Niko Salmi

HENKILÖSTÖN MOTIVOINNIN KEINOT TIETO-TURVAPOLITIIKAN VAHVISTAMISEKSI

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2015

TIIVISTELMÄ

Salmi, Niko
Henkilöstön motivoinnin keinot tieturvapolitiikan vahvistamiseksi
Jyväskylä: Jyväskylän yliopisto, 2015, 27 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja(t): Moilanen, Panu

Organisaatiot joutuvat enenevässä määrin suojautumaan niiden tietojärjestelmiin kohdistuvilta uhilta. Pelkät tekniset suojausratkaisut eivät kuitenkaan riitä, sillä henkilöstö saattaa tahattomasti tai tahallisesti kiertää nämä tietoturvatyökalut helpottaakseen omaa työtään. Organisaation tietoturvapolitiikka pyrkii estämään nämä tahattomat työkalujen kiertämiset antamalla henkilöstölle ohjenuorat, joita seuraamalla he voivat turvata käsittelemänsä tiedon. Tietoturvapolitiikan suurimpana ongelmana on se, ettei sitä noudateta henkilöstön toimesta, jolloin tulevaisuudessa tärkeäksi osaksi tietoturvan johtamista muodostuu henkilöstön motivointi tietoturvapolitiikan noudattamiseen. Tämä tutkielma keräsi kirjallisuudesta viisi eri motivoinnin osa-aluetta, joihin tietoturvajohtamisen tulisi tulevaisuudessa keskittyä: koulutus, valvonta, organisaation kulttuurin muokkaaminen, palkkiot ja rangaistukset. Näiden osa-alueiden ymmärtäminen ja implementointi organisaation toimintaan varmistaa henkilöstön motivoinnin onnistumisen ja sitä kautta tietoturvan kehittymisen.

Asiasanat: tietoturvapolitiikka, motivointi, tietoturva, noudattaminen

ABSTRACT

Salmi, Niko
Means to enhance employee compliance of information security policy
Jyväskylä: University of Jyväskylä, 2015, 27 p.
Information Systems, Bachelor's Thesis
Supervisor(s): Moilanen, Panu

Organizations have to protect their information assets from outsider threats. Sadly technical solutions don't provide enough protection, as the organizations' employees tend to turn them off. The information security policy tries to stop the employees from turning off the technical security tools. This is done by giving them information and precepts of how to protect the information they have access to. The biggest problem with the information security policy is that the employees don't follow it. Employee non-compliance increases the future need of compliance management in organizations. By studying the corresponding literature this thesis was able to point out five sections that these compliance managers should focus on: training, surveillance, improving organization culture, rewards and sanctions. By understanding and implementing these sections to the organization's everyday activities it will ensure the improved compliance of employees and additionally better overall information security.

Keywords: information security policy, motivating, information security, compliance

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Tämän päivän informaatiopainotteisessa taloudessa organisaation informaation suojaaminen on tärkeää kilpailukyvyn ylläpitämisen ja yritysmaailmassa selviytymisen kannalta (Calder & Watkins, 2010). Organisaatioiden tietoturvan tarve on kasvanut suuremmaksi sitä mukaa kuin tietoturvaloukkaukset ovat lisääntyneet (Stanton, Stam, Mastrangelo & Jolton, 2005).

Muuttuva globaali talous ja viimeaikaiset muutokset yritys- ja IT-hallinnossa ovat aiheuttaneet sen, että organisaatioissa joudutaan yhä enenevässä määrin hallitsemaan niiden etuihin kohdistuvia riskejä (Calder & Watkins, 2010). Organisaatioiden normaaleihin riskienhallinnan toimenpiteisiin kuuluu riskienkartoitus. Organisaatioissa tehtävän tietoturvariskien kartoituksen tarkoituksena on tiedostaa liiketoiminnan kannalta tietoon kohdistuvia uhkia. Eräs näistä uhista on ihmisten tekemät virheet. (Baskerville, Straub & Goodman, 2008). Toisin sanottuna käyttäjää, joka toimii harkitsemattomasti tietoverkoissa, pidetään riskinä, jota pitää jollakin tavalla hallita. Näiden riskien vähentämiseksi ja informaatioon liittyvän omaisuuden turvaamiseksi organisaatiot useimmiten turvautuvat ennen kaikkea teknologisiin ratkaisuihin (Kraemer, Carayon & Clem, 2009). Vaikka tällaiset tekniset ratkaisut ovatkin tärkeä osa nykypäivän organisaatioiden tietoturvaa, niillä ei kuitenkaan voida turvata informaatiota täydellisesti, sillä usein käyttäjät ohittavat nämä suojat joko tahallisesti tai tahattomasti (Siponen, Pahnila, Mahmood, 2006; Furnell & Clarke, 2012). Onneksi viimeaikaiset tutkimukset ovat alkaneet nähdä myös ihmisen osana ratkaisua (Furnell & Clarke, 2012).

Tällainen ihmisten toiminnasta riippuva ratkaisu on esimerkiksi tietoturvapolitiikan laatiminen, joka pyrkii ohjaamaan ihmisten toimintaa siten, että tieto voidaan turvata. Tämän tutkielman yhteydessä termillä tietoturvapolitiikka (*engl. information security policy*) tarkoitetaan ylimmän johdon vision pohjalta tehtyjä sääntöjä (sekä teknisiä että ei-teknisiä), joilla voidaan turvata informaatioon liittyvää omaisuutta (Baskerville ym., 2008; Thomson & von Solms, 2005). Tietoturvapolitiikan ongelmana on, että henkilöstö ei aina noudata sen ohjeita, jolloin siitä ei ole käytännössä mitään hyötyä. Siksi organisaatioiden tulee keskittyä tietoturvapolitiikan noudattamiseen tähtääviin toimiin,

jolloin kokonaistietoturva voidaan varmistaa. Tässä tutkielmassa tietoturvapolitiikan noudattamisella (*engl. information security policy obedience*) tarkoitetaan henkilöstön käytännön toimintaa, joka noudattelee ylemmän johdon visiota siten, kuin se on määritelty organisaation tietoturvapolitiikassa (Thomson & von Solms, 2005).

Tämä tutkielma käsittelee tietoturvapolitiikkaa ja sen noudattamiseen pyrkiviä motivoinnin keinoja tutkimalla, mikä on tietoturvapolitiikan merkitys ja mahdolliset ongelmat nykypäivän ja tulevaisuuden organisaatioissa, sekä miten organisaatioiden tulisi kannustaa henkilöstöä tietoturvapolitiikan noudattamiseen. Näiden pohjalta tutkielma vastaa sen tutkimuskysymykseen:

- Millaisia eri tietoturvapolitiikan noudattamiseen tähtääviä keinoja on olemassa?

Tutkimuskysymykseen lähdetään vastaamaan seuraavien alakysymysten avulla:

- Mitä tietoturvapolitiikalla tarkoitetaan?
- Miksi tietoturvapolitiikka ja henkilöstön motivointi on tärkeä osa informaation turvaamista nyt ja tulevaisuudessa?

Tutkielman ensimmäinen varsinainen asialuku käsittelee tietoturvapolitiikkaa avaten sen käsitteen ja selittäen tietoturvapolitiikan tarkoituksen, ongelmat ja mahdollisen tulevaisuuden kirjallisuuden pohjalta. Tutkielman toinen asialuku esittelee kirjallisuudesta esiin tulleet keinot motivoida henkilöstöä noudattamaan tietoturvapolitiikkaa. Viimeinen luku on yhteenveto, jossa käydään läpi vastaukset tutkimuskysymyksiin ja esitellään tutkielman oleelliset tulokset.

2 TIETOTURVAPOLITIIKKA

Tässä luvussa käsittelen organisaatioiden tietoturvapolitiikkaa lyhyesti. Alaluvussa 2.1 tarkoituksenani on esitellä tietoturvapolitiikan määritelmän ja kertoa, mikä sen tarkoitus on. Lisäksi tulen nostamaan esille tietoturvapolitiikkaan usein liittyvät ongelmat ja arvion siitä, millainen tulevaisuus tietoturvapolitiikan käytöllä tulee olemaan lähiaikoina. Alaluvussa 2. tarjoan myös havainnollistavan taulukon, josta tulee ilmi, millaisia tietoturvapolitiikan rikkeet ovat, sillä ne liittyvät oleellisesti tutkielman aiheeseen ja mahdollistavat havainnollistavien esimerkkien käytön tulevissa luvuissa.

2.1 Tietoturvapolitiikka yleisesti

Tietoturvapolitiikkaa on käsitelty laajasti eri näkökulmista akateemisten tutkimusten osalta. Vaikka tietoturvapolitiikasta on tehty useita tutkimuksia, harvat niistä keskittyvät hyvien tietoturvapolitiikkojen luontiin (Baskerville & Siponen, 2002). Tämä on yllättävää, sillä useilla organisaatioilla on ongelmia luoda tietoturvapolitiikka, tai implementoida jo olemassa olevaa tietoturvapolitiikkaansa onnistuneesti. CSI:n tekemässä tutkimuksessa 20 prosentilla organisaatioista ei joko ollut ollenkaan tietoturvapolitiikkaa (2,8 %), tai sen luominen oli vasta työn alla (17,2 %) (Richardson, 2011).

Vaikka useissa organisaatioissa ei ole toteutettu määrämuotoista tietoturvapolitiikkaa, sen on todettu olevan tärkeä työkalu tiedon turvaamisessa (von Solms & von Solms, 2004a). Baskervillen ym. (2008) mukaan tietoturvapolitiikka onkin yksi tärkeimmistä ja kaikkein halvimmista työkaluista, joilla voidaan yrittää turvata organisaation omaisuutta. Tietoturvapolitiikan toteuttamisen halpa hinta johtuu pääasiassa siitä, että se tarvitsee ainoastaan johdon aikaa sen luomiseen, hyväksymiseen ja esittämiseen henkilöstölle. Vaikka organisaatio päättäisikin käyttää ulkopuolista apua, kuten konsulttia, tietoturvapolitiikan luomiseen, olisivat kulut silti vähäiset verrattuna useisiin teknisiin ratkaisuihin.

Tietoturvapolitiikka on kuitenkin myös yksi vaikeimmista työkaluista toteuttaa onnistuneesti. Toteuttamisen vaikeudet johtuvat pääasiassa siitä, että tietoturvapolitiikan sisältö vaihtelee usein riippuen organisaatiosta ja sen tarpeista – yhdessä organisaatiossa toimiva ratkaisu ei siis välttämättä toimi toisessa. (Höne & Eloff, 2002).

Termin turvallisuuspolitiikka (*engl. security policy*) merkitys vaihtelee riippuen siitä, missä kontekstissa sitä käsitellään. Politiikka viittaa varsinkin yhdyssanojen jälkiosana käytettynä määrätarkoitukseen tähtäävään toimintalinjaan tai jollakin julkisen elämän alueella oleviin periaatteisiin (Kotimaisten kielten keskus, 2015).

Tietoturvapolitiikka käsitteenä jakautuu usein kahteen eri näkökulmaan: tekniseen tietoturvaan ja tietoturvan johtamiseen (Baskerville & Siponen, 2002). Teknisen tietoturvan näkökulmasta tietoturvapolitiikka on lähinnä teknisten järjestelmien turvallisuuteen liittyviä toimintoja, kuten käytönhallintaa. Tietoturvan johtaminen taas keskittyy lähinnä ei-teknisiin toimenpiteisiin.

Organisaatiossa tietoturvapolitiikka määrittää hyväksyttävän toiminnan tarjoamalla kokoelman lakeja, jotka sanelevat mitä organisaation henkilöstö voi ja ei voi sanoa tai tehdä. Turvallisuuspolitiikan luominen muistuttaa lain säätämistä: Valtuutettu yksikkö muotoilee turvallisuuspolitiikan, ja se ratifioidaan osaksi täytäntöönpanokelpoista sääntökokoelmaa. Tämän jälkeen se julkistetaan henkilöstölle, ja sen noudattamiseen kannustetaan säätämällä selkeät rangaistukset turvallisuuspolitiikan rikkojille. (Baskerville ym., 2008).

Tietoturvapolitiikan tarkoitus on suojella tiedon luottamuksellisuutta, eheyttä ja saatavuutta. Tieto on luottamuksellista silloin, kun sen luvaton käyttö järjestelmien tai henkilöiden toimesta on estetty. Luottamuksellisuus on siis sen varmistamista, että vain ne, joilla on oikeutus tietoon, pääsevät siihen käsiksi. Tieto on eheää silloin, kun se on kokonaista ja täydellistä. Eheys on vaarassa silloin, kun tieto altistuu korruptoitumiselle, vahingolle tai tuhoutumiselle. Tieto on saatavilla silloin, kun siihen oikeutetut henkilöt ja järjestelmät voivat minkään häiritsemättä päästä siihen käsiksi. (Baskerville ym., 2008).

2.2 Tietoturvapolitiikan rikkeet käytännössä

Tietoturvapolitiikkaa voidaan rikkoa monin eri tavoin. Siponen & Vance (2010) loivat tutkimuksensa yhteydessä listan, josta käy ilmi tyypillisimmät organisaatioissa tapahtuneet tietoturvapolitiikan loukkaukset (taulukko 1).

Tietoturvapolitiikan rikkeet	Määrä
Tietokoneen lukitsematta jättäminen tai uloskirjautumisen unohtaminen	*24*
Henkilökohtaisten salasanojen merkitseminen näkyville	*17*
Salasanojen jakaminen työtovereille tai ystäville	*14*
Luottamuksellisen tiedon kopioiminen turvaamattomille USB-tikuille	*14*
Luottamuksellisen tiedon paljastaminen ulkopuolisille	*13*
Turvallisuusominaisuuksien pois kytkeminen	*13*
Kannettavien tietokoneiden vastuuton käyttäminen organisaation ulkopuolella	*11*
Luottamuksellisen tiedon lähettäminen suojaamattomassa muodossa	*11*
Arvattavien ja helppojen salasanojen käyttäminen	*10*

Taulukko 1 - Tietoturvapolitiikan rikkeiden esiintyminen organisaatioissa (Siponen & Vance, 2010).

Taulukossa 1 on esiteltynä viidenkymmenenneljän (54) tietoturva-asiantuntijan näkemykset omien organisaatioidensa yleisimmistä tietoturvapolitiikan rikkeistä. Taulukko havainnollistaa, miten moninaisin eri tavoin henkilöstö rikkoo organisaatioiden tietoturvapolitiikkoja. Esimerkiksi tietokoneen lukitsematta jättäminen koneelta poistuttaessa nähdään yhtenä yleisimmistä tietoturvapolitiikan rikkomuksista. Tulen käyttämään taulukossa esiintyviä rikkeitä havainnollistavina esimerkkeinä tulevissa luvuissa.

2.3 Tietoturvapolitiikan ongelmat

Vaikka tietoturvapolitiikka on yksi tärkeimpiä organisaation tietoturvastrategian osa-alueita, sellaisen kokoon saattaminen ei aina ole ongelmatonta. Usein organisaation johdolla on erilaisia mielikuvia siitä, mitä tietoturvapolitiikka pitää sisällään. Lisäksi johdon taidot tällaisen dokumentin luomiseen voivat olla vajavaiset. Koska tällaisen dokumentin laatiminen tyhjästä on usein vaikeaa, siihen saatetaan hakea apua muiden organisaatioiden tietoturvapolitiikoista sekä julkisesti saatavista lähteistä, kuten internetissä tarjolla olevista dokumenttipohjista. Silloin riskinä on, että tietoturvapolitiikka luodaan ottamatta tarpeeksi huomioon organisaation kulttuuria. Organisaation kulttuuri määrittelee, miten henkilöstö näkee organisaation (Schlienger & Teufel, 2003). Organisaation kulttuuri onkin usein näkymätön voima, joka vaikuttaa ihmisten käyttäytymiseen, ja siten asettaa vaatimuksia useille toimille. Mikäli organisaation kulttuuria ei oteta huomioon, tietoturvapolitiikka jää vajavaiseksi, eikä se tällöin

tarjoa organisaation henkilöstölle tehokkaita toimintaohjeita tietoturvan varmistamiseksi. (Höne & Eloff, 2002).

Lisääntyvä tietoturvaan liittyvä lainsäädäntö aiheuttaa myös usein vaikeuksia organisaatioille, sillä tietoturvapolitiikan tulee voida vastata näihin lain vaatimuksiin. Yhä useammat säännökset ja standardit edellyttävät, että muun muassa opiskelijoiden, työntekijöiden, potilaiden, kuluttajien ja kansalaisten yksityisyys on turvattava. Monet näistä säännöksistä aiheuttavat ylimääräisiä rasitteita näiden alojen henkilöstölle. Henkilöstön tulee varmistaa tiedon turvallisuus asiakkaan ja lähettäjäorganisaation välisessä kommunikoinnissa siten kuin eri säännöksissä on asiasta määrätty. Tähän liittyvät esimerkiksi säännökset tiedon säilytyksestä, jakamisesta ja jopa formaatista. (Warkentin, Johnston & Shropshire, 2011). Siten organisaatioiden tietoturvapolitiikan tulee

- olla lainmukainen, eli se ei saa olla ristiriidassa lainsäädännön kanssa,
- kestää oikeuden tarkastelua, sekä
- olla oikein hallinnoitu, mukaan lukien asiakirjojen levittäminen henkilöstölle ja henkilöstön suostumusten dokumentointi siitä, että henkilö on lukenut, ymmärtänyt ja suostunut tietoturvapolitiikan sisällön vaatimuksiin (Baskerville ym., 2008).

Tarpeiden ja teknologioiden muuttuminen organisaatiossa aiheuttaa muuttumistarpeen myös tietoturvapolitiikalle (Baskerville ym., 2008). Uudenlaisten teknologioiden käyttö organisaatiossa lisää lainsäädännöllistä ongelmaa, sillä lainsäädäntö ei useinkaan pysy mukana teknologian kehityksessä. Näissä tapauksissa organisaatiot luovat omat politiikat ja toivovat, että tulevat lait vastaavat niitä. (Jaeger, Lin & Grimes, 2008). Ehkä suurin tietoturvapolitiikkojen ongelma liittyy kuitenkin käyttäjiin.

Käyttäjät eivät useinkaan noudata organisaation niille asettamaa tietoturvapolitiikkaa. Tällöin hyväkään tietoturvapolitiikka ei turvaa organisaation omaisuutta, sillä hyökkääjät voivat päästä käsiksi arkaluonteiseen tietoon henkilöstön tekemien virheiden kautta. CSI:n vuonna 2011 tekemän tutkimuksen mukaan noin puolet organisaatioiden havaitsemista hyökkäyksistä oli henkilöstön tahallisesti tai tahattomasti aiheuttamia (Richardson, 2011). Tutkimuksen seuraavassa pääluvussa syvennyn lähemmin henkilöstön käyttäytymisestä aiheutuviin ongelmiin.

2.4 Tietoturvapolitiikan tulevaisuus

Nykypäivän käyttäjät ovat pääasiassa uhatumpia kuin ennen vanhaan. Useat käyttäjät eivät vieläkään ymmärrä nykypäivän teknologioita, mikä heijastuu siihen, ettei uhkiakaan ymmärretä kunnolla (Furnell & Clarke, 2012). Kuitenkin

samaan aikaan nämä henkilöt joutuvat käyttämään sellaisia turvallisuuden työkaluja, jotka ennen olivat vain muutaman korkeasti koulutetun asiantuntijan vastuulla (Renaud & Goucher, 2014; Furnell & Clarke, 2012).

Tulevaisuudessa organisaatiot joutuvat entistä enemmän luottamaan henkilöstön käsiin erinäisiä turvallisuuskontrolleja, kuten virustorjunnan. Organisaation laitteiden ja palveluiden monipuolisen tarjonnan ja verkottumisen takia yksittäiset käyttäjät joutuvat tekemään yhä enemmän turvallisuuteen liittyviä päivittäisiä ratkaisuja (Furnell & Clarke, 2012). Jos edes murto-osa näistä ratkaisuista on väärin, organisaation tieto saattaa joutua uhatuksi (Leach, 2003). Lisäksi yhä suurempi osa tietoturvauhista ottaa nykyään kohteekseen tietojärjestelmien loppukäyttäjän. Koska käyttäjät joutuvat osallistumaan tietoturvan ylläpitoon, ei ole kohtuutonta sanoa, että nykypäivänä turvallisuudesta vastaavat kaikki organisaatiossa olevat henkilöt.

Myös organisaation ulkopuolisten henkilöiden tietoturvaosaaminen saattaa vaikuttaa organisaation turvallisuuteen. Yksityishenkilöiden kohtaamat tietoturvaongelmat voivat helposti levitä muiden ongelmiksi nykypäivän verkottuneessa maailmassa (Furnell & Clarke, 2012). Esimerkiksi yksityishenkilöiden kotikoneet saattavat muodostua organisaatiolle uhaksi, mikäli ne joutuvat haittaohjelmien tai muiden hyökkäysten johdosta osaksi bottiverkkoa (*engl. Botnet*). Bottiverkkoon kuuluvia koneita voidaan käyttää tuleviin palvelunestohyökkäyksiin ja haittaohjelmien levittämisyrityksiin useita eri organisaatioita vastaan (Symantec, 2015). Tulevaisuudessa nämä ongelmat voivat eskaloitua, kun yhä useammat laitteet liitetään osaksi internetiä. Organisaatioiden ja muiden yhteiskunnan toimijoiden tuleekin kiinnittää yhä enemmän huomiota ihmisten kouluttamiseksi turvalliseen tietoverkkojen käyttöön.

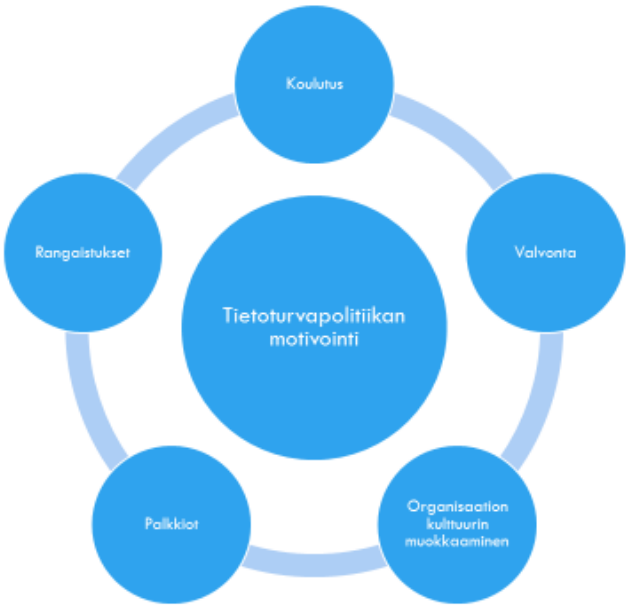
Edellä mainittujen syiden vuoksi on realistista olettaa, että tulevaisuudessa jotkin käyttäjät eivät pysty suorittamaan työhönsä liittyviä turvallisuuden toimintoja, sillä he eivät ymmärrä toimintaansa liittyviä uhkia tai keinoja uhkien välttämiseksi. Tämä johtuu siitä, että tietoturvan siirtyminen jokaisen työntekijän vastuulle on tapahtunut nopeammin kuin työntekijöiden koulutus. Siten koulutuksen ja työntekijöiden vastuun välillä on ristiriita, joka tulee ratkaista tulevaisuudessa koulutuksella (Furnell & Clarke, 2012). Kuitenkin vielä suurempi uhka organisaatioille tulevat olemaan yksilöt, jotka tietoisesti, mahdollisesti johonkin syyhyn vedoten, päättävät olla suojautumatta näiltä uhilta. (Furnell & Clarke, 2012). Siksi tietoturvapolitiikka ja keinot sen noudattamisen motivoinniksi tulevat olemaan yhä tärkeämpi osa organisaatioiden tietoturvaa tulevaisuudessa.

3 TIETOTURVAPOLITIIKAN MOTIVOINNIN KEINOT

Onnistunut tietoturvapolitiikan toteutus on yleisesti ottaen riippuvainen henkilöstön yhteistyöstä (von Solms & von Solms, 2004a; Vroom & von Solms, 2004). Vaikka tietoturvapolitiikan ja ohjenuorien luominen on hyvä lähtökohta, se ei vielä varmista että työntekijät noudattavat kyseisiä ohjeita (Bulgurcu, Cavusoglu & Benbasat, 2010; von Solms & von Solms, 2004a). Henkilöstön havaittu piittaamattomuus on johtanut siihen, että tiedon turvaamiseksi useat tietoturvaalan tutkijat ovat alkaneet keskittyä inhimillisiin ja organisatorisiin seikkoihin löytääkseen ratkaisuja ongelmaan (Kraemer ym., 2009; Bulgurcu ym., 2010; Puhakainen & Siponen, 2010). Näiden seikkojen ymmärtäminen auttaa organisaatioiden tietoturva-asiantuntijoita analysoimaan ja tekemään ratkaisuja käyttäytymiseen liittyvissä kysymyksissä.

Henkilöstön motivoinnista on useita tutkimuksia, jotka tarjoavat välillä ristiriitaisiakin tuloksia. Tämän tutkimusmäärän keskellä tietoa hakeva lukija voi helposti hämmentyä ristiriitaisuuksista ja siitä, mikä tieto on relevanttia hänen tapauksessaan. Nämä tutkimukset sisältävät usein toisen kahdesta perusolettamuksesta: Jotkin määrittelevät ihmisen rikkovan tietoturvapolitiikkaa tahallisesti (Siponen & Vance, 2010; Herath & Rao, 2009a; Herath & Rao, 2009b; Siponen ym., 2006), kun taas toiset uskovat pääasiassa ympäristön vaikutusten aiheuttavan näiden rikkeiden muodostumisen (Furnell & Clarke, 2012, Furnell, 2005; Puhakainen & Siponen, 2010). Riippuen perusolettamuksista, tutkimusten sisällöt usein vaihtelevat ja siten antavat lukijalle vain oman näkökulmansa henkilöstön motivoinnista. Tarkoituksenani on sivuuttaa nämä perusolettamukset ja antaa laajan kuvan tietoturvapolitiikan motivoinnin keinoista, jossa perusolettamukset eivät sulje toisiaan pois.

Olen kirjallisuutta lukiessani tullut siihen tulokseen, että tietoturvapolitiikan noudattamisen motivointi voidaan karkeasti jakaa viiteen eri osa-alueeseen. Nämä osa-alueet ovat havainnollistettuna seuraavassa kuviossa (kuvio 1):



KUVIO 1 – Tietoturvapolitiikan motivoinnin osa-alueet.

Kuviossa 1 on havainnollistettu viisi eri osa-aluetta, joiden merkityksen tiedostamalla organisaatiot voivat vaikuttaa henkilöstönsä aikomukseen noudattaa tietoturvapolitiikkaa. Nämä osa-alueet ovat: koulutus, valvonta, organisaation kulttuurin muokkaaminen, palkkiot ja rangaistukset. Kuten kuviossa näkyy, mikään näistä osa-alueista ei ole eriarvoisessa asemassa muihin nähden, vaan organisaatiot voivat käyttää jokaista näistä haluamassaan suhteessa riippuen organisaation arvoista ja visiosta, jotka määrittelevät organisaation suhtautumisen tietoturvaan. Kuvion osa-alueet ovat itseni määrittelemiä, eivätkä ne välttämättä sisällä kaikkia tietoturvapolitiikan motivoinnin keinoja, eivätkä ne myöskään ole absoluuttisia. Organisaatioiden henkilöstö voi siis noudattaa tietoturvapolitiikkaa, vaikka organisaatio ei käyttäisikään tutkielmassa mainittuja rangaistuskäytänteitä. Tutkielmassa mainitut osa-alueet on kuitenkin poimittu useista asiaa koskevista lähteistä, joten uskon niiden kattavan aihealueen erittäin hyvin.

Seuraavissa alaluvuissa käsittelen kuviossa 1 esittelemäni tietoturvapolitiikan motivoinnin osa-alueet. Niiden avulla vastaan tutkielman tutkimuskysymykseen. Eri osa-alueet liittyvät usein läheisesti toisiinsa, mutta niitä ei ole järjestelty mihinkään tärkeysjärjestykseen.

3.1 Koulutus

Kouluttamisen on todettu olevan yksi tärkeimmistä keinoista parantaa tietoturvapolitiikan noudattamista. Kuitenkin monissa organisaatioissa on unohdettu koulutusohjelmien tärkeys (von Solms & von Solms, 2004a). CSI:n tekemän tut-

kimuksen mukaan 35 prosenttia organisaatioista käytti koko turvallisuusbudjetistaan alle prosentin verran tietoturvakoulutukseen - 15 prosentilla (14,9 %) ei ollut tietoturvan koulutusohjelmaa lainkaan (Richardson, 2011). Vähäisen tietoturvakoulutuksen seurauksena henkilöstö ei välttämättä ole tietoinen organisaation tietoon kohdistuvista riskeistä tai edes tietoturvapolitiikan olemassaolosta (von Solms & von Solms, 2004a). Tietoturvakontekstissa organisaatiot pyrkivät kouluttamisella opettamaan henkilöstölle sen, miten he voivat turvata tietoa, johon heillä on käyttöoikeus. Ajatus on peräisin liiketoimintaympäristöstä, jossa koulutuksen prosessi on nähty hyvin yksinkertaisena: Tietoa syötetään henkilöstölle, jolloin saadaan tuloksena toivottua käytöstä. (Renaud & Goucher, 2014). Käytännössä tämä ei kuitenkaan ole toiminut odotetulla tavalla (Albrechtsen, 2007). Määritelmä on myös hyvin laaja, sillä se käsittää melkein kaikki tietoturvaan liittyvät asiat, eikä se avaudu asiaan perehtymättömälle. Tässä luvussa pyrin avaamaan kouluttamiseen liittyviä haasteita ja tarpeita spesifien tietoturvapolitiikan noudattamiseen liittyvien ongelmien ratkaisemiseksi. Näitä ongelmia ovat seuraavat:

- Henkilöstö ei osaa käyttää tietoturvatyökaluja tai ne ovat muuten vaikeasti käytettäviä (Furnell, 2005).
- Henkilöstö ei ymmärrä uhkia, niiden vakavuutta tai todennäköisyyttä (Furnell & Clarke, 2012; Pahnila, Siponen & Mahmood, 2007).
- Tietoturvapolitiikat ovat vaikeasti saatavilla, niitä ei tunneta tai niihin tutustumiseen ei anneta riittävästi aikaa ja tukea (Pahnila ym., 2007).

Tietoturvasta huolehtiminen on uhkien ja niiltä suojautumisen kehittymisen myötä siirtynyt muutaman tietoturva-asiantuntijan vastuulta kaikille organisaation jäsenille (Furnell & Clarke, 2012; Renaud & Goucher, 2014). Tämä ei kuitenkaan ole välttämättä huono kehityksen suunta, sillä työntekijöiden osallistaminen tietoturvaprosesseihin voi parhaassa tapauksessa vähentää turvallisuuden aiheuttamia kokonaiskuluja (Chia, Maynard & Ruighaver, 2002). Kuitenkin ongelmaksi voi nousta se, ettei henkilöstö osaa käyttää sen vastuulle annettuja teknisiä tietoturvatyökaluja oikein. Tästä esimerkkinä ovat huonot salasanakäytännöt tai huonosti ylläpidetty virustorjuntaohjelmisto (Taulukko 1). Henkilöstön turvallisuustyökalujen huono käyttötaito ei yksinään selitä, miksi niitä ei käytetä oikein. Myös tietoturvatyökalujen huono käytettävyys vaikuttaa tähän ongelmaan. (Furnell, 2005). Organisaatiot eivät useinkaan pysty vaikuttamaan ohjelmistojen käytettävyyteen, jolloin valittujen tietoturvatyökalujen käytön kouluttaminen henkilöstölle saattaa olla hyvä vaihtoehto näiden hallitsemisen varmistamiseksi. Mikäli teknisten ohjelmistojen helppokäyttöisyydessä ei tulevaisuudessa tapahdu oleellisia muutoksia, työkalujen käytön koulutusta joudutaan harjoittamaan aina, kun organisaatio vaihtaa ohjelmistojen tarjoajaa.

Useissa tutkimuksissa on todettu, että henkilöstön korkeat arviot tietoturvauhan vakavuudesta ja todennäköisyydestä vaikuttavat positiivisesti sen aikomuksiin noudattaa tietoturvapolitiikkoja (Herath & Rao, 2009a; Pahnila ym., 2007; Ng, Kankanhalli & Xu, 2009;). Toisin sanoen, mikäli henkilö tiedostaa tie-

toturvauhan vakavuuden ja kokee sen toteutumisen todennäköiseksi, hän todennäköisemmin pyrkii noudattamaan organisaation tietoturvapolitiikkaa. Kuitenkin varsinkin vanhemmalla henkilöstöllä on harvoin riittävästi tietoa tietoturvauhista, eivätkä he ole tottuneet käyttämään tietoturvatyökaluja (Furnell & Clarke, 2012; Furnell, 2005). Tietoturvauhkien ymmärtämättömyys aiheuttaa siten pikemminkin tietoturvauhan, sillä henkilöstö ei näe tarvetta tietoturvatyökalujen käytön opettelemiseen. Samalla tämä henkilöstöryhmä aiheuttaa omalla vapaa-ajan tietokoneen käytöllään uhan organisaatioille, mikäli henkilöstön omat koneet altistuvat tietoturvauhille (Furnell & Clarke, 2012). Furnell & Clarke (2012) ehdottavat ongelman ratkaisuksi sitä, että tietoturvaohjelmien tulisi olla osa julkista koulutusta. Silloin voitaisiin turvata myös henkilöstön henkilökohtaisten koneiden käyttö, jolloin vaikutus ulottuisi koko yhteiskuntaan. Tällä hetkellä organisaatiot joutuvat kuitenkin itse antamaan tietoa uhista henkilöstölleen (Siponen & Vance, 2010). Vaikka tämän koulutuksen vaikutus yhteiskunnallisesti katsoen onkin vähemmän merkittävä, se on tärkeä osa organisaation tietoturvapolitiikan noudattamiseen pyrkivää toimintaa.

Pahnila ym. (2007) totesivat tutkimuksessaan, että organisaation antamat ympäristölliset mahdollisuudet vaikuttavat henkilöstön asenteisiin noudattaa tietoturvapolitiikkaa. Nämä ympäristölliset mahdollisuudet ovat tiedon helpon saatavuuden varmistaminen sekä avun ja ajan tarjoaminen, jotta tietoturvapolitiikkaan voidaan perehtyä tarpeeksi syvällisesti. Toisin sanoen, mikäli henkilöstö kokee, ettei sillä joko ole aikaa tutustua tietoturvapolitiikkaan, se ei saa apua vaikeasti ymmärrettäviin tietoturvapolitiikan kohtiin, tai se ei löydä tietoturvapolitiikkaa helposti, se ei myöskään todennäköisesti noudata sitä. Siksi organisaation tuleekin nähdä vaivaa tietoturvapolitiikan ymmärrettävän kieliasun varmistamiseksi (Siponen & Vance, 2010; Leach, 2003), sekä mielellään antaa se saataville useiden eri lähteiden kautta. Lisäksi esimiesten tulee määrätä henkilöstölle aikaa tutustua tietoturvapolitiikkaan.

Tietoturvaa ja sen noudattamista voidaan kouluttaa organisaatioissa monella eri tavoin: luennoimalla, käytännön projekteilla tai case-tutkimuksilla. Näistä parhaaksi vaihtoehdoksi on kuitenkin huomattu käytännön projektit, jotka ottavat huomioon koulutettavan henkilökohtaiset koulutustarpeet (Puhakainen & Siponen, Pahnila & Mahmood, 2010; Meso, Ding, Xu (2013). Tämä sisältää sen, että koulutus ottaa huomioon myös henkilön aikaisemman tiedon tietoturvan noudattamisesta. Lisäksi Puhakainen ja Siponen (2010) tekivät huomion, että tietoturvan noudattamisen koulutuksen tulisi olla mieluummin jatkuvaa, verrattuna lyhytkestoisiin koulutusyrityksiin parantaa tietoturvapolitiikan noudattamista. Kaiken kaikkiaan koulutus on oikein toteutettuna erinomainen keino vastata useisiin tietoturvapolitiikan noudattamiseen liittyviin ongelmiin. Se ei kuitenkaan toimi yksinään, vaan tarvitsee rinnalleen esimerkiksi oikeanlaisen organisaatiokulttuurin (Renaud & Goucher, 2014).

3.2 Organisaation turvallisuuskulttuurin muokkaaminen

Henkilöstö näkee tietoturvan takaamisen usein ylimääräisenä työnä, joka vaikeuttaa omien työtehtävien hoitamista (Ross, Jackson, Miyake, Boneh & Mitchell 2005). Jos tietoturvatyökalut ovat vaikeasti käytettäviä tai niiden käyttö ei tuo selkeitä tuloksia, käyttäjiä saattaa alkaa houkutella näiden työkalujen kiertäminen (Leach, 2003). Turvallisuus usein verottaakin järjestelmien ja työtehtävien helppokäyttöisyyttä ja nopeutta. Organisaatiot joutuvat usein tasapainottelemaan turvallisuuden ja käytettävyyden välillä, jotta toisaalta työtehtävät saadaan hoidetuksi ilman kohtuuttomia henkilöstökustannuksia, ja toisaalta tietojärjestelmien turvallisuus voidaan taata mahdollisimman hyvin. Vahvan turvallisuuskulttuurin on nähty helpottavan tätä vastakkainasettelua, sillä sen ansiosta henkilöstö tekee turvallisia päätöksiä joutumatta miettimään niitä erikseen. Vahva turvallisuuskulttuuri siis integroi turvallisen toiminnan osaksi päivittäistä työskentelyä niin, ettei sitä edes huomata (Thomson, von Solms & Louw 2006; Schlienger & Teufel, 2003).

Turvallisuuskulttuuri on osa organisaation kulttuuria, joka määrittelee miten henkilöstö näkee organisaation (Schlienger & Teufel, 2003). Jokaisella organisaatiolla on organisaatiokulttuuri, tiedostivat ne sen tai eivät. Tämä kulttuuri on olemassa sekä tietoisella tasolla että alitajuntaisesti. Organisaation kulttuuri on voimakas ja usein tiedostamaton voima, joka vaikuttaa yksilöiden ja kokonaisten ryhmien käyttäytymiseen. (Thomson ym., 2006). Organisaation kulttuuri on muuttuva, ja johto voi vaikuttaa siihen omilla toimillaan tiettyyn rajaan asti (Schlienger & Teufel, 2003). Siten myös organisaatioiden turvallisuuskulttuureihin voidaan vaikuttaa. Koska tietojärjestelmien turvallisuus on usein riippuvainen ihmisten käyttäytymisestä (Siponen ym., 2010), on tärkeää että organisaatiot luovat hyvän turvallisuuskulttuurin.

Organisaation turvallisuuskulttuurin muuttamiseksi on puututtava muun muassa henkilöstön normeihin (Thomson ym., 2006). Nämä normit ovat uskomuksia siitä, millaista käyttäytymistä esimiehet tai työtoverit odottavat henkilöltä (Herath & Rao, 2009a). Ihmiset siis kokevat muiden käyttäytymisen olevan tiedonlähde, joka osoittaa, mikä toiminta on soveliasta tai sopimatonta kyseisessä ympäristössä. Mikäli siis henkilön esimiehet ja työtoverit osoittavat toimillaan ja sanoillaan, että turvallisuus on tärkeä osa toimintaa, se vaikuttaa positiivisesti myös kyseisen henkilön käyttäytymiseen (Leach, 2003; Herath & Rao, 2009a).

Koska henkilöstön käyttäytyminen saa vaikutteita esimiehiltä, organisaation turvallisuuskulttuurin muuttaminen on suurelta osin riippuvainen esimiesten omista asenteista (Leach, 2003; Chia ym., 2002). Siksi ylimmän johdon tuleekin esimerkkiä näyttäen noudattaa organisaation tietoturvapolitiikkaa (Thomson & von Solms, 2005) sekä viestinnässään korostaa henkilöstölle, ettei tietoturvapolitiikkaa tule rikkoa edes tiukan aikataulun aiheuttamassa paineessa. Lisäksi

tulee varmistaa, etteivät alemman tason esimiehet rohkaise alaisiaan poikkeamaan turvallisuusmääräyksistä missään olosuhteissa. (Siponen & Vance, 2010).

Henkilöstö tekee päivittäin tietoturvaan liittyviä päätöksiä osana heidän päivittäistä työtään. Jotkin näistä päätöksistä joudutaan tekemään nopeastikin, ilman että henkilö ehtii turvautumaan kirjallisiin ohjemateriaaleihin. Tietyn ajan kuluttua tämä henkilö on kerännyt suuren määrän kokemuksia, jotka koostuvat hänen tekemistään tietoturvaan liittyvistä päätöksistä. Nämä ovat joko hyviä tai huonoja päätöksiä, riippuen henkilön saamasta palautteesta. Mikäli henkilö ei saa kritiikkiä toiminnastaan, hän todennäköisesti liittää kyseisen toiminnan osaksi työskentelyään, ja tästä toiminnasta muodostuu siten tapa. (Leach, 2003). Pahnila ym. (2007) totesivat tutkimuksessaan, että henkilöstölle muodostuneet tavat vaikuttavat tietoturvapolitiikan noudattamiseen. Näistä tavoista on harmia silloin, kun ne ovat ristiriidassa tietoturvapolitiikan kanssa. Tämän tiedostamalla organisaatiot voivat pyrkiä vaikuttamaan tapojen muodostumiseen antamalla aktiivisesti palautetta henkilöstön tietoturvaan liittyvästä toiminnasta. Siten voidaan saada aikaan tapoja, jotka noudattavat organisaation tietoturvapolitiikkaa ja parantavat näin tietoturvan noudattamista tiedostamattomalla tasolla.

Organisaation turvallisuuskulttuuri on yksi tärkeimmistä tietoturvapolitiikan noudattamiseen tähtäävistä keinoista, jonka muodostumiseen vaikuttavat kaikki tietoturvapolitiikan motivoinnin keinot. Kaikki nämä keinot osaltaan osoittavat organisaation johdon motivoituneisuutta tietoturvaan, jolloin organisaation turvallisuuskulttuuri muovautuu pääasiassa muiden toimien pohjalta ilman, että siihen tarvitsee erikseen kiinnittää huomiota. Oikeastaan organisaatiokulttuurin voimakas muuttaminen saattaa pikemminkin aiheuttaa henkilöstössä muutosvastarintaa (Vroom & von Solms, 2004). Kuitenkin on hyvä ymmärtää organisaation turvallisuuskulttuurin merkitys henkilöstön käyttäytymisen taustalla vaikuttavana voimana.

3.3 Palkkiot

Myös henkilöstön sitoutumisen taso vaikuttaa tietoturvakäyttäytymiseen. Mikäli henkilöstö on sitoutunut organisaatioon, se myös todennäköisemmin noudattaa tietoturvapolitiikkaa. Lisäksi sitoutunut henkilöstö kokee, että sen toiminta vaikuttaa vahvasti organisaation suorituskykyyn. He siis kokevat tiedon turvallisen käsittelyn vaikuttavan koko organisaation tietoturvaan. (Herath & Rao, 2009a). Koska sitoutuneet henkilöt noudattavat organisaation tietoturvapolitiikkaa todennäköisemmin kuin sitoutumattomat, organisaatioiden tulisi pohtia miten he voivat sitouttaa henkilöstöään. Organisaatiot käyttävät tähän usein palkitsemisjärjestelmiä, kuten rahaa.

Yleisen uskomuksen mukaan ihmisen käyttäytymiseen on helppo vaikuttaa kepin (rangaistusten) ja porkkanan (rahan) avulla. Organisaatiot uskovat edelleen, että henkilöstöä voidaan motivoida rahan ja rangaistusten avulla (Stanton, Stam, Mastrangelo & Jolton, 2005). Tämä voidaan huomata useista tapauksista,

joissa organisaatiot palkitsevat työntekijöitään usein suurienkin bonusten avulla (Talouselämä, 2015). Tämä uskomus on alun perin lähtöisin Taylorilta (ks. Renaud & Goucher, s. 364), jonka näkemys ulkoisista palkkioista henkilöstön motivaation lähteenä on edelleen suosittu yritysmaailmassa. Kuitenkin useat tutkimukset ovat todenneet, että henkilöstön palkitseminen toimii vain tiettyyn rajaan asti, jonka jälkeen muut henkilöstön tarpeet nousevat tärkeämmiksi. Näitä tarpeita ovat muun muassa hyvä työilmapiiri, työuralla eteneminen ja joustavat työtunnit. Siten rahalliset palkkiot eivät useinkaan toimi henkilöstön motivaattorina hyvin palkatuissa tehtävissä. (Renaud & Goucher, 2014).

On olemassa kuitenkin muita palkkioita kuin raha. Kun henkilöstö tuntee olevansa hyvin kohdeltu, arvostettu ja palkittu, se usein vastaa tähän toimimalla organisaation intressien hyväksi. Samalla tavoin väärin kohdeltuna henkilöstöstä voi tulla uhka organisaatiolle ja sen turvallisuudelle. Nykypäivän organisaatiot tiedostavat henkilöstöllä olevan erilaisia tarpeita riippuen yksilöstä. Joitakin kiinnostaa hyvä palkka, jolla voidaan maksaa laina ja parantaa elämänlaatua vapaa-ajalla. Toiset arvostavat työpaikan sosiaalista ilmapiiriä tai uralla etenemistä. Mikä tahansa tarve yksilöllä onkaan, sen täyttämällä organisaatiot parantavat henkilön motivaatiota toimia organisaation hyväksi. (Leach, 2003).

Palkitsemista tietoturvapolitiikan noudattamiseen tähtäävänä keinona ei ole tutkittu kovinkaan paljoa. Asiaa on sivuttu useissa tutkimuksissa, mutta ne eivät ole olleet kovinkaan syvällisiä (Pahnila ym., 2007; Herath & Rao, 2009a; Bulgurcu ym., 2010; Siponen ym., 2010; Boss, Kirsch, Angermeier, Shingler & Boss, 2009). Näiden tutkimusten tulos on ollut kuitenkin selvä: Palkkiot eivät vaikuta merkittävästi henkilöstön aikomukseen noudattaa tietoturvapolitiikkaa. Näissä tutkimuksissa on ollut tarkastelussa sekä rahalliset palkkiot että joitakin muita arvostukseen viittaavia palkkioita, kuten esimiehen osoittama henkilökohtainen arvostus. Yleisten tutkimusten valossa näyttääkin siltä, etteivät palkkiot motivoi henkilöstöä noudattamaan tietoturvapolitiikkaa.

Kuitenkin kuten Leach (2003) totesi, henkilöstölle kohdistettu yleinen arvostus vaikuttaa usein henkilöstön haluun toimia organisaation tavoitteiden mukaisesti. Arvostusta voidaan osoittaa usealla eri tavalla, eivätkä tähänastiset tutkimukset ole analysoineet näitä eri tapoja tarpeeksi kattavasti. Lisäksi tutkimukset ovat pääasiassa kohdistuneet hyvin palkattuihin organisaatioihin, jolloin myös rahallisten palkkioiden vaikutus henkilöstöön on todettu ainoastaan yhtä henkilöstönosaa tarkastellen. Uskon, että rahalliset palkkiot ovat edelleen hyvä kannustin niissä organisaatioissa, joissa on paljon lyhyitä tai määräaikaisia työsuhteita, sekä pieni peruspalkka tai provisiopalkkausjärjestelmä. Myös eri maiden kansalaisten välillä on suuria tuloeroja, jolloin varsinkin kehitysmaissa tällainen kannustin saattaisi toimia. Lisäksi palkkiot viestivät henkilöstölle johdon näkökulmaa tietoturvapolitiikkaan (Boss ym., 2009), jolloin ne omalta osaltaan edistävät organisaation kulttuurin kehittymistä. Palkkioiden merkitystä tietoturvapolitiikan noudattamisen motivoijana tuleekin tutkia vielä lisää, jotta asiasta voidaan saada varmuus.

3.4 Rangaistukset

Peloteteoria (*engl. Deterrence theory*) on yksi käytetyimmistä teorioista tietoturvapolitiikan noudattamista käsittelevässä kirjallisuudessa (Siponen & Vance, 2010). Teorian mukaan ihmisen ei-toivottu käytös vähenee, kun rangaistuksen todennäköisyys ja vahvuus kovenee (Herath & Rao, 2009a; Herath & Rao, 2009b; Siponen & Vance, 2010; Pahnila ym., 2007). Toisin sanoen yksilö arvioi kiinni jäämisen mahdollisuuden ja rangaistuksen kovuuden, jonka jälkeen päättää ryhtyykö sääntöjenvastaiseen toimintaan. Rangaistukseen voi organisaatioiden tapauksessa kuulua niin johdon säätämät toimet, kuten esimerkiksi ääritapauksissa irtisanominen, kuin myös oma häpeä ja muiden paheksunta (Siponen & Vance).

Rangaistusten merkitystä organisaatioissa on tutkittu paljon ja siitä on saatu useita erilaisia vastauksia riippuen kontekstista. Esimerkiksi rangaistusten koventumisen on huomattu vähentävän ohjelmistopiratismin hyväksyntää organisaatioissa (Peace, Galletta & Thong, 2003). Samalla tavoin rangaistuksien uhalla voidaan pyrkiä vaikuttamaan henkilöstöön, jotta se noudattaisi organisaatioiden tietoturvapolitiikkaa. Esimerkiksi jos henkilöstön toimet aiheuttavat organisaation tietoturvan loukkauksen, organisaatio voi tutkia sen ja asettaa sen aiheuttaneille henkilöille rangaistuksen. Peloteteorian mukaan jos henkilöstö kokee tietoturvapolitiikan noudattamatta jättämisestä saadun rangaistuksen, kuten työn menettämisen, sakon tai muun kurinpitomenettelyn, olevan suurempi suhteessa siitä saatuihin hyötyihin, se saa heidät toimimaan halutulla tavalla (Herath & Rao, 2009a; Herath & Rao, 2009b; Siponen & Vance, 2010; Pahnila ym., 2007). Henkilöstöön kohdistuva valvonta ja rangaistukset eivät kuitenkaan mitenkään vahvista henkilöstön positiivista suhtautumista tietoturvapolitiikkaan (Leach, 2003). Useat tutkimukset rangaistusten vaikutuksesta tietoturvapolitiikan noudattamiseen ovatkin todenneet, etteivät rangaistukset vaikuta henkilöstön aikomukseen noudattaa tietoturvapolitiikkaa (Siponen & Vance, 2010; Pahnila ym., 2007). Jotkin tutkimukset ovat jopa todenneet asian olevan päinvastoin, eli rangaistukset saattavat jopa aiheuttaa henkilöstön suhtautumisen muuttuvan kielteisemmäksi (Herath & Rao, 2009a; Herath & Rao, 2009b).

Siponen ja Vance (2010) ovat selittäneet kriminologian tutkimukseen perustuvassa tutkimuksessaan henkilöstön usein käyttävän neutralisoivia tekniikoita (*engl. Neutralization techniques*), jotka estävät säädettyjä rangaistuksia saavuttamasta toivottua käyttäytymistä. Neutralisoivat tekniikat ovat keinoja, joilla ihminen oikeuttaa toimensa – tässä tapauksessa tietoturvapolitiikan noudattamatta jättämisen. Siponen ja Vance huomasivat kuuden näistä tekniikoista soveltuvan tietoturvakontekstiin. Näitä tekniikoita ovat:

- Vastuun kieltäminen (*engl. denial of responsibility*), jolloin henkilöstö saattaa esimerkiksi kyseenalaistaa tietoturvapolitiikan selkeyden.

- Ongelman kieltäminen (*engl. denial of injury*), jolloin henkilöstö voi kieltää ongelman olemassaolon esimerkiksi toteamalla, ettei organisaatiolle aiheudu harmia tietoturvapolitiikan kiertämisestä.
- Tarpeellisuuden perustelu (*engl. defense of necessity*), jolloin tietoturvaa kierretään vetoamalla sen tarpeellisuuteen, kuten tiukkoihin aikatauluihin.
- Tuomitsijoiden syyttäminen (*engl. condemnation of condemners*), jolloin henkilöstö saattaa syyttää tietoturvapolitiikan kohtuuttomia vaatimuksia.
- Prioriteetteihin vetoaminen (*engl. appeal to higher loyalties*), jolloin henkilöstö saattaa väittää, että tietoturvapolitiikan kiertäminen on ainoa tapa saada työ tehdyksi.
- Ledgerin metaforan (*engl. the metaphor of the Ledger*) käyttäminen, jolloin henkilö pyrkii oikeuttamaan satunnaisen tietoturvapolitiikan rikkomisen vetoamalla siihen, että hän kuitenkin pääasiallisesti noudattaa niitä. (Siponen & Vance, 2010)

Neutralisoivat tekniikat vaikuttavat huomattavasti henkilöstön aikomukseen rikkoa tietoturvapolitiikkaa. Ne edesauttavat toimijoita rikkomaan tai joustamaan säännöissä niin, että heidän omatuntonsa on puhdas. Monessa organisaatiossa on kohdattu edellä mainittujen kaltaisia perusteluja tietoturvapolitiikan kiertämisestä (Puhakainen, 2006), mutta niiden merkitystä ei välttämättä ole linkitetty neutralisoiviin tekniikkoihin. Henkilöstö voikin käyttää useita neutralisoivia tekniikoita jokaiseen Taulukossa 1 mainittuun tietoturvapolitiikan rikkeeseen. Esimerkiksi henkilöstö voi kieltää, että tietokoneelta uloskirjautumisen unohtaminen olisi ongelma, sillä lyhyen poissaolon aikana ei kukaan ehdi käyttää konetta. Toisaalta samassa rikkeessä voidaan vedota Ledgerin metaforaan, jolloin todetaan unohduksen tapahtuvan välillä, mutta useimmiten koneelta kirjaudutaan ulos.

Vaikka tutkimukset ovat pääasiassa osoittaneet, etteivät rangaistukset lisää henkilöstön halua noudattaa tietoturvapolitiikkaa, ne ovat silti tärkeä osa sitä. Tämä johtuu siitä, että rangaistukset tietoturvapolitiikan osana eivät ole pelkästään pelotetoiminto, vaan ne tarjoavat organisaatiolle selkeät toimintalinjat tietoturvapolitiikan rikkojia vastaan. (Siponen & Vance, 2010; Harrington, 1996). Lisäksi ne osaltaan viestivät henkilöstölle johdon suhtautumista tietoturvapolitiikkaan ja siten vaikuttavat mahdollisesti organisaation kulttuurin kehittymiseen. Siksi rangaistukset tulee pitää osana organisaation keinoja, mutta niiden vaikutuksen rajallisuus tulee tiedostaa.

3.5 Valvonta

Jeremy Bentham (1791) kehitti aikanaan omaperäisen ajatuksen, jonka hän nimesi Panopticoniksi. Hänen aikomuksenaan oli perustaa vankila, jonka keskellä

olisi vartiotorni, josta näkisi jokaisen vangin. Nämä vangit eivät kuitenkaan näkisi valvojaa, eivätkä siten koskaan tietäisi koska heidän toimintaansa tarkkaillaan. Epätietoisuus aiheuttaisi sen, etteivät vangit uskaltaisi tehdä kiellettyä toimintaa, koska heitä saatetaan juuri sillä hetkellä tarkkailla. Vaikka Benthamin ajatuksia on kritisoitu laajasti, se onnistuu kiteyttämään valvonnan perusajatuksen: valvonnan alla tietoisesti toimivat ihmiset pyrkivät noudattamaan sääntöjä (Vroom & von Solms, 2004).

Edellisessä luvussa mainitun peloteteorian mukaan rangaistusten kovuuden lisäksi rangaistuksen todennäköisyydellä on vaikutusta henkilöstön käyttäytymiseen. Toisin sanoen yksilö arvioi kiinnijäämisen todennäköisyyden ja rangaistuksen kovuuden, jonka jälkeen päättää ryhtyykö sääntöjenvastaiseen toimintaan.

Tietoturvakontekstissa rangaistuksen todennäköisyys kasvaa sen mukaan, mitä enemmän valvontaa organisaatiossa tapahtuu (Herath & Rao, 2009a, Herath & Rao, 2009b). Henkilöstön vastuullisen käytöksen ja tietoturvapolitiikan noudattamisen varmistamiseksi organisaatioiden tuleekin käyttää jotakin arviointimenetelmää, jotta henkilöstön käyttäytymistä voidaan seurata (Vroom & von Solms, 2004; von Solms & von Solms, 2004b). Mikäli henkilö on tietoinen valvonnasta, hän todennäköisemmin pyrkii noudattamaan tietoturvapolitiikkaa kiinni jäämisen ja rangaistuksen pelossa. Valvonta myös mahdollistaa rangaistusten langettamisen tietoturvapolitiikkaa rikkoville henkilöille. Jotta valvonta aiheuttaisi peloteteorian mukaisen vaikutuksen, sen tulee olla kuitenkin selkeästi näkyvää. Näkyvä valvonta lisää henkilön arvioimaa kiinnijäämisen riskiä, jolloin hän saattaa luopua sääntöjenvastaisesta toiminnasta. Pieni kiinnijäämisen riski puolestaan saattaa vahvistaa sääntöjenvastaista toimintaa. Se on esimerkiksi listattu yhdeksi tärkeimmistä tekijöistä, miksi ihmiset päättävät ladata tietoa laittomasti verkosta (Straub, 1990). Etätyön mahdollisuuden lisääntyessä organisaatioissa myös työn valvonnan mahdollisuudet vähenevät. Henkilöstön huolimaton kannettavien tietokoneiden käyttö on silti listattu yhdeksi useimmin sattuvista tietoturvapolitiikan rikkomuksista (Taulukko 1).

Toisin kuin rangaistusten tapauksessa, valvonnalla on todettu olevan positiivinen vaikutus henkilöstön tietoturvapolitiikan noudattamiseen (Herath & Rao, 2009b). Tämä saattaa johtua siitä, että kiinnijäämisen todennäköisyys vaikuttaa peloteteorian ominaisuuksista vahvimmin henkilön käyttäytymiseen. (Hollinger & Clark, 1983). Valvonta myös viestii henkilöstölle johdon mielipidettä tietoturvapolitiikasta, jolloin organisaation kulttuuri saattaa kehittyä. Valvonta on organisaation näkökulmasta tärkeä keino parantaa tietoturvapolitiikan noudattamista. Samalla tavoin kuin rangaistukset, myöskään valvonta ei paranna henkilöstön mielipidettä tietoturvapolitiikasta (Leach, 2003), jolloin organisaatiot joutuvat pohtimaan missä määrin haluavat näillä henkilöstöään uhkailla. Valvonta ei auta henkilöstöä saavuttamaan maksimaalista suorituskykyä, vaan ainoastaan vaaditun minimin.

4 YHTEENVETO JA POHDINTA

Henkilöstöön kohdistuvat odotukset tietoturvan osalta ovat kasvaneet organisaatioissa, kun siihen liittyvien työkalujen käyttö on siirtynyt käyttäjien vastuulle. Samalla tietoturvauhat ovat alkaneet enenevässä määrin kohdistaa hyökkäyksiään juuri käyttäjiä kohtaan. Käyttäjien tiedot näistä uhista ovat kuitenkin usein puutteellisia, jolloin heidän vastuullaan olevien tietoturvaominaisuuksien hallinta on vailla tietoon perustuvaa pohjaa. Ilman riittävää tietotaitoa henkilöstö helposti sivuuttaa työkalujen käytön, koska se nähdään ylimääräisenä työnä, joka vie huomion pois tärkeämmistä tehtävistä, ja vaikeuttaa aikatauluissa pysymistä.

Tietoturvapolitiikka pyrkii selventämään henkilöstöön kohdistuvia odotuksia sekä tarjoamaan toimintaohjeita tietoturvan varmistamiseksi. Se ei kuitenkaan aina pysty selventämään tietoturvan tarvetta henkilöstölle riittävästi, sillä henkilöstö ei aina noudata sen vaatimuksia. Syitä tietoturvan noudattamatta jättämiseen on useita:

- Henkilöstöllä ei ole riittävästi tietoa uhista tai niiltä suojautumisen menetelmistä.
- Tietoturvapolitiikka on huonosti rakennettu, jolloin se on ristiriidassa organisaation kulttuurin kanssa – henkilöstö näkee tietoturvapolitiikan olevan irrationaalinen.
- Tietoturvapolitiikka ei ole riittävän hyvin saatavilla, tai siihen tutustumiseen ei ole aikaa eikä apua.
- Henkilöstön entiset työskentelytavat ovat ristiriidassa tietoturvapolitiikan kanssa.
- Henkilöstö turvautuu neutralisoiviin tekniikkoihin.

Koska tietoturvapolitiikan noudattamatta jättämiselle on useita syitä, organisaatioiden tulevaisuuden haasteena on henkilöstön motivointi. Tutkielman tutkimuskysymys oli: *Millaisia eri tietoturvapolitiikan noudattamiseen tähtääviä keinoja on olemassa?* Henkilöstön motivoimiseksi ja siten tietoturvapolitiikan noudattamisen edistämiseksi ei ole yhtä oikeaa keinoa, vaan sitä käsittelevä kirjallisuus keskittyy yleensä yhteen aiheeseen kerrallaan. Kun nämä keinot kootaan yhteen,

saadaan viisi motivoinnin osa-aluetta: koulutus, valvonta, organisaation kulttuurin muokkaaminen, palkkiot ja rangaistukset. Nämä osa-alueet ovat esillä pääosin kaikissa organisaatioissa, mutta niiden merkitystä henkilöstön motivoinnin kannalta ei välttämättä tiedosteta.

Organisaation kulttuurin muokkaamisen merkitys tietoturvapolitiikan noudattamisen edistämiseksi on selkeä. Mikäli kaikki organisaatiossa näkevät tietoturvan tarpeellisena, siitä tulee pitkällä aikavälillä automaattista toimintaa osana jokapäiväistä työskentelyä. Organisaation kulttuurin muokkaaminen on tiukasti sidoksissa muihin motivoinnin osa-alueisiin, sillä pääosin kaikki organisaation toimet tietoturvan edistämiseksi edistävät myös organisaation kulttuurin kehitystä.

Koulutus on nähty tärkeänä osana organisaation kulttuurin kehittämistä, sillä se ei toimi tehokkaasti, ellei henkilöstö ole vastaanottavainen. Se on lisäksi keino, jolla voidaan auttaa henkilöstöä ymmärtämään tietoturvapolitiikan merkitystä, uhkia ja suojautumiskeinoja. Siten sen avulla voidaan vastata suurimpaan osaan henkilöstön motivaation ongelmista.

Palkkiot ovat tietoturvapolitiikan motivoinnin osa-alueista kyseenalaisin alue. Kirjallisuuden mukaan palkkioiden antaminen ei vaikuta merkittävästi henkilöstön aikomukseen noudattaa tietoturvapolitiikkaa. Itse kuitenkin kyseenalaistan tämän väitteen, sillä tutkimukset ovat pääasiassa kohdistuneet hyvin palkattuun henkilöstöryhmään. Siten väitän että keino on pätevä, mikäli kohderyhmä osataan valita oikein. Kuitenkin aihealue tarvitsee lisää tutkimusta, jotta palkkioiden merkitys voidaan arvioida tarkemmin.

Rangaistukset ovat toinen ryhmä, jonka merkitys henkilöstön motivoinnin kannalta on kyseenalainen. Vaikka rangaistusten on usein nähty toimivan useilla motivoinnin osa-alueilla, niiden ei ole todettu vaikuttavan tietoturvapolitiikan noudattamiseen positiivisesti, vaan niiden vaikutus on jopa päinvastainen. Kuitenkin kuten Harrington (1996) toteaa, ne eivät ole pelkästään pelotetoiminto, vaan ne tarjoavat organisaatiolle selkeät toimintalinjat tietoturvapolitiikan rikkojia vastaan, jolloin ne ovat tärkeä osa organisaatioiden motivoinnin keinoja.

Valvonta perustuu samaan peloteteoriaan kuin rangaistukset, mutta niiden positiivinen merkitys tietoturvapolitiikan noudattamisen tehostamiseksi on selkeä. Valvonnan avulla voidaan saada henkilöstö toimimaan organisaation haluamalla tavalla. Valvonnan on myös todettu olevan ainoa keino saada selville, noudattaako henkilöstö tietoturvapolitiikkaa. Kuitenkin valvonta saattaa rangaistusten tavoin vaikuttaa työilmapiiriin, jolloin organisaatioiden tulee pohtia missä suhteessa toteuttavat näitä keinoja. Valvonnan avulla henkilöstöstä saadaan irti minimi, kun taas kannustuksella ja positiivisella ilmapiirillä siitä voidaan saada irti maksimi.

LÄHTEET

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security, 26*(4), 276-289.

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

Baskerville, R., Straub, D. W., & Goodman, S. E. (2008). *Information security: Policy, processes, and practices*. Armonk, NY: M.E. Sharpe.

Bentham, J. (1791). *Panopticon or the inspection house*

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.

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.

Calder, A., & Watkins, S. G. (2010). *Information security risk management for ISO27001/ISO27002*. Cambridgeshire: IT Governance Pub.

Chia, P., Maynard, S., & Ruighaver, A. (2002). Understanding organizational security culture. *Proceedings of PACIS2002.Japan,*

Furnell, S., & Clarke, N. (2012). Power to the people? the evolving recognition of human aspects of security. *Computers & Security, 31*(8), 983-988. doi:http://dx.doi.org.ezproxy.jyu.fi/10.1016/j.cose.2012.08.004

Harrington, S. J. (1996). The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly,* , 257-278.

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

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165. doi:http://dx.doi.org.ezproxy.jyu.fi/10.1016/j.dss.2009.02.005

Hollinger, R. C., & Clark, J. P. (1983). Deterrence in the workplace: Perceived certainty, perceived severity, and employee theft. *Social Forces, 62*(2), 398-418.

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

Jaeger, P. T., Lin, J., & Grimes, J. M. (2008). Cloud computing and information policy: Computing in a policy cloud? *Journal of Information Technology & Politics, 5*(3), 269-283. doi:10.1080/19331680802425479

Kotimaisten kielten keskus (2015). Kielitoimiston sanakirja. Viitattu 6.4.2015. http://www.kielitoimistonsanakirja.fi/netmot.exe?motportal=80

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security, 28*(7), 509-520.

Leach, J. (2003). Improving user security behaviour. *Computers & Security, 22*(8), 685-692. doi:http://dx.doi.org.ezproxy.jyu.fi/10.1016/S0167-4048(03)00007-5

Meso, P., Ding, Y., & Xu, S. (2013). Applying protection motivation theory to information security training for college students. *Journal of Information Privacy and Security, 9*(1), 47-67.

Ng, B., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 46*(4), 815-825. doi:http://dx.doi.org.ezproxy.jyu.fi/10.1016/j.dss.2008.11.010

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on,* 156b-156b. doi:10.1109/HICSS.2007.206

Peace, A. G., Galletta, D. F., & Thong, J. Y. (2003). Software piracy in the workplace: A model and empirical test. *Journal of Management Information Systems, 20*(1), 153-177.

Puhakainen, P. (2006). A Design Theory for Information Security Awareness. Oulun Yliopisto. Tieto- ja sähkötekniikan tiedekunta. Tietojenkäsittelytieteiden laitos.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly, 34*(4), 767-A4.

Renaud, K., & Goucher, W. (2014). The curious incidence of security breaches by knowledgeable employees and the pivotal role a of security culture. Teoksessa T. Tryfonas, & I. Askoxylakis (toim.), (s. 361-372) Springer International Publishing. doi:10.1007/978-3-319-07620-1_32

Richardson, R. (2011). CSI 15th annual computer crime and security survey. *Computer Security Institute (CSI),*

Ross, B., Jackson, C., Miyake, N., Boneh, D., & Mitchell, J. C. (2005). Stronger password authentication using browser extensions. *Usenix Security,* 17-32.

Schlienger, T., & Teufel, S. (2003). Analyzing information security culture: Increased trust by an appropriate information security culture. *Database and Expert Systems Applications, 2003. Proceedings. 14th International Workshop on,* 405-409.

Siponen, M., Pahnila, S., & Mahmood, A. (2006). Factors influencing protection motivation and IS security policy compliance. *Innovations in Information Technology, 2006,* 1-5. doi:10.1109/INNOVATIONS.2006.301907

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer, 43*(2), 64-71. doi:10.1109/MC.2010.35

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly, 34*(3), 487-A12.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security, 24*(2), 124-133. doi:http://dx.doi.org.ezproxy.jyu.fi/10.1016/j.cose.2004.07.001

Straub Jr, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255-276.

Symantec (2015). Botit ja bottiverkot - kasvava uhka. Viitattu 29.4.2015. https://fi.norton.com/botnet

Talouselämä (2015). Keva jakaa yli 2 miljoonaa tulospalkkioina - henkilöstö saa kuukauden palkan bonuksena. Viitattu 22.4.2015. http://www.talouselama.fi/uutiset/keva+jakaa+yli+2+miljoonaa+tulospalkkioina++henkilosto+saa+kuukauden+palkan+bonuksena/a2300784

Thomson, K., & Von Solms, R. (2005). Information security obedience: A definition. *Computers & Security, 24*(1), 69-75.

Thomson, K., von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security, 2006*(10), 7-11.

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

Von Solms, R., & Von Solms, B. (2004). From policies to culture. *Computers & Security, 23*(4), 275-279.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security, 23*(3), 191-198.

Warkentin, M., Johnston, A. C., & Shropshire, J. (2011). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems, 20*(3), 267-284.