareness) parantamisella (Bauer et al., 2017). Tämä on johtanut siihen, että myös ihmisten käyttäytymiseen liittyvää tutkimusta on tehty tietoturvaan liittyen, kun on yritetty selvittää, mitkä asiat johtavat tietoturvasäädöksien ja ohjeiden seuraamiseen (Kim & Kim, 2017). Vuonna 2002 tehdyn tutkimuksen mukaan enemmistö tutkituista organisaatioista oli ilmoittanut suurimmaksi huolenaiheekseen ulkoiset uhat, vaikka useat tutkijat ovat sitä mieltä, että jopa 75% uhista tulisi organisaation sisältä (Willison & Backhouse, 2006).

Tutkimuksissa on todettu, että asioilla, kuten tietotekniikan roolilla työtehtävässä on merkitystä siihen, kuinka käyttäjä suhtautuu tietoturvaan, minkä takia tietoturvakoulutusta suunniteltaessa tulisi ottaa huomioon, kuinka eri käyttäjäryhmille saataisiin paremmin heidän rooliaan vastaava koulutus. On esimerkiksi huomattu, että käyttäjät, jotka eivät käytä aktiivisesti tietotekniikkaa työtehtävässään, saavat myös huonompia tuloksia tietoturvaohjeiden seuraamista parantavista ratkaisuisista. (Kim & Kim, 2017.) Käyttäjien näkemys tiettyjen toimenpiteiden pakollisuudesta on myös todettu vaikuttavaksi tekijäksi, koska käyttäjät voivat usein olla välinpitämättömiä tietoturvaa kohtaan, elleivät he koe siihen liittyviä käytäntöjä välttämättömiksi (Boss et al., 2009). Yksi merkittävä syy käyttäjien huonolle toiminnalle on kuitenkin tietämättömyys, koska on yleistä, että käyttäjät olisivat motivoituneita tekemään itsenäisiä tietoturvatoimia, mutta he eivät osaa tai eivät ole tietoisia niistä. (Albrechtsen, 2007).

Käyttäjien tietämättömyys tietoturvaohjeista voi johtua kiinnostuksen puutteen lisäksi myös ohjeiden vaikeasta saatavuudesta tai ymmärrettävyydestä, joka taas johtuu käyttäjien erilaisista tietotekniikan taidoista, kun verrattaan niihin, jotka suunnittelevat ohjeita (Bauer et al., 2017). Ohjeiden tulisi sisältää kyseiselle ryhmälle sopivaa kieltä, koska ohjeiden suunnittelija, osaa esimerkiksi tietoteknisen termistön usein paljon paremmin, kuin se työntekijä, jolle ohjeet on suunnattu. Ohjeita tulisi olla myös sopiva määrä, jotta saataisiin käyttäjät paremmin ymmärtämään ja lukemaan ne. (Pahnila et al., 2007.) Myös ominaisuuksien kuten sukupuoli ja ikä, on havaittu vaikuttavan siihen, miten käyttäjät suhtautuvat tietoturvaan, joten niitäkin voitaisiin miettiä, kun suunnitellaan organisaation omaa koulutusta (Ahmad et al., 2016). Samassa tutkimuksessa todettiin myös, että vahva tietotekninen osaaminen ei johda siihen, että ohjeita seurataan, vaan yleensä se johtaa tapauksiin, jossa käyttäjä on joko erittäin vahvasti tai heikosti ohjeita seuraava ääripää. Toisaalta taas huomattiin, että esimerkiksi naiset tietoteknisestä osaamisestaan riippumatta seurasivat ohjeita paremmin. Sen sijaan alle 30- tai yli 50-vuotiaat miehet, joilla oli vähäisemmät akateemiset saavutukset, seurasivat ohjeita yleensä huonosti ja muutenkin johdon alapuolella olevilla työntekijöillä oli yleensä heikompi tietämys tietoturvasta. (Ahmad et al., 2016). Joissain organisaatioissa on ollut myös tilanteita, joissa organisaation tietoturvaohjeita on päivitetty, mutta siitä ei ole koskaan informoitu työntekijöitä. Ongelmana on myös, että vaikka ne olisivat saatavilla, niin käyttäjät eivät lue ohjeita, joko niiden suuren määrän tai oletuksen, että he käyttäytyvät niin kuin he olettavat ohjeiden olevan. (Albrechtsen, 2007.)

Jos tietoturva koetaan asiana, joka vaatii lisää työtä normaalin työpanoksen lisäksi, sitä toteutetaan huonommin, kuin tilanteissa, joissa se nähdään kuuluvan normaaliin toimintaan (Boss et al., 2009). Albrechtsenin (2007) tutkimuksessa yksi tutkitun pankin työntekijä esimerkiksi totesi, että tietoturva ei kuulu hänen työhönsä, vaan hän luottaa olemassa oleviin turvallisuusmenetelmiin ja että hänen työntekonsa kärsisi, jos hän joutuisi huolehtimaan myös tietoturvasta (Albrechtsen, 2007). Tämän takia täytyy muistaa, kun koulutetaan käyttäjiä, että kun he tietävät mitä tehdään, tulisi heidän myös jollain tasolla tietää miksi näin tehdään. Jos ohje ohjaa käyttäjän askel askeleelta ja yhden askeleen ohittaminen ei aiheuta heti näkyvää ongelmaa, käyttäjä voi helposti ohittaa sen myös tulevaisuudessa. Toisaalta, jos ohje on hyvin räätälöity tietylle ryhmälle ja he ymmärtävät sen merkityksen, käyttäjät voivat käyttää myös omaa maalaisjärkeään toiminnassaan. (Kearney, 2010.) Työntekijöille on tärkeää, että he kokevat olevansa luotettavia, jonka pitää näkyä myös siinä, miten heitä ohjeistetaan, koska huonot ohjeet voivat saada työntekijät kokemaan, että heitä kohdellaan alentavasti tai kuin lapsia, joka vaikuttaa heidän asenteeseen (McIlwraith, 2006). Tietoturva on myös konfliktissa toiminnallisuuden kanssa ja esimerkiksi töissä, joissa käyttäjät saavat palkkansa myyntilukujen perusteella, tietoturva jää helposti prioriteeteissa jälkeen. Toinen yleinen ongelma voi olla liiallinen työn vaikeutuminen esimerkiksi salasanojen määrässä ja vaikeudessa, joka johtaa käyttäjät turvautumaan Post-it lappuihin tai muihin keinoihin, jotka voivat kumota niiden tietoturvamenetelmien vaikutuksen, joita varten apukeinoja on alun perin tarvittu. (Albrechtsen, 2007.)

Siponen ja Vance (2010) tutkivat ohjeiden rikkomista neutralisaatiotekniikoiden näkökulmasta, joita on alun perin käytetty selittämään sitä, miksi sekä rikolliset, että lainkuuliaiset kansalaiset rikkovat sääntöjä tai lakeja, vaikka molemmat ryhmät kuitenkin uskovat yleisesti yhteisöllisyyteen ja sen arvoihin. Ensimmäinen tekniikka on vastuun kieltäminen, jossa tekijä ei ota vastuuta tekemästään teosta, vaan selittää sitä itselleen esimerkiksi sillä, että hän ei pystynyt vaikuttamaan siihen tai sillä, että ohjeet olivat epäselvät. Toinen tekniikka on vahingon kieltäminen tai vähättely, jossa käyttäjä voi selittää, että tietokoneelle aiheutettu vahinko ei ole vakavaa, koska se ei aiheuta suoranaisesti vahinkoa kenellekään. Tarpeellisuuden puolustaminen on myös yksi tekniikka, kuinka käyttäjä voi selittää tekoansa, koska hän on kokenut, että teko oli tarpeellinen ja ainoa vaihtoehto. Käyttäjä voi myös syyttää sitä osapuolta, joka syyttää häntä sääntöjen rikkomisesta ja selittää sitä esimerkiksi sillä, että asetetut säännöt olivat sopimattomia, jonka takia se ei ollut hänen vikansa. Hän voi myös kokea, että sääntöjen rikkominen on ainut keino saada hänen työnsä tehtyä. Näille eri tekniikoille on ehdotettu myös eri keinoja, joilla niitä voitaisiin parantaa organisaatioympäristössä. Vastuun välttelyä ja tarpeellisuuteen vetoamista voidaan esimerkiksi yrittää vähentää käymällä keskusteluja ja ottaa koulutuksissa esille se, että politiikkojen rikkomiselle ei ole tekosyitä ja vaikka käyttäjät eivät ymmärtäisi täysin politiikkojen tarkoitusta, niiden noudattaminen on ehdotonta. Vahinkoa vähätteleville käyttäjille on tärkeä tehdä selväksi, mitä heidän toimistaan on seurannut, koska ne eivät ole välttämättä selviä hänelle suoraan. On myös tärkeää tehdä selväksi, että politiikkojen rikkominen on aina käyttäjän oma valinta, josta hän on vastuussa. Tulisi myös varmistaa, että esimerkiksi eri ryhmien tai osastojen johtajat eivät kannustaisi alaisiaan rikkomaan sääntöjä tehokkuuden parantamiseksi. (Siponen & Vance, 2010.)

Tang et al. (2016) mukaan asenteisiin tietoturvaa kohtaan voi vaikuttaa myös koko organisaation sisäinen kulttuuri ja on ehdotettu, että samoja organisaatiokulttuurin piirteitä jakavissa organisaatioissa, on myös samankaltaisuuksia tietoturvakulttuurissa. Heidän tutkimuksensa mukaan organisaation asenne ei saa olla liian rento, koska vapaammin toimivissa ympäristöissä tietoturvaan kiinnitetään vähemmän huomiota jopa johtotasolla. Tutkimuksessa ehdotetaan myös, että organisaatiot, joissa käyttäjät kokevat

itsensä ennemmin sen jäseniksi, eivätkä oman ammattinsa edustajina, seurataan paremmin ohjeita ja sääntöjä. Niissä ei kuitenkaan pidetä tietoturvaa niin tärkeässä asemassa, kuin ammattipohjaisissa organisaatioissa. He myös löysivät eroja organisaatioissa, jotka ovat enemmän normatiivisia, eli uskovat vahvasti ohjeiden ja periaatteiden seuraamiseen. Näissä organisaatioissa ohjeita seurataan yleensä hyvin. Toisaalta on myös olemassa organisaatioita, joissa suositaan pragmaattisempaa tapaa, eli ohjeita ja käytäntöjä pidetään vähemmän tärkeinä. Näissä organisaatioissa käyttäjät priorisoivat asiakkaiden tarpeiden täyttämisen, vaikka se olisi osittain ohjeita vastaan. Tällaisissa organisaatioissa käyttäjiä pidetään myös harvemmin vastuussa näistä rikkomuksista, kuin sellaisissa joissa ohjeiden noudattamista pidetään tärkeämpänä. (Tang et al., 2016.) Organisaation sisällä johdon tuki tietoturvalle ja työpaikalle kehittyneet normit ovat tärkeässä asemassa vaikuttamassa siihen, miten käyttäjät suhtautuvat tietoturvaan. Normien vaikutus kuitenkin vaihtelee erilaisten organisaatioiden välillä ja esimerkiksi poliisityössä ja uskonnollisissa järjestöissä, niiden on havaittu vaikuttavan erittäin vahvasti. Toisaalta taas jo aiemmin mainituissa työpaikoissa, joissa työntekijät nähdään enemmän yksilöinä, niiden vaikutus on vähäisempi. (Cuganesan, Steele, & Hart, 2018.)

Tietoturvaratkaisujen suunnittelijoiden olisi myös hyvä huomioida organisaation oman kulttuurin lisäksi myös kansallinen kulttuuri. Esimerkiksi vietnamilaisessa yhtiössä toteutetussa tutkimuksessa todettiin, että käyttäjät hakevat paljon apua IT asiantuntijoilta. Tämä saattaa johtua ainakin osittain siitä, että paikallisessa kulttuurissa imagon ylläpitäminen on tärkeää, jolloin kollegoilta pyydetään harvemmin apua (Dang-Pham, Pittayachawan, & Bruno, 2017b). Kansallista kulttuuria voi olla vaikea määritellä, koska yhdestä maasta saattaa löytyä useita alaryhmiä esimerkiksi sosiaalisten tai poliittisten jakaumien mukaan, mikä johtaa eroihin heidän tavoissaan. Samalla täytyy myös huomioida se, että teknisistä tarpeista johtuvaan toimintaan, kulttuurilliset erot ovat havaittu vaikuttavan vähemmän, joten kansallisen kulttuurin vaikutus ei välttämättä vaikuta yhtä vahvasti tietoturvaan, kuin moneen muuhun toimintaan. Kulttuurin vaikutus on myös havaittu merkittävämmäksi alemman tason työntekijöissä. Se näkyy esimerkiksi siinä, kuinka hyvä käsityskyky työntekijöillä on yleisesti teknologian suhteen. (Govender, Kritzinger, & Loock, 2016.)

Toisessa tutkimuksessaan Dang-Pham et al. (2017c) käsittelivät sitä, miten käyttäjät organisaation sisällä jakavat apua ja ohjeita tietoturvan suhteen. He totesivat, että käyttäjät, joilla on positiivisempi asenne tietoturvatoimien tekemiseen, myös jakavat enemmän apua kollegoilleen. Toisaalta taas käyttäjät, jotka kokevat turvatoimet tärkeäksi sosiaalisen ympäristön luoman paineen takia, jakavat ohjeita vähemmän. Tätä on selitetty mahdollisesti sillä, että se loisi heille lisää painetta, jos tietoturva olisi laajemmin esillä organisaatiossa. He myös tutkivat sitä, keneltä käyttäjät lähtevät useimmiten kysymään apua tietoturvatoimissa ja suurin osa otti ensimmäisenä yhteyttä niihin henkilöihin, jotka ovat heitä aiemmin auttaneet tietoturvaongelmissa. Seuraavana tulivat käyttäjän luotetut työkaverit ja kolmantena sellaiset henkilöt, joilta he saivat yleensä muita ohjeita työhönsä liittyen. (Dang-Pham, Pittayachawan, & Bruno, 2017c.)

Yksi tavoista parantaa käyttäjien ohjeiden seuraamista, on yrittää tehdä siitä tapa, jonka on todettu vaikuttavan siihen, kuinka käyttäjät tottelevat ohjeita, koska palkitseminen tai rankaiseminen eivät ole joidenkin tutkimuksien mukaan tarpeeksi vaikuttavia tekijöitä. Jotta ohjeiden seuraaminen saataisiin tehtyä tavaksi, olisi hyvä, että käyttäjät kokisivat positiivista ryhmäpainetta johtajilta, omalta esimieheltään, vertaisiltaan, sekä IT-ammattilaisilta, koska ympäristön on todettu vaikuttavaksi tekijäksi yksilön toimintaan. (Pahnila et al., 2007.) Hyvästä toiminnasta palkitseminen on joissain tutkimuksissa todettu vaikuttavan vähemmän tietoturvaohjeiden seuraamisessa, kuin monissa muissa

kontekseissa, koska yleensä niihin on liittynyt johdon asettamien tavoitteiden ylittämistä, mikä on tietoturvakontekstissa vaikeaa. Tämän takia voitaisiin keskittyä ohjeisiin, joista selviää mitä tapahtuu, kun ohjeita ei seurata, hyvästä toiminnasta palkitsemisen sijaan. (Boss et al., 2009.) Toisessa tutkimuksessa todettiin, että rangaistuksella voi olla joissain tapauksissa jopa negatiivisia vaikutuksia ohjeiden seuraamiseen, mutta jos käyttäjät kokivat, että he jäävät todennäköisesti kiinni rikkoessaan ohjeita, he myös seurasivat niitä paremmin. Nämä tulokset ovat kuitenkin vaihtelevia eri tutkimusten välillä. (Herath & Rao, 2009.) Yhdessä tutkimuksessa on todettu, että käyttäjien halukkuus tehdä vastoin ohjeita voi kasvaa, jos he kokevat, että he pystyvät välttämään asetetun rangaistuksen (Bénabou & Tirole, 2003). Toisessa tutkimuksessa taas on todettu, että jos käyttäjät ovat tietoisia tietoturvapoliitikoista, he tulevat todennäköisesti tekemään vähemmän tietoturvarikkomuksia, mutta rangaistuksen vahvuus vaikuttaa siihen, kuinka tehokasta tietoisuuden parantaminen on. Siinä oli toisaalta myös ristiriitaisia ajatuksia siitä, että vaikuttaako rangaistuksen varmuus väärinkäyttöön ja yhtenä syynä sille annettaan se, että tietoisuus politiikoista voi auttaa käyttäjiä ymmärtämään, kuinka vaikea väärinkäyttäjiä on saada kiinni. (D'Arcy, Hovav, & Galletta, 2009.)

Koska palkitseminen on erittäin paljon tutkittu alue, siitä löytyy myös paljon erilaisia tuloksia, joten on vaikea sanoa, että jokin tietty ratkaisu olisi oikea. Yhdessä tutkimuksessa on esimerkiksi todettu, että jos työstä on etukäteen määritelty jokin tietty palkkio, työntekijä voi kokea sen vieraannuttavana ja alentavana, mikä vähentää heidän kiinnostustaan ja vaikuttaa heidän asenteeseensa. Toisaalta taas, jos onnistumisen jälkeen annettaan palkkio, josta ei ollut etukäteen sovittu, työntekijä ei koe, että häntä olisi ohjattu tekemään työtä tietyllä tavalla ja palkitsija ei ollut pakotettu antamaan mitään ylimääräistä. Tämä antaa myös työntekijälle yhdenlaisen mittarin siitä, miten hän on onnistunut työssään. (Bénabou & Tirole, 2003.)

Myös käyttäjien ottamisella mukaan tietoturvaratkaisujen hallintaan, etenkin omaan roolinsa liittyvissä asioissa, on nähty vaikutusta heidän ymmärrykseensä säännöistä ja toimenpiteistä, mutta se myös mahdollistaa heiltä saatavan palautteen, jotta nämä ratkaisut saataisiin suunniteltua juuri heille sopiviksi. Tämän vuoksi, vaikka on tärkeää, että osa tietoturvatoimista toimii taustalla käyttäjille näkymättömissä, tulisi heidän myös päästä välillä itse osaksi tekemään niitä. Tällöin he tulevat myös tietoisemmiksi riskeistä ja syistä, minkä takia nämä toimet ovet olemassa. (Spears & Barki, 2010.) On todettu, että käyttäjien opettamisella on positiivisia vaikutteita heidän asenteisiin ja sitä myöten tietoturvaohjeiden seuraamiseen (Safa et al., 2016). Näiden lisäksi on myös todettu, että tietoturvasta kommunikointi voisi tapahtua samoja viestintäkanavia pitkin, kuin muukin kommunikaatio, jotta se saataisiin paremmin integroitua osaksi suurempaa kokonaisuutta. Samalla se voisi näyttää sen, että organisaation johto seisoo tietoturvapäätösten takana ja valvoo niiden noudattamista. (Puhakainen & Siponen, 2010.)

Yksi tutkittu käyttäjien toiminta on ohjelmien päivittäminen ja kuinka paljon käyttäjien liian hidas päivittäminen uhkaa tietoturvaa. Tutkimuksessa todetaan, että käyttäjien päivittäminen ei riipu siitä, mitä sisältöä päivityksessä on, joka on hyvä asia, koska moni käyttäjä voisi pitää päivityksiä, jotka eivät sisällä toiminallisia muutoksia, vähemmän tärkeinä. Siltikin ohjelmien päivittäminen tapahtuu usein hitaasti, jonka takia uusien uhkien torjuminen tapahtuu hitaammin ja järjestelmä on altis uhille pidemmän aikaa. Tätä voidaan parantaa esimerkiksi hiljaisilla eli taustalla toimivilla päivityksillä, joista käyttäjä ei ole tietoinen, mutta sekään ei onnistu poistamaan koko ongelmaa. Lisäksi tutkimuksessa huomattiin, että eri ohjelmilla on eroavia päivitysnopeuksia. Esimerkiksi ohjelmat, joiden vanhempien versioiden toiminnan tukeminen lopetetaan nopeammin, myös päivitetään nopeammin. (Sarabi, Zhu, Xiao, Liu, & Dumitraş, 2017.) Muita ratkaisuja, joilla käyttäjien päivittämishalukkuutta voitaisiin parantaa, olisi esimerkiksi

virustentorjuntaohjelmien kohdalla näyttää, kuinka paljon uhkia nykyinen järjestelmä on torjunut ja kuinka paljon uusia uhkia on olemassa, joita nykyinen versio ei vielä pysty torjumaan. Niiden ja myös muiden ohjelmien kohdalla voitaisiin myös näyttää, kuinka vanha nykyinen versio on verrattuna uusimpaan ja kuinka monta kertaa päivitystä on lykätty. Tällaiset keinot voisivat auttaa syyllistämään käyttäjää, jotta hän päivittäisi ohjelman. (Furnell, Khern-am-nuai, Esmael, Yang, & Li, 2018.)

Vaikka käyttäjien auttamisella ei voida koskaan parantaa kaikkien käyttäjien toimintaa, on silti havaittu, että oikeanlainen tuki ja auttaminen voivat johtaa haluttuun käytökseen. Tämän ei tarvitse aina tarkoittaa sitä, että käyttäjät ovat ymmärtäneet täysin, kuinka heidän käyttämänsä tietoturvaratkaisut toimivat ja miksi näin tehdään. Motivaatio käytöksen parantamiseen voi syntyä useista eri syistä ja sen merkitys ei ole välttämättä niin tärkeä, jos se auttaa käyttäjät toimimaan niin kuin organisaatio on todennut hyväksi. (Furnell et al., 2018.) Tietoturvapolitiikat, -koulutukset ja käyttäjien toiminnan valvonta ovat esimerkiksi kaikki todettu tekijöiksi, jotka vähentävät ainakin jollain tasolla käyttäjien riskiä tehdä tietoturvarikkomuksia. Politiikkojen kohdalla se voi tapahtua muuttamalla käyttäjien käsitystä väärinkäytön vakavuudesta ja koulutuksen ja valvonnan kohdalla vakavuuden lisäksi myös voidaan vahvistaa käsitystä siitä, kuinka todennäköisesti virheestä jää kiinni. Nämä ovat kuitenkin sellaisia tekijöitä, joita organisaatio voi hallita, mutta ne ovat vasta pieni osa tekijöistä, jotka vaikuttavat rikkomusten todennäköisyyteen. Käyttäjien moraalinen sitoutuminen on esimerkiksi tekijä, jonka on todettu vaikuttavan myös, mutta sitä on todella vaikea hallita, koska kaikilla ihmisillä on omat arvomaailmansa, joten niitä on vaikea yrittää muokata. (D'Arcy et al., 2009.)

5. Pohdinta

Tässä tutkielmassa oli tarkoitus esitellä tekijöitä, jotka vaikuttavat työntekijöiden käyttäytymiseen organisaatiossa koskien tietoturvaa. Eri tutkimukset käsittelevät tietoturvakäyttäytymistä eri näkökulmista ja määrittelevät sitä eri tavoin. Kaikille yhteisenä tavoitteena on parantaa käyttäjien toimintaa tietoturva-asioissa, mutta sitä on lähestytty useista eri näkökulmista.

Käyttäytymisen parantaminen tietoisuuden parantamisella on yksi usein toistuva tapa, mutta sitäkin on käsitelty eri näkökulmista. Tietoisuuden parantamista kampanjoilla ja koulutuksella on tutkittu, mutta myös sitä, miten käyttäjät kokevat ne ja kuinka vaikuttavia ne ovat (Bauer et al., 2017). Tulevaisuuden tutkimusmahdollisuuksia varten tietoturvakäyttäytymisestä on otettu esille sellaisia kategorioita, kuten eri kulttuurien vertaaminen, tarkoituksella haitallisen teon ja vahingossa tapahtuvan väärinkäytön erottaminen, sekä ohjeiden noudattamisen parantaminen (Crossler et al., 2013). Tietoturvapolitiikkojen noudattaminen on yksi paljon tutkittu ilmiö ja sitäkin on yritetty parantaa usein eri tavoin, koska ilman sitä, toteutetut tietoturvaratkaisut menettävät tehokkuutensa (Puhakainen & Siponen, 2010). Käyttäjien kouluttaminen (Puhakainen & Siponen, 2010), palkitseminen ja rangaistukset (Pahnila et al., 2007) ovat esimerkkejä vaihtoehdoista, joilla sitä on pyritty parantamaan.

Tahallaan aiheutettu haitta on alue, jota on tutkittu etenkin siitä näkökulmasta, kuinka näitä tekoja voidaan ehkäistä, koska syitä tällaiseen toimintaan voi olla monia (Willison & Warkentin, 2013). Vahingossa tapahtuvaa haitantekoa on myös tutkittu ja sille on löydetty syiksi esimerkiksi huolimattomuus ja inhimilliset virheet, joita ei voida kitkeä kokonaan pois, mutta niitä voidaan pyrkiä vähentämään (Furnell et al., 2018).

Taulukossa 1 tiivistetään tutkimuksen tulokset luokittelemalla tietoturvakäyttäytymistä selittävät tekijät neljään kategoriaan: käyttäjän ominaisuuksiin (13 kpl), ohjeiden ominaisuuksiin (9 kpl), ympäristön ominaisuuksiin (5 kpl) ja johdon toimintaan (11 kpl).

Taulukko 1. Yhteenveto tietoturvakäyttäytymistä selittävistä tekijöistä

Käyttäjien ominaisuuksia	**Ohjeiden ominaisuuksia**	**Ympäristön ominaisuuksia**	**Johdon toiminta**
Tietotekniikan rooli työtehtävässä (Kim & Kim, 2017)	Sopiva kieli (Pahnila et al., 2007; Bauer et al., 2017)	Organisaation kulttuuri (Tang et al., 2016) - toiminnanvapaus-aste - yksilöllisen jäsenyyden kokeminen - ammattipohjaisuus - normatiivisuus - pragmaattisuus - asiakkaiden tarpeiden priorisointi - käyttäjien vastuullisuus	Luodaan kuva, että työntekijöihin luotetaan (McIlwraith, 2006)

Käyttäjien ominaisuuksia	**Ohjeiden ominaisuuksia**	**Ympäristön ominaisuuksia**	**Johdon toiminta**
Demografiset ominaisuudet: Sukupuoli, ikä, koulutustausta, organisatorinen asema (Ahmad et al., 2016)	Sopiva määrä (Boss et al., 2009; Pahnila et al., 2007; Albrechtsen, 2007)	Kansallinen kulttuuri (Dang-Pham et al., 2017b; Govender et al., 2016) - imagon ylläpitäminen - kulttuurin vaikutus riippuu organisatorisesta asemasta ja teknologia-osaamisesta	Palkintojen ja rangaistusten asema (Pahnila et al., 2007; Boss et al., 2009; Herath & Rao, 2009; Bénabou & Tirole, 2003; D'Arcy et al., 2009)
Neutralisaatiotekniikoiden käyttö (Siponen & Vance, 2010) - vastuun kieltäminen - vahingon kieltäminen - tarpeellisuuden puolustaminen - syyttely - konflikti työtehtävän kanssa	Kuormittavuus (Kearney, 2010; Boss et al., 2009; Albrechtsen, 2007)	Sosiaalinen paine (Pahnila et al., 2007; Dang-Pham et al., 2017c)	Roolia vastaava koulutus työntekijöille (Kim & Kim, 2017)
Tavanomaisuus (Pahnila et al., 2007)	Informointi käyttäjille olemassaolosta ja muutoksista (Albrechtsen, 2007; Bauer et al., 2017)	Käyttäjien keskinäinen auttaminen ja ohjeiden jakaminen (Dang-Pham et al., 2017c)	Käyttäjien osallistaminen (Spears & Barki, 2010; Safa et al., 2016)
Tietotekninen osaaminen (Ahmad et al., 2016; Bauer et al., 2017)	Ohjeiden perusteleminen (Kearney, 2010)	Organisaation normit (Cuganesan et al., 2018)	Tietoturvakoulutus (Safa et al., 2016; D'Arcy et al., 2009))
Tietoturvatietoisuus (Bauer et al., 2017; Albrechtsen, 2007)	Sisältävät myös seuraukset ohjeiden rikkomisesta käyttäjälle ja organisaatiolle (Boss et al., 2009)		Johdon tuki tietoturvapolitiikoille (Cuganesan et al., 2018; Puhakainen & Siponen, 2010)
Tietoturvakontrollien kiertäminen (Albrechtsen, 2007)	Konfliktit työtehtävän kanssa (Albrechtsen, 2007)		Viestintäkanavat (Puhakainen & Siponen, 2010; Bauer et al., 2017)

Käyttäjien ominaisuuksia	**Ohjeiden ominaisuuksia**	**Ympäristön ominaisuuksia**	**Johdon toiminta**
Pakollisuuden kokeminen (Boss et al., 2009)	Epäselvä syy-seuraus-suhde (Kearney, 2010)		Noudattamisen valvonta (Cuganesan et al., 2018; Puhakainen & Siponen, 2010; D'arcy et al., 2009)
Motivaation puute (Bauer et al., 2017)	Kontekstin huomioiminen (Kearney, 2010)		Teknologinen tuki (Sarabi et al., 2016)
Noudattamisharha (Albrechtsen, 2007)			Teknologian haavoittuvuuden osoittaminen (Furnell et al., 2018)
Luottamus teknologiaan (Albrechtsen, 2007)			Käyttäjien virheiden osoittaminen (Furnell et al., 2018)
Vastuun kieltäminen (Albrechtsen, 2007)			
Moraalinen sitoutuminen (D'Arcy et al., 2009)			

Tietoturvakäyttäytymistä selittävistä tekijöistä tutkimuksessa löydettiin eniten käyttäjien ominaisuuksia (13 kategoriaa, ks. Taulukko 1). Käyttäjien ominaisuuksia, joita tulisi huomioida, kun kehitetään tietoturvaa ovat esimerkiksi tietotekniikan rooli työtehtävässä, sukupuoli, ikä, organisatorinen asema ja tietotekninen osaaminen. Nämä tekijät voivat vaikuttaa myös siihen, minkälaiset ohjeet heille tulisi suunnitella. Näiden kaikkien huomioon ottaminen on kuitenkin vaikeaa ja kaikkia ominaisuuksia ei voida yleistää jokaiseen ryhmän jäseneen, jonka takia käytännössä tällaisten ohjeiden suunnittelu yksittäisiä ryhmiä kohtaan on vaikeaa tai jopa mahdotonta. Tutkimuksessa nousi myös esille, että käyttäjien tietoisuuden, motivaation, moraalikäsitysten ja tapojen parantaminen on oleellinen osa tietoturvakäyttäytymisen kehittämistä. Tietoturvakoulutuksen suunnittelussa on lisäksi hyvä ottaa systemaattisesti huomioon tutkimuksessa esiin nousseita tietoturvan näkökulmasta haitallisia käyttäjien asenteita ja ajattelutapoja: neutralisaatiotekniikoiden käyttöä, noudattamisharhaa, luottamusta teknologiaan ja vastuun kieltämistä.

Tutkimuksessa löydettiin yhdeksän ohjeiden ominaisuuksiin liittyvää tekijää, jotka selittävät käyttäjien tietoturvakäyttäytymistä (ks. Taulukko 1). Ohjeiden tulisi sisältää kieltä, jota käyttäjät ymmärtävät ja ohjeiden määrän pitäisi olla sellainen, että käyttäjien on mahdollista sisäistää ohjeet realistisella perehtymisen määrällä. Ennen tätä tulisi tietenkin myös varmistaa se, että käyttäjät ovat tietoisia, mistä nämä ohjeet ovat saatavilla ja jos niihin tulee joskus muutoksia. Ohjeiden tulisi sisältää myös tietoa siitä, miksi asiat tehdään niin kuin ne on ohjeistettu. Oikeanlaiset ohjeet antaisivat käyttäjille kuvan myös siitä, että johto luottaa heihin ja he kokisivat itsensä paremmin osaksi organisaatiota. Se antaisi myös heille mahdollisuuden soveltaa omaa osaamistaan ja käyttää maalaisjärkeä.

Vääränlaisilla ohjeilla voi olla juuri päinvastainen vaikutus ja ne saavat käyttäjät hankaamaan vastaan entistä enemmän.

Ympäristöllä on myös vaikutusta siihen, kuinka käyttäjät toimivat ja tässä tutkimuksessa löydettiin viisi sen ominaisuutta, jotka voivat vaikuttaa käyttäjiin (ks. Taulukko 1). Organisaation sisäinen ja kansallinen kulttuuri voivat vaikuttaa käyttäjiin, koska eri puolilla maailmaa voidaan toimia tiettyjen asioiden suhteen eri tavoilla. Olisi hyvä, että käyttäjä tuntisi positiivista painetta muilta työntekijöiltä ja näkisi, että hänen toimintansa on tärkeää ja hän itse haluaa olla osa toimivaa organisaatiota. Käyttäjät jakavat myös ohjeita keskenään ja on havaittu, että jos käyttäjä näkee tietoturvan positiivisena asiana, hän myös jakaa enemmän apua muille työntekijöille siihen liittyen. Työpaikoille kehittyy myös usein sellaisia tapoja ja normeja, joita ei muilta työpaikoilta välttämättä löydy ja tämä vaikuttaa myös siihen, kuinka käyttäjät toimivat. Sen takia on tärkeää, että ei uskota yhteen universaaliin ratkaisuun, vaan otetaan hyväksi todettuja ratkaisuja ja sovitetaan ne omaan organisaatioon sopivalla tavalla.

Johdon toiminta on myös erittäin tärkeää onnistuneen tietoturvan kannalta ja tämän tutkimuksen aikana nousi esille 11 kategoriaa, jotka tulisi huomioida (ks. Taulukko 1). Heillä on paljon vastuuta, koska on heidän tehtävänsä varmistaa, että tietoturvakoulutusta järjestetään ja se on tehokasta. He ovat myös vastuussa tukipalveluiden hankkimisesta, jotta käyttäjät, jotka haluavat toimia oikein myös saavat apua, kun he sitä tarvitsevat. Heidän pitää myös viestiä tietoturvasta oikeita kanavia pitkin ja osoittaa, että ne eivät ole pelkkää puhetta, vaan he seisovat tehtyjen päätöksien takana. Käyttäjiä tulisi ottaa mukaan, kun kehitetään tietoturvaa ja opettaa heille siitä enemmän. Tällä voidaan myös varmistaa se, ettei tietoturva ole liian suuressa konfliktissa toiminnallisuuden kanssa. Rangaistukset ja palkitseminen tietoturva-asioissa on todettu joissain tutkimuksissa huonommin toimivaksi, kuin muissa ympäristöissä ja esimerkiksi kiinnijäämisen todennäköisyys voi vaikuttaa enemmän, kuin rangaistuksen vakavuus. Tämä asia ei kuitenkaan ole yksiselitteinen ja sitä tulisi käsitellä tilannekohtaisesti. Siihen voi vaikuttaa esimerkiksi se, että onko palkkio määritelty jo ennen työtä vai ilmoitetaanko siitä vasta sitten, kun työ on hyvin suoritettu. Heidän tulee myös pystyä osoittamaan käyttäjille heidän tekemiään virheitä ja niiden seurauksia, jotta heidät saataisiin vakuutettua tietoturvan tärkeydestä.

Jos näitä asioita otettaisiin huomioon, kun organisaatiot kehittävät omia tietoturvapolitiikkojaan ja suunnittelevat ohjeita käyttäjille, voitaisiin parantaa organisaatioiden tietoturvaa. Kun ei luoteta pelkästään teknisiin ratkaisuihin, vaan otettaisiin mukaan myös työntekijät, voitaisiin saada torjuttua enemmän uhkia ja estettyä uusien syntymistä käyttäjien toiminnan takia.

6. Yhteenveto

Tietoturvaa ei voida luottaa pelkästään teknisten ratkaisujen varaan, vaan huomiota tulee kiinnittää myös ihmisiin, jotka teknologian kanssa työskentelevät, koska heidän käyttäytymisensä on avannut uusia mahdollisuuksia uhille, joihin tekniset menetelmät eivät aina auta (Safa et al., 2016). Organisaatioissa, joissa toimii suuri määrä työntekijöitä, on vaikea varmistaa, että kaikki työntekijät osaavat ja ymmärtävät tietoturvakäytännöt, mutta oikeanlaisilla ohjeilla, jotka ovat oikeasti suunniteltu käyttäjille, tätä on pystytty parantamaan (Kearney, 2010). Käyttäjille pitäisi pystyä luomaan sellainen asenne, että tietoturva on osa heidän työtään (Pahnila et al., 2007).

Myös ympäristön vaikutusta käyttäjien toimintaan on tutkittu, mutta toistaiseksi se on usein rajoittunut yksittäisiin organisaatioihin, mutta eri kulttuureissa olevien organisaatioiden ja niissä olevien käyttäjien eroja on vertailtu vähemmän. Esimerkiksi Vietnamilaisessa yhtiössä (Dang-Pham et al., 2017b) ja suomalaisessa yhtiössä (Pahnila et al., 2007) tehdyt tutkimukset tutkivat samankaltaisia piirteitä organisaatioissa, mutta molempien tuloksiin voivat vaikuttavaa myös kansalliset piirteet, joita voitaisiin ottaa huomioon, kun näiden tuloksia vertaillaan. Huomioitavaa on kuitenkin se, että kansallista kulttuuria voi olla vaikea määritellä ja sen vaikutus tietoteknisessä työssä on havaittu vähemmän merkittäväksi (Govender et al., 2016).

Käyttäjät jättivät harvoin seuraamatta tietoturvaohjeita tarkoituksella, vaan sen on todettu yleensä johtuvan tiedon puutteesta tai ohjeiden liian vaikeasta ymmärrettävyydestä (Albrechtsen, 2007). Tämä kannustaisi tutkimaan lisää ohjeiden suunnittelua erilaisille osastoille ja eri rooleille niin, että käyttäjät oikeasti saisivat ohjeet, joista he ovat tietoisia ja joita he oikeasti ymmärtävät (Kearney, 2010). Sen lisäksi olisi hyväksi, jos työntekijät saisivat työympäristöstään positiivisia vaikutteita tietoturvasta, jolloin he itse alkaisivat toimimaan ohjeiden mukaan (Pahnila et al., 2007). Työstä palkitseminen tai virheistä rankaisu ovat molemmat vaihtoehtoja tietoturvakäyttäytymisen parantamiseen, mutta niistä saadut tulokset ovat vaihtelevia ja tilannekohtaisia, joten tulosten yleistäminen on vaikeaa. Vaikuttavia tekijöitä niiden tehokkuuteen ovat esimerkiksi se, onko palkkiosta kerrottu ennen työtä vai annetaanko se vasta hyvän suorituksen päätteeksi, rangaistuksen suuruus ja kiinnijäämisen todennäköisyys. (Bénabou & Tirole, 2003; Pahnila et al., 2007; Boss et al., 2009; Herath & Rao, 2009.)

Tämä tutkimus sisältää katsauksen suhteellisen pieneen määrään tutkimusta, jota on valittu usealta eri osa-alueelta, joten yksityiskohtiin ei päästy. Lisäksi kuten heti alussa on mainittu, tietoturvakäyttäytyminen on vielä suhteellisen uusi tutkimuksen ala, joten se kehittyy jatkuvasti. Laajempaa tutkimusta varten kirjallisuuskatsauksen tulisi olla systemaattinen ja sisältää enemmän artikkeleita, jotta saataisiin enemmän näkökulmia aiheeseen. Laajan ja systemaattisen näkökulman lisäksi tuleva tutkimus voisi keskittyä tarkastelemaan tietoturvakäyttäytymistä tarkkaan rajatuista näkökulmista, joista aikaisempaa tutkimusta ei vielä ole tehty riittävästi. Tutkimuksessa nousi esille tarve tarkastella tietoturvakäyttäytymistä muun muassa kulttuurillisten erojen näkökulmasta. Tutkimuksia on suoritettu hyvinkin erilaisissa kulttuureissa, mutta vähemmälle huomiolle on jäänyt kahden tai useamman kulttuurin välinen vertailu ja niiden vaikutukset tietoturvakäyttäytymiseen. Vaikka kulttuuria tutkiessa onkin pakko yleistää paljon, niin saadut tulokset voisivat antaa uusia näkökulmia siihen, ovatko tietynlaiset ongelmat esimerkiksi yleisempiä eri kulttuureissa. Myös kotikäytön ja työkäytön välistä yhteyttä voitaisiin tutkia lisää. Lisää tutkimusta voisi tehdä siitä, vaikuttaako kotikäytön määrä ja laatu siihen, kuinka käyttäjä toimii työympäristössä.

Kvalitatiivinen tutkimus on tapa, jolla pyritään kuvaamaan olemassa olevaa henkilöä, ryhmää tai ilmiötä ja antamaan laajemman kuvan tutkittavasta kohteesta, kuin kvantitatiivisessa tutkimuksessa. Siinä keskitytään tutkimuskohteen laadullisiin ominaisuuksiin ja pyritään vastaamaan siihen, millainen se on luonnollisessa ympäristössään. (Alasuutari, 2010). Jatkossa voitaisiin tehdä kvalitatiivista tutkimusta organisaatioiden sisällä olevista ryhmistä, joiden tietoturvataidot eroavat toisistaan ja yrittää löytää miten he luovat riskejä organisaation tietoturvalle ja kuinka niitä voitaisiin ehkäistä. Näitä tuloksia voitaisiin verrata aikaisempiin tutkimuksiin, jotka tunnistivat tietoturvakäyttäytymisen pohjalta ryhmiä organisaatioiden sisällä, joita on tässäkin tutkielmassa esitetty.

Lähdeluettelo

Ahmad, Z., Norhashim, M., Song, O. T., & Hui, L. T. (2016). A typology of employees information security behaviour. *2016 4th International Conference on Information and Communication Technology (ICoICT)*. doi:10.1109/icoict.2016.7571929

Alasuutari, P. (2010). The rise and relevance of qualitative research. *International Journal of Social Research Methodology,* 13(2), 139-155. doi:10.1080/13645570902966056

Albrechtsen, E. (2007). A qualitative study of users view on information security. *Computers & Security, 26*(4), 276-289. doi:10.1016/j.cose.2006.11.004

Anderson, B. B., Vance, A., Kirwan, C. B., Eargle, D., & Jenkins, J. L. (2016). How users perceive and respond to security messages: A NeuroIS research agenda and empirical study. *European Journal of Information Systems, 25*(4), 364-390. doi:10.1057/ejis.2015.21

Baskerville, R., Goodman, S. E., & Straub, D. W. (2008). *Information Security Policy, Processes, and Practices*. Armonk, NY: Routledge.

Bauer, S., Bernroider, E. W., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users non-compliance with information security policies in banks. *Computers & Security, 68*, 145-159. doi:10.1016/j.cose.2017.04.009

Bénabou, R., & Tirole, J. (2003). Intrinsic and Extrinsic Motivation. *The Review of Economic Studies, 70*(3), 489-520. doi:https://doi.org/10.1111/1467-937X.00253

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what Im asked: Mandatoriness, control, and information security. *European Journal of Information Systems, 18*(2), 151-164. doi:10.1057/ejis.2009.8

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*, 90-101. doi:10.1016/j.cose.2012.09.010

Cuganesan, S., Steele, C., & Hart, A. (2017). How senior management and workplace norms influence information security attitudes and self-efficacy. *Behaviour & Information Technology, 37*(1), 50-65. doi:10.1080/0144929x.2017.1397193

Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2017a). Applications of social network analysis in behavioural information security research: Concepts and empirical analysis. *Computers & Security, 68*, 1-15. doi:10.1016/j.cose.2017.03.010

Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2017b). Exploring behavioral information security networks in an organizational context: An empirical case study. *Journal of Information Security and Applications, 34*, 46-62. doi:10.1016/j.jisa.2016.06.002

Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2017c). Why employees share information security advice? Exploring the contributing factors and structural patterns of security advice sharing in the workplace. *Computers in Human Behavior, 67*, 196-206. doi:10.1016/j.chb.2016.10.025

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. doi:10.1287/isre.1070.0160d

Doherty, N. F., & Fulford, H. (2005). Do information security policies reduce the incidence of security breaches: An exploratory analysis. *Information Resources Management Journal, 18*(4), 21-39.

Furnell, S., Khern-Am-Nuai, W., Esmael, R., Yang, W., & Li, N. (2018). Enhancing security behaviour by supporting the user. *Computers & Security, 75*, 1-9. doi:10.1016/j.cose.2018.01.016

Govender, S., Kritzinger, E., & Loock, M. (2016). The influence of national culture on information security culture. *2016 IST-Africa Week Conference*. doi:10.1109/istafrica.2016.7530607

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. doi:10.1016/j.dss.2009.02.005

Höne, K., & Eloff, J. (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

Johnson, R. (2015). *Security policies and implementation issues*. Burlington, MA: Jones & Bartlett Learning

Kearney, P. (2010). *Security: The human factor*. Ely: IT Governance Publishing.

Kim, S. S., & Kim, Y. J. (2017). The effect of compliance knowledge and compliance support systems on information security compliance behavior. *Journal of Knowledge Management, 21*(4), 986-1010. doi:10.1108/jkm-08-2016-0353

Li, Y., & Siponen, M. (2011). A Call For Research On Home Users' Information Security Behaviour. *PACIS 2011, 112*. doi:https://aisel.aisnet.org/pacis2011/112

McIlwraith, A. (2006). *Information security and employee behaviour how to reduce risk through employee education, training and awareness*. Aldershot, England: Gower.

Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review, 34*(2), 39. doi:10.1145/997150.997156

Niemimaa, E., & Niemimaa, M. (2017). Information systems security policy implementation in practice: From best practices to situated practices. *European Journal of Information Systems, 26*(1), 1-20. doi:10.1057/s41303-016-0025-y

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees Behavior towards IS Security Policy Compliance. *2007 40th Annual Hawaii International Conference on System Sciences (HICSS07)*. doi:10.1109/hicss.2007.206

Puhakainen, P., & Siponen, M. (2010). Improving Employees Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly, 34*(4), 757-778. doi:10.2307/25750704

Safa, N. S., Solms, R. V., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security, 56*, 70-82. doi:10.1016/j.cose.2015.10.006

Sarabi, A., Zhu, Z., Xiao, C., Liu, M., & Dumitraş, T. (2017). Patch Me If You Can: A Study on the Effects of Individual User Behavior on the End-Host Vulnerability State. *Passive and Active Measurement Lecture Notes in Computer Science,* 113-125. doi:10.1007/978-3-319-54328-4_9

Siponen, M., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly, 34*(3), 487. doi:10.2307/25750688

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31-41. doi:10.1108/09685220010371394

Spears, J. L., & Barki, H. (2010). User Participation in Information Systems Security Risk Management. *MIS Quarterly, 34*(3), 503. doi:10.2307/25750689

Tang, M., Li, M., & Zhang, T. (2015). The impacts of organizational culture on information security culture: A case study. *Information Technology and Management, 17*(2), 179-186. doi:10.1007/s10799-015-0252-2

Vroom, C., & Solms, R. V. (2004). Towards information security behavioural compliance. *Computers & Security, 23*(3), 191-198. doi:10.1016/j.cose.2004.01.012

Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security*. Boston, MA: Cengage Learning.

Willison, R. (2006). Understanding the perpetration of employee computer crime in the organisational context. *Information and Organization, 16*(4), 304-324. doi:10.1016/j.infoandorg.2006.08.001

Willison, R., & Backhouse, J. (2006). Opportunities for computer crime: Considering systems risk from a criminological perspective. *European Journal of Information Systems, 15*(4), 403-414. doi:10.1057/palgrave.ejis.3000592

Willison, R., & Warkentin, M. (2013). Beyond Deterrence: An Expanded View of Employee Computer Abuse. *MIS Quarterly, 37*(1), 1-20. doi:10.25300/misq/2013/37.1.01

Zou, C., Gong, W., Towsley, D., & Gao, L. (2005). The monitoring and early detection of Internet worms. *IEEE/ACM Transactions on Networking, 13*(5), 961-974. doi:10.1109/tnet.2005.857113