

Tietoturvakoulutus pelastuslaitoksessa

Koulutuksen vaikutus tietoturvaohjeiden noudattamiseen

Oulun yliopisto
Tietojenkäsittelytieteiden laitos
Pro gradu tutkielma
Pentti Ukkola
25.3.2008

Tiivistelmä

Tämän tutkimuksen tavoitteena oli tutkia empiirisesti tietoturvakoulutuksen vaikutuksia pelastuslaitoksen henkilökunnan aikomukseen noudattaa tietoturvaohjeita ja sitä, kuinka pelastuslaitoksen erityispiirteet huomioon ottava koulutus koettiin. Tietoturvakoulutus annettiin noudattamalla valmista koulutusmallia, joten yhtenä tutkimuskysymyksenä oli myös verrata saatuja tuloksia käytetyllä mallilla aiemmin suoritettun tietoturvatutkimuksen tuloksiin.

Koulutuksen jälkeen suoritettun kyselyn perusteella koulutus paransi vastaajien asenteita tietoturvaohjeiden noudattamista kohtaan. Tuloksista käy myös ilmi, että koulutus koettiin tärkeäksi ja sen vaikutuksia koulutettavat arvioivat myönteisesti. Koulutusmalli, jolla pystyttiin ottamaan huomioon pelastuslaitoksen erityispiirteet, sopi siten tietoturvakoulutuksen malliksi myös viranomaisorganisaatioon.

Suomessa ei ole yhtenäistä tietoturvallisuuslainsäädäntöä, vaan tietoturvallisuutta koskevat säädökset sisältyvät useihin eri lakeihin ja asetuksiin. Tämä aiheuttaa haasteita tietoturvan hallintaan, sillä tietoturvasäädösten tunteminen on yksi edellytys sille, että tietojen luottamuksellisuus, eheys ja saatavuus turvataan. Kansalaisten on kaikista tietoturvallisen toiminnan aiheuttamista haasteista huolimatta pystyttävä luottamaan siihen, että heitä koskevissa asioissa viranomaisilla on kyky ja taito toimia lain edellyttämällä tavalla. Vaikka viranomaisilta odotetaan hyvää tietoturvan hallintaa, eivät viranomais tahot, kuten esim. pelastuslaitokset ole aiemmin olleet tietoturvatutkimuksen kiinnostuksen kohteena. Tämän tutkimuksen tieteellisenä kontribuutiona on viranomaisorganisaation tuominen tietoturvatutkimuksen piiriin.

Asiasanat

Pelastuslaitos, viranomainen, tietoturvatietoisuus, asenne, aikomus, motivaatio, tietoturvakoulutus.

Sisällys

TIIVISTELMÄ	2
SISÄLLYS	3
1. JOHDANTO	4
1.1 TUTKIELMAN RAKENNE	5
1.2 TUTKIMUSMENETELMÄ	5
1.3 TUTKIMUKSEN TAUSTA.....	6
1.4 TUTKIMUSKOHDDE	6
1.5 TUTKIMUKSEN RAJAUKSET	7
2. TUTKIMUSMALLI JA TUTKIMUSONGELMAT	9
2.1 THE UNIVERSAL CONSTRUCTIVE INSTRUCTIONAL THEORY (UCIT)	9
2.2 PELASTUSLAITOKSEN TIETOTURVAKOULUTUKSEN NELJÄ VAIHETTA	11
3. KATSAUS TUTKIMUSKIRJALLISUUTEEN	13
3.1 TIETOTURVAN MÄÄRITTELY	13
3.2 TIETOTURVA JA TIETOTURVATIE TOISUUS	15
3.3 TIETOTURVAN HALLINTA.....	19
3.4 TIETOTURVAKOULUTUS.....	22
3.5 JOHTOPÄÄTÖKSET TEORIOISTA.....	25
4. EMPIIRINEN TUTKIMUS TIETOTURVAKOULUTUKSEN VAIKUTUKSISTA	27
4.1 EMPIIRISEN TUTKIMUKSEN TULKINTAKEHYS	27
4.2 MITTARIT JA MENETELMÄT	34
4.3 SUMMAMUUTTUIJEN MUODOSTAMINEN.....	35
4.4 TIETOTURVAKOULUTUKSEN KÄYTÄNNÖN TOTEUTUS JA AINEISTON KERÄÄMINEN.....	36
4.5 AINEISTON KOODAAMINEN	37
4.6 MITTAREIDEN LUOTETTAVUUS JA PÄTEVYYS	38
5. EMPIIRISEN TUTKIMUKSEN TULOKSIEN TARKASTELU	40
5.1 KÄYTETYT ANALYYSIMENETELMÄT	40
5.1.1 SEM-mallinnus ja PLS.....	41
5.1.2 Korrelaatioanalyysi	42
5.2 SUORITETTUIJEN KYSELYJEN VASTAUSTEN ANALYSOINTI	42
5.3 FORMATIIVISEN SEM-MALLINNUKSEN TULOKSET	45
6. POHDINTA JA JOHTOPÄÄTÖKSET	52
LÄHTEET	55
LIITE A. OPPIJAKESKEISEN OPETUKSEN TEORIA	60
LIITE B. ENSIMMÄISEN KYSELYN KYSYMYKSET	62
LIITE C. TOISEN KYSELYN KYSYMYKSET	68
LIITE D. ENSIMMÄISEN KYSELYN TOINEN OSIO	70
LIITE E. KYSELYKAAVAKE PELASTUSLAITOSTEN TIETOHALLINNOLE	74
LIITE F. FORMATIIVISEN SEM-MALLINNUKSEN VALIDOINNIN TULOKSET	75
TAULUKKO 1. VALIDOINNIN KESKEISET TULOKSET ENNEN KOULUTUSTA.	75
TAULUKKO 2. VALIDOINNIN KESKEISET TULOKSET KOULUTUKSEN JÄLKEEN.	77
LIITE G. ENSIMMÄISEN KYSELYN SUMMAMUUTTUIJAT	78
LIITE H. TOISEN KYSELYN SUMMAMUUTTUIJAT	81

1. Johdanto

Nykyaikaiset organisaatiot ovat riippuvaisia tietotekniikasta (Dibbern, Goles, Hirschheim ja Jayatilaka, 2004). Riippuvuus tietotekniikasta tekee organisaatioista kuitenkin myös haavoittuvia, sillä niiden toimintaan kohdistuu ulkoisia ja sisäisiä tietoturvauhkia, joista vaikeimmin torjuttavia ovat organisaation sisältä tulevat tietoturvauhat (Stanton, Stam, Mastrangelo ja Jolton, 2004, sekä D'Arcy ja Hovav, 2007). Esimerkiksi vuonna 2001 Computer Security Institutun mukaan 60 % rikkomuksista oli organisaatioissa työskentelevän tekemiä, joten päinvastaisista luuloista huolimatta suurimman osan tietoturvarikkomuksista aiheuttaa nimenomaan organisaation oma työntekijä (Lee ja Lee, 2002.)

Paraskaan tekniikka ei auta täysin estämään väärinkäytöksiä, sillä vain 10–20 % tietoturvaongelmista on teknisiä, loput johtuvat inhimillisistä tekijöistä (Torres, Sarriegi, Santos ja Serrano, 2006). Inhimillisten tekijöiden minimoimiseksi organisaation tulee luoda sellainen turvallisuuskulttuuri, jossa yksittäinen käyttäjä ymmärtää organisaation tavoitteet ja haluaa sitoutua niihin. Tähän päästään tuomalla työntekijöille tehokkaasti tietoon organisaation visio, säännöt ja ohjeet. Koulutus ja opastus ovat yksi tapa toteuttaa se (Torres et al., 2006, vrt. Schlienger, 2003.) Tietoturvatietoisuuteen vaikuttamisen problematiikkaa tutkitaan nykyään myös yhä enemmän (Siponen ja Oinas-Kukkonen, 2007). Pyrkimyksenä on löytää käyttäjien tietoturvakäyttäytymistä selittäviä tekijöitä tekniikasta, sekä ihmisestä itsestään (Aytes ja Conolly, 2003).

Pelastusalalla on tapahtunut viimevuosina merkittäviä muutoksia. Kunnallisista palolaitoksista on siirrytty alueellisiin pelastuslaitoksiin, jolloin alueellisen hajanaisuuden vuoksi monet toiminnot tapahtuvat verkossa. Onnettomuusselosteiden, potilas- ja kohdetietojen osalta ollaan siirtymässä sähköiseen arkistointiin. Hälytystietojen perillemenon, hälytysaikaisen informaation, sekä -raportoinnin onnistuminen vaatii käyttäjiltä järjestelmä- ja laitetason osaamista. Edellä esitelty toimintaympäristön ja työtapojen muutos on haasteellista tietoturvan kannalta.

Tutkimuskohteena olleessa pelastuslaitoksessa aloitettiin syksyllä 2007 parempaan tietoturvan hallintaan tähtäävä kehitystyö. Tietoturvakoulutus on tärkeä osa kehitystyötä ja yksi keino edistää tietoturvaohjeiden sisäistämistä (Siponen, 2000). Tässä opinnäytetyössä tutkittiin pelastuslaitoksessa suoritetun tietoturvakoulutuksen vaikutusta työntekijöiden aikomukseen noudattaa tietoturvaohjeita ja koulutettavien kokemuksia koulutuksen hyödyllisyydestä. Kun puhutaan tietoturvatietoisuudesta, usein tarkoitetaan yksilön aikomusta noudattaa tietoturvaohjeita.

Pelastuslaitoksissa (22 kpl) tietohallintoa ei ole järjestetty yhdenmukaisesti¹. Valtaosa laitoksista tukeutuu keskuskunnan tietohallintoon, missä ei välttämättä ymmärretä alan

¹ Tutkimuksen alkuvaiheessa pelastuslaitoksille tehtiin kysely, jossa selvitettiin laitosten tietoturvakäytäntöjä. Osa kyselyyn osallistuneista toivoi joidenkin kohtien käsittelemistä luottamuksellisesti, mistä syystä kaikkia tuloksia ei esitellä.

erityispiirteitä. Toisaalta laitoksissa, joissa tietohallinto hoidetaan oman organisaation puitteissa, tietoturvasubstanssia ei välttämättä löydy. Tähän mennessä julkishallinnon organisaatiot ovat olleet harvoin tietoturvatutkimuksen kohteena. Tästä syystä pelastuslaitoksen valitsemista kohdeorganisaatioksi voidaan pitää perusteltuna. Tutkimuksen ollessa vielä kesken, se herätti mielenkiintoa tietoturvasta vastaavien keskuudessa pelastusalan sisällä.

1.1 Tutkielman rakenne

Tutkielman johdanto-osassa esitellään tutkimuksen motiivien ja tutkimusmenetelmien lisäksi tutkimuskohde, tutkimuksen taustat ja rajaukset. Tutkielman toinen pääluke sisältää tutkimusmallin ja tutkimusongelmien esittelyt. Katsaus tutkimuskirjallisuuteen ja tämän tutkielman suhde aiempaan tutkimukseen käsitellään kolmannessa pääluvussa.

Neljäs pääluke käsittää empiirisen tutkimuksen kuvauksen pelastuslaitoksessa. Tässä luvussa esitellään tutkimuksessa käytetyt mittarit ja menetelmät, sekä kuvataan tutkimuskohteena ollut koulutusprosessi ja aineiston keruu. Luvun lopussa arvioidaan mittarien luotettavuus ja pätevyys.

Viidennessä pääluvussa tarkastellaan tutkimuksen tuloksia. Ensiksi esitellään käytetyt analyysimenetelmät: SEM-mallinnus ja PLS, sekä korrelaatioanalyysi. Koulutusta ennen ja jälkeen suoritettujen kyselyiden analysointi suoritetaan viidennen luvun alaluvuissa. Viimeinen eli kuudes pääluke keskittyy tulosten pohdintaan ja johtopäätösten tekoon.

1.2 Tutkimusmenetelmä

Tämä tutkimus on kvantitatiivinen tutkimus, jota käytetään melko paljon sosiaali- ja yhteiskuntatieteissä. (Hirsjärvi, Remes ja Sajavaara, 2004). Tässä tutkimuksessa käytettiin datan keräämiseen kolmea kyselyä. Kyselyt valittiin tiedonkeruun menetelmäksi muun muassa siksi, että ne sopivat kvantitatiivisen eli määrällisen tutkimuksen havaintoaineiston keruumenetelmiksi. Niiden avulla voitiin melko vaivattomasti kerätä riittävän suuri määrä dataa, jonka avulla selvitettiin suoritettujen koulutuksen ja tietoturvatietoisuuden välillä mahdollisesti vallitseva kausaalisuuhde. Kausaalisuus voidaan päätellä, jos voidaan todistaa, että muuttamalla riippuvan muuttujan arvoa, vaikutetaan riippumattoman muuttujan arvoon toisessa muuttujassa (Lewin, 2004).

Kyselytutkimus ei myöskään vaadi niin paljon menetelmäosaamista, kuin muut aineistonkeruumenetelmät ja sen avulla oli helppo tehdä yleistyksiä tutkimustuloksista ja se sopi hyvin tutkittaessa vastaajien mielipiteitä tutkittaviin asioihin. Tässä tutkimuksessa kyselyillä saatuja tuloksia voidaan pitää luotettavina, koska vastaajien anonymiteetti pystyttiin takaamaan. Anonymiteetin takaaminen on yksi edellytys vastausten luotettavuudelle. Tämä onnistuu kyselyissä yleensä paremmin, kuin muissa aineistonkeruumenetelmissä (Muijs, 2004.)

Usein pragmaattisessa lähestymistavassa tutkimukseen valitaan käyttökelpoisin tutkimusmetodi (Muijs, 2004). Hirsjärvi et al. (2004) antavat hyväksi ohjeeksi tutkimusta suunnitteleville valita sellainen lähestymistapa ja metodi, jonka käyttökelpoisuudesta hän itse on vakuuttunut. Tämän tutkimuksen tutkimuskysymysten kannalta valitut me-

netelmät tuntuivat käyttökelpoisimmilta, koska tutkimuksen kohteena olevan pelastuslaitoksen henkilökunta työskentelee kahdessakymmenessä kahdessa toimipisteessä, tutkimuksen tiedonkeruu ja tutkimuskohteena ollut koulutus kesti lähes kolme kuukautta ja se toteutettiin viidessä eri koulutusilaisuudessa.

Tutkimusongelmaa lähestyttäessä pragmaattisesti selvitetään siis ensin, minkälaisiin tutkimuskysymyksiin ajateltu metodi sopii. Kvantitatiivisen metodin avulla voidaan vastata sellaisiin tutkimuskysymyksiin, jotka edellyttävät 1) määrien esittämistä, 2) määrällisen vaihtelun havainnointia 3) ilmiöiden selittämistä, tai 4) hypoteesien todistamista (Mujis, 2004.) Kvantitatiiviseen tutkimusmetodiin kuuluu oleellisesti luotettavuuden kelpoisuuden ja yleistettävyyden vaatimus. Tällä tarkoitetaan sitä, että samat tulokset saadaan uusilla mittauskerroilla. Kelpoisuus saavutetaan jos varmistetaan siitä, että tutkimustulokset vastaavat tutkimuskysymyksiin. Tulokset voivat olla luotettavia, vaikka eivät olisikaan kelvollisia. Sen sijaan tutkimustulokset, jotka eivät ole luotettavia eivät ole kelvollisiakaan (Lewin, 2004).

1.3 Tutkimuksen tausta

Vuonna 2002 tutkimuksen kohteena olevan pelastuslaitoksen keskuskunnassa tehtiin tietoturvan esiselvitys ulkopuolisen konsultin toimesta. Raportin pohjalta aloitettiin tietoturvan hallinnan kehitystyö. Todenteolla kehitystyö alkoi kuitenkin vasta vuoden 2004 jälkeen ja tietoturvapoliittikka ja tietoturvaohjeistus laadittiin vuoden 2005 keväällä. Tietoturvapoliittikan laatimisen yhteydessä suoritettiin riskikartoitus haastattelemalla kaupungin virastojen avainhenkilöitä. Riskikartoituksessa löydettyihin puutteisiin kiinnitettiin ohjeistuksen laatimisessa huomiota siten, että ohjeistuksen painopiste on käytäjätasolla. Ohjetta laadittaessa tiedostettiin se, että pelkkä ohje ei riitä, vaan tietoturvatietoisuutta on lisättävä ja työntekijöiden sitoutumista ohjeiden noudattamiseen on ylläpidettävä jatkuvalla koulutuksella.

Kaupungin tapaisessa erilaisiin virastoihin jakautuneessa organisaatiossa yhtenäisen tietoturvatason saavuttaminen on haasteellista. Virastot edustavat erilaisia toimintakulttuureita ja niillä on toisistaan poikkeavat tehtävät. Ne sijaitsevat kaiken lisäksi fyysisesti erillään toisistaan ja ovat työntekijämääriltään hyvin erikokoisia.

Koulutuksen avulla kaupungin tietoturvapoliittikka ja – ohjeet esitellään kaikille työntekijöille, mikä yhtenäistää tietoturvakäytännöt eri hallintokuntien välillä. Pelastuslaitos oli ensimmäinen virasto, jossa tietoturvakoulutus toteutettiin.

1.4 Tutkimuskohde

Tutkimuskohteena oleva pelastuslaitos syntyi vuonna 2004, jolloin 22 kunnan pelastustoimet yhdistettiin yhdeksi alueelliseksi pelastuslaitokseksi. Alueellisten pelastuslaitosten hallintomalleista yleisin on sellainen, jossa jokin alueen kunnista on ottanut hoidaakseen alueellisen pelastustoimen. Tässä tutkittavassa tapauksessa pelastuslaitos toimii hallinnollisesti keskuskunnan virastona. Pelastuslaitoksessa on runsas sata työntekijää, asemien koon vaihdellessa muutaman miehen asemasta useamman kymmenen henkilön paloasemaan.

Pelastuslaitoksessa työskentelevän henkilökunnan tietotekniset valmiudet vaihtelevat huomattavasti. Hallinnossa ja esimiestehtävissä työskentelevien on hallittava tietotekniset perustaidot selvitäkseen työtehtävistään. Sen sijaan miehistöltä ei tähän mennessä ole työtehtävistä selviytymiseen edellytetty tietotekniikan hallitsemista. Tässä ryhmässä tietoteknisten taitojen kehittäminen on ollut työntekijän oman kiinnostuksen varassa. Muutaman viime vuoden aikana pelastuslalle on tullut kuitenkin yhä enemmän tietoteknisiä valmiuksia vaativia sovelluksia. Palotarkastus tullaan jatkossa suorittamaan pda-päätelaitteilla. Niin sanottu pelastuksen kenttäjohto – ohjelmisto (*PEKE*) ja sen tarvitsemat päätelaitteet tulevat vuoden 2008 aikana pelastusyksiköihin. Edellisten johdosta pelastuslaitoksen työpaikkakoulutuksessa on henkilökunnan tietoteknisten valmiuksien lisääminen aloitettu.

Pelastuslaitoksissa henkilökunnan säännöllisellä koulutuksella on suuri merkitys, sillä työntekijöiden tiedollisille ja taidollisille valmiuksille asetetaan paljon vaatimuksia. Henkilökunnan psyykkisiä ja fyysisiä ominaisuuksia testataan säännöllisesti. Tämän johdosta pelastuslaitoksissa koulutusta pidetään luonnollisena osana päivittäistä työruutiinia. Koulutusmyönteisyys mahdollistaa myös tietoturvakoulutuksen ottamisen osaksi säännöllistä työpaikkakoulutusta. Ongelmia tuottaa tietoturvan alalle tuoma vieras asiatekijäkokonaisuus ja koulutettavien erilaiset perustiedot tietotekniikasta.

1.5 Tutkimuksen rajaukset

Tietoturvakoulutus on tärkeä osa tietoturvan hallintaprosessia. Koulutuksen lisäksi siihen kuuluu teknisiä ratkaisuja ja hallinnollisia toimia (Pfleeger, Schramm ja Palmer, 2007 ja Wang, 1987.) Tietoturvatietoisuuteen vaikuttavia mekanismeja ymmärtää paremmin jos ymmärtää myös tietoturvan hallintaprosessia. Siksi tietoturvan hallintaprosessia käsitellään varsin laajasti luvun kolme kirjallisuuskatsauksessa.

Mikä osa tietoturvan hallintaprosessin kehittämisestä aiheutuvalla tietoturva-asioiden esillä pitämällä on tutkimushetken tietoturvatietoisuuden kasvuun, rajattiin tässä tutkimuksessa pois ja keskityttiin koulutuksen vaikutusten tutkimiseen. Ainakin johdon ja hallinnon henkilökunta on tietoturvan hallintaprosessin kehitystyön parissa työskennellyt tietoturva-asioiden kanssa. Tällä saattaa olla samanlaisia myönteisiä vaikutuksia tietoturvatietoisuuteen, kuin Puhakaisen väitöskirjassa esitellyllä kampanjoinnilla (Puhakainen, 2006). Vaikka Puhakaisen (2006) esittelemällä koulutusmallilla oli keskeinen rooli tutkimuksessa, ei tämän tutkimuksen yhteydessä testattu mallia eikä teoriaa, vaan niiden rooli oli tutkimuksen tavoitteiden täsmentämisessä ja ohjaamisessa

Tutkimuksen rajausta mietittäessä päädyttiin siihen, että pelastuslaitoksen lisäksi sen taustaorganisaation ottaminen mukaan tutkimukseen veisi liikaa aikaa ja olisi Pro Gradu-tutkielmaa silmällä pitäen liian laaja kohde. Tämän johdosta koulutuksen vaikutuksen tutkiminen rajattiin pelastuslaitokseen.

Kvalitatiivista tutkimusmetodia olisi tässä tutkimuksessa voitu käyttää yhdessä kvantitatiivisen kanssa. Kvalitatiivisena metodina kysymykseen olisivat tulleet silloin lähinnä teemahaastattelut tai observointi. Observointi hylättiin sen vuoksi, että havainnoitsijana olisi tässä tapauksessa toiminut henkilökunnan kouluttaja, joten objektiivisuuden todentaminen olisi saattanut tuottaa liikaa hankaluuksia. Vaikka aivan näihin päiviin tutkimuspiireissä kvalitatiivisen ja kvantitatiivisen tutkimusparadigman yhdistämistä on haluttu välttää (Mujis, 2004), niin triangulaatio, tai sekametodi (*Mixed Method*) olisi

voinut tuoda vahvuutta tällaiseen empiiriseen tutkimukseen. Kvalitatiivisen ja kvantitatiivisen tutkimusparadigman yhdistäminen olisi ollut Pro Gradun mittakaavassa haastavaa ja työlästä. Sen vuoksi teemahaastatteluistakin luovuttiin.

2. Tutkimusmalli ja tutkimusongelmat

Tässä luvussa esitellään tämän tutkimuksen tutkimuskohteena olleen koulutuksen teoreettinen viitekehys, siitä johdettu tutkimusmalli ja tutkimuskysymykset. Koulutuksen teoreettiseksi viitekehyyksi otettiin Puhakaisen väitöskirjassa (Puhakainen, 2006, s. 74–76) esitelty tietoturvakoulutuksen suunnittelumalli, jonka UCIT (*The Universal Constructive Instructional Theory*)-ydinteoriasta johdettiin tämän tutkimuksen tutkimusmalli (kuva 2 s. 12). Sen tarkoituksena on kuvata tutkimuskohde ja tutkimuksen kulku mahdollisemman selvästi.

Puhakainen (2006) esittelee suunnitteluteorian (*Design Theory*)², joka on yleinen tapa esitellä prosesseja, joiden tuloksena syntyy jokin artefakti, tässä tapauksessa koulutusmalli. Suunnitteluteorian avulla tuotetaan siis artefakti. Puhakaisen (2006) mallissa on kolme pääelementtiä: tietoturvakoulutus, tietoturvan markkinointi, sekä palkitseminen ja rangaistukset.

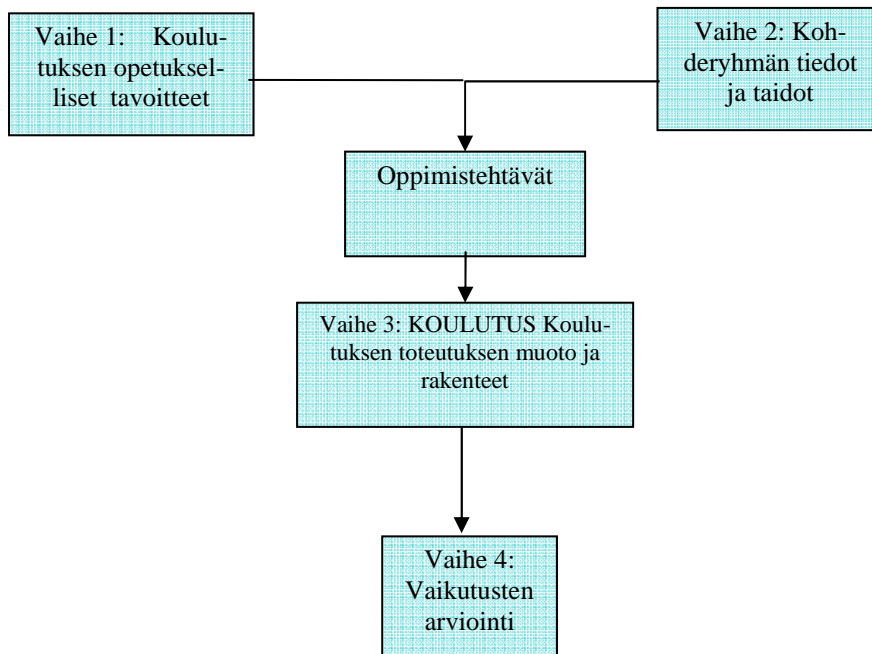
Suunnitteluteorian mukaisesti Puhakainen (2006) esittelee tietoturvatietoisuusohjelmansa ydinteoriat. Tässä tutkimuksessa käytetään Puhakaisen (2006) esittelemän tietoturvatietoisuuskoulutuksen toista ydinteoriaa, joka on konstrukttiivinen koulutusteoria (*The Universal Constructive Instructional Theory*, UCIT). Siitä käytetään tästä eteenpäin sopivan suomenkielisen termin puutteessa UCIT-lyhennettä. Tämän tutkimuksen yhtenä tutkimustehtävänä oli soveltaa käytettyä mallia pelastuslaitoksen tietoturvakoulutuksessa ja arvioida sen käyttökelpoisuus.

2.1 The Universal Constructive Instructional Theory (UCIT)

Tutkimuksessaan Puhakainen (2006) esittelee kolme uutta suunnitteluteoriaa parantamaan käyttäjien toimintatapoja tietoturvan kannalta. Tutkimuksessaan Puhakainen (2006) väittää, että tutkimuskirjallisuudessa on puutteita tietoturvatietoisuuden osalta. Lähestymistapa tietoturvatietoisuuteen kaipaa koulutusteoriaa, joka olisi empiirisesti testattu. Tämä hyödyntää käytännön tietoturvatyössä mukanaolevia, joilla ei usein ole aikaa kahlata läpi laajaa tutkimuskirjallisuutta antamalla heille työkaluksi testatun teorian. Tutkimusmaailmaa testatun teorian esitleminen hyödyntää osoittamalla tutkimuskentässä tutkitut alueet ja ne alueet jotka yhä kaipaavat lisätutkimusta (Puhakainen, 2006.) Puhakainen luettelee 59 erilaista lähestymistapaa tietoturvatietoisuuteen, joista vain muutama perustuu teoriaan joka on käytännössä testattu. Suunnitteluteorian mukaisesti tietoturvatietoisuuden kehittämisen on perustuttava kolmeen seikkaan: 1) sopiviin ydinteorioihin, 2) annettava konkreettiset ohjeet, kuinka tietoturvaohjeet huomioon ottava käyttäytymisen tila saavutetaan ja 3) asettaa testattava tutkimussuunnitelma tutkijoiden käyttöön (Puhakainen, 2006, s. 74–76).

² Joskus käytetään myös muotoa System theory, (Spillers & Newsome 1990)

Laajan tutkimuskirjallisuuden perehtymisen jälkeen Puhakainen (2006) esittelee suunnitteluteorian periaatteiden mukaiset ydinteoriat, joilla on teoreettinen tausta ja jotka ovat empiirisesti testattuja. UCIT on Puhakaisen (2006) väitöskirjassa koulutuksen ydinteoria. F. Schott ja MP. Driscoll (1997) kehittivät teorian (kuva 3), koska oppiminen on heidän mukaansa niin monimutkainen asia, jotta sitä pystyisi kuvaamaan yhdellä teoriolla riittävän laajasti kattaakseen kaikki oppimisen osa-alueet, tai toisaalta riittävän tarkasti, että siitä olisi hyötyä koulutukseen (Puhakainen, 2006, s.71).



Kuva 1. Koulutuksen neljä vaihetta Scottin ja Driscoll'n mukaan (Puhakainen, 2006).

Kuvassa esitellään koulutuksen neljä vaihetta: 1) *opetukselliset tehtävät (tavoitteet)*, 2) *koulutettavien aikaisempien kokemusten selvittäminen*, josta seuraa *oppimistehtävät (tavoitteet)*, 3) *suunniteltu opetustapahtuma*, jossa opetukselliset tehtävät ja - ympäristö on rekonstruoitu, sekä 4) *onnistumisen arviointi*. UCIT koostuu lisäksi kolmesta elementistä. Ensimmäisenä elementtinä ovat toiminnot, toisena peruskomponentit ja kolmantena olemassa olevat mahdollisuudet ja rajoitteet. Peruskomponentit sisältävät neljä osaa: 1) oppimisympäristön 2) oppimistehtävät 3) oppilaat ja 4) toiminnan puitteet, jossa koulutus annetaan (Puhakainen, 2006).

Koulutusteorian mukaan koulutuksen tulee ottaa huomioon oppilaan tiedot ja taidot. Koulutuksessa täytyy myös huomioida koulutustavoitteiden, koulutusympäristön, sekä organisationaalisten puitteiden tuomat mahdollisuudet ja rajoitteet. Koulutusteorian mukaan koulutuksen täytyy vielä mahdollistaa järjestelmällinen ja tiedostettu informaation käsittely ja motivoida opiskelijaa siihen. Tällaisia opiskelijalle tärkeitä toimintoja ovat tiedon hankkiminen, varastointi ja käyttö (Puhakainen, 2006).

Puhakaisen (2006) mukaan UCIT tarkastelee sitä käytettävissä olevaa tietoa, joka koskee sisäisen ja ulkoisen informaation mahdollisuuksien ja rajoitteiden vaikutuksia opettaviin. Lisäksi opetukseen voi vaikuttaa opetuksellisten tavoitteiden rajoitteet ja mahdollisuudet. Jotta asiaankuuluvat mahdollisuudet ja rajoitteet tulevat otetuksi huo-

mioon, opettajan pitää järjestellä opetusolosuhteet vastaamaan opetuksellisia tavoitteita. (Puhakainen ja Siponen, 2005).

2.2 Pelastuslaitoksen tietoturvakoulutuksen neljä vaihetta

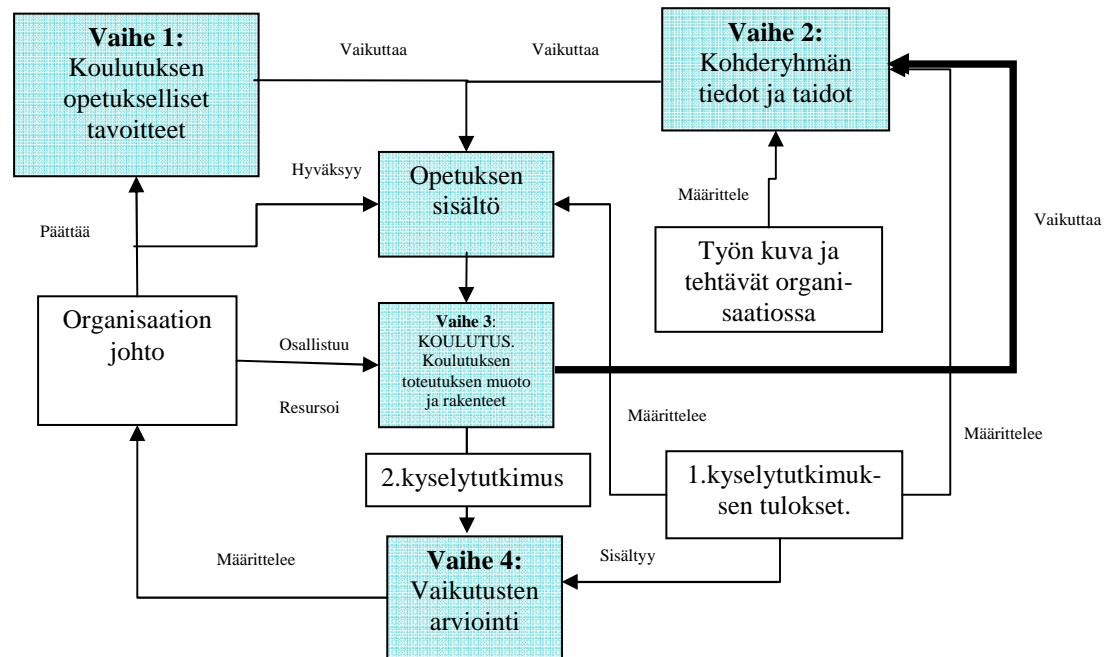
Tässä luvussa kuvataan tutkimusmalli, joka on rakennettu pelastuslaitokselle annettavan koulutusmallin ympärille. UCIT valittiin koulutusmallin ydinteoriaksi, koska se ottaa huomioon organisaation ja koulutettavien erityispiirteet (Puhakainen, 2006). Malli kuvaa tutkimuksessa kerättävän aineiston sisällön ja rakenteen ja osoittaa riippuvuus- ja vaikutussuhteita, joita tutkimuksessa halutaan selvittää. Mallin ytimenä oleva UCIT-teoria on mallissa korostettu turkoosilla värillä. Tutkimusmallissa käytetyt käsitteet määritellään seuraavassa tarkemmin.

UCIT:in ensimmäisen vaiheen mukaisesti määriteltiin johdon päättämät *opetukselliset tavoitteet*, joita pelastuslaitoksen koulutuksessa olivat: 1) tietoturvapoliittikan sisällön ja merkityksen oppiminen, 2) koulutettavien saaminen ymmärtämään kyselytutkimuksessa havaittujen ongelmien vakavuus, 3) kyselytutkimuksessa havaittujen ohjeiden noudattamisen kannalta tärkeiden seikkojen edelleen vahvistaminen ja 4) saada koulutettavat ymmärtämään käytännön esimerkein ohjeiden noudattamisen hyödyllisyys käyttäjän ja pelastuslaitoksen kannalta nimenomaan pelastuslaitoksen erityispiirteet huomioiden.

Toisessa vaiheessa käyttäjien tietoturvatietämyksen taso tutkittiin kohderyhmälle osoitetulla kyselyllä. Pari vuotta aiemmin suoritetussa riskikartoituksessa saatiin selville joitain käyttäjille tyypillisiä tietoturvaluutteita. Esimerkiksi päätteiltä uloskirjautumisessa ja asiakirjojen säilytyksessä havaittiin puutteita. Toisen vaiheen *oppimistavoitteet* määriteltiin suoritetun kyselytutkimuksen avulla. Kohderyhmien tietoja ja taitoja selvitettyä työntekijöiden työn kuva ja tehtävät organisaatiossa vaikuttivat mihin koulutettavaan ryhmään hänet sijoitettiin. Koulutuksen ensimmäinen ja toinen vaihe vaikuttivat *opetuksen sisältöön*, jonka pelastuslaitoksen johto lopullisesti hyväksyi.

Kolmannessa vaiheessa päätettiin koulutuksen *muoto ja rakenteet*, sekä toteutettiin koulutus. Tässä vaiheessa otettiin UCIT:in periaatteiden mukaisesti huomioon ne seikat, joilla parhaiten toteutetaan edellisten vaiheiden tavoitteet. Pelastuslaitoksen tapauksessa päätettiin jakaa koulutettavat ryhmiin pääsääntöisesti koulutettavien virka-aseman mukaan. Poikkeuksen muodosti johdon ja hallinnon ryhmä, jossa oli mukana kaikki suoritusportaat. Johdon tuella oli merkittävä rooli koulutuksen onnistumisen varmistamisessa. Johto osallistui koulutuksen suunnitteluun, hyväksyi sisällön ja antoi tarvittavat resurssit.

UCIT:in neljäs vaihe toteutettiin kyselyllä, jonka avulla koulutuksen *onnistuminen arvioitiin*. Kyselyä ei suoritettu välittömästi koulutustapahtuman jälkeen vaan noin viikon kuluttua koulutuksesta. Koulutettavat saivat täytettäväkseen kysymyskaavakkeet, jotka pyydettiin lähettämään nimettöminä kirjepostissa. Näin toimimalla pyrittiin säilyttämään luottamuksellisuus. Toisen kyselyn tulokset ovat johdon apuna määriteltäessä koulutuksen onnistumista, mikä puolestaan vaikuttaa johdon päätöksiin jatkotoimia suunniteltaessa.



Kuva 2. Pelastuslaitoksen tietoturvakoulutusprosessin kuvaus.

Tämän tutkimuksen päätutkimusongelmana oli tutkia pelastuslaitoksessa aloitettuun tietoturvan kehitystyöhön kuuluvan tietoturvakoulutuksen vaikutuksia käyttäjien aikomukseen noudattaa tietoturvaohjeita ja sitä, kuinka koulutettavat kokivat tietoturvakoulutuksen. Asiaa lähestyttiin koulutuksen vaikutusta tutkimalla. Sellaista tutkimusta on tehty vähän, jos ollenkaan, missä tutkitaan kohdennetun koulutuksen vaikutusta viranomaisorganisaatioissa. Tässä työssä ei ensisijaisesti testattu mallia, vaan sitä kuinka kohdeorganisaation ehdoilla suoritettu koulutus onnistui vaikuttamaan tietoturva- asenteisiin ja kuinka koulutus koettiin, mikä oli tämän opinnäytetyön ensimmäinen alatutkimusongelma. Teorian rooli oli siten tutkimuksen tavoitteiden täsmentämisessä ja ohjaamisessa. Koska koulutus on toteutettu Petri Puhakaisen väitöskirjassa esitetyn mallin mukaisesti (Puhakainen, 2006), niin toisena alatutkimusongelmana oli selvittää, soveltuiko Puhakaisen (2006) esittelemä malli tällaisen koulutuksen järjestämiseen. Tutkimuskysymyksiin pyrittiin löytämään ratkaisu empiirisen tutkimuksen avulla, sekä teoreettisen tarkastelun kautta tutustumalla tutkimuskirjallisuuteen.

Sen lisäksi, että tämän tutkimuksen kontribuutiona oli tuoda pelastuslaitos tietoturvatutkimuksen kohteeksi, toisena motiivina tutkimukselle oli Puhakaisen (2006) tutkimuksessa käytetyn koulutusmallin testaaminen isommassa organisaatioissa. Tutkimuksen tuloksena olisi siten käyttökelpoinen ja empiirisesti tutkittu koulutusmalli tietoturvakoulutukseen pelastuslaitoksissa.

3. Katsaus tutkimuskirjallisuuteen

Aihepiiriin kuuluvaan tieteelliseen kirjallisuuteen tutustuminen ja sen pohjalta syntynyt kirjallisuuskatsaus kuuluvat tutkimusprosessin ensivaiheisiin. Kirjallisuuskatsaukseen valittavien tieteellisten artikkeleiden ja tutkimusten joukosta pyrittiin valitsemaan primaarilähteitä. Primaarilähteillä tarkoitetaan lähteitä, joissa annetaan mahdollisimman täydellinen tai ensikertainen selostus tutkimuksesta tai sen suorittamisesta (Hirsjärvi et al., 1997).

Tutkimuksen teoreettinen tarkastelu aloitetaan tutustumalla tietoturvan eri käsitteisiin tieteellisiä julkaisuja ja artikkeleita läpikäymällä. Tietoturvan hallinta koostuu monesta osatekijästä koulutuksen lisäksi, joten niiden tunteminen on tämän työn kannalta tärkeää. Tätä kirjallisuuskatsausta varten tutkittiin artikkeleita muun muassa seuraavista sähköisistä tietokannoista: ACM Digital Library, EBSCO, Elsevier Science Direct, Emerald Library, IEEE/IEE Electronic Library ja Springer Link).

Viranomaisorganisaatiota koulutuksen kohdeorganisaationa käsittelevää tutkimusta erilaisista elektronisista tietokannoista hakusanoilla ”authority + is-training” tai ”authority + instruction” ei löytynyt kuin yksi lähde: Analysis of End User security behaviors. Siinä selvitetään käyttäjien toimia organisaatioiden tietoturvan kannalta ja mainitaan armeija esimerkkinä viranomaisorganisaatiosta (Stanton et al., 2005). Tietoturva koulutuksesta ja -valistuksesta löytyi artikkeleita huomattavan paljon. Tietoturvatutkimuksen, jossa tietoturvatietoisuuden olemusta ja syntyä selvitetään, on viimeaikoina lisääntynyt. Tutkimustulokset koskevat yleensä käyttäjien tietoturvakäyttäytymistä ja tietoturvaohjeiden noudattamista tai niiden noudattamatta jättämistä, sekä pyrkivät antamaan ehdotuksia tietoturvatietoisuuden parantamiseksi. Olemassa olevasta tutkimuksesta ei kuitenkaan löydy riittävästi teoriaan ja empiriaan tukeutuvia mittareita selittämään käyttäjien tietoturvaohjeiden noudattamiseen vaikuttavia tekijöitä (Pahnila, Siponen ja Mahmood, 2007.)

3.1 Tietoturvan määrittely

Tietoturvalla ei ole yksiselitteistä ja yleisesti hyväksyttyä määritelmää. Tietoturvassa on kyse tekniikasta, prosessista ja ihmisistä ja se voidaan määritellä hyvin informoiduksi turvallisuuden tilaksi, jossa tietoriskit ja erityyppiset kontrollit ovat dynaamisesti tasapainossa (Torres et al., 2006.) Valtionvarainministeriön VAHTI- julkaisu määrittelee tietoturvan seuraavasti: ”Tietoturvallisuudella tarkoitetaan tietojen, järjestelmien, palveluiden ja tietoliikenteen asianmukaista suojaamista sekä normaali- että poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä. Tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä turvataan laitteisto- ja ohjelmistovikojen, luonnontapahtumien sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhilta ja vahingoilta” (VAHTI 5/2003, s.9). Englanninkielisessä tutkimuksessa tietoturvasta käytetään useampaa termiä; computer security, information security, data security ja joskus data protection. Information security käsitetään joskus myös tietosuojaksi. Informaation ja datan välinen suhde määräytyy usein sen mukaan, mikä olomuoto tiedolla on. Tietoturva määritellään tässä tutkimuksessa tiedon tai informaation turvaamiseksi kaikilta

tahallisilta, tai tahattomilta yrityksiltä paljastaa, muuttaa tai tuhota tietoja olipa aiheuttaja valtuutettu tai valtuuttamaton taho (Wang, 1987.)

Tietoturvatietoisuus (paremminkin voitaisiin puhua käyttäjän aikomuksesta noudattaa tietoturvaohjeita) on keino systeemin pitämiseksi turvallisena (McCovern, 2002). Torresin (2006) mukaan se on harvoja vastatoimenpiteitä ahneutta, epärehellisyyttä, tai jotain muuta käyttäjästä johtuvaa väärinkäytöstä vastaan. Sen tarkoitus on olla ennaltaehkäisevä toimenpide, joka antaa kaikille työntekijöille oikeat toimintatavat. Tietoturvatietoisuus on tärkeä siksi, että kaikki tekniset toimenpiteet, jotka tähtäävät tietoturvan parantamiseen, voidaan kiertää. Tietoturvatietoisuus suojelee tietojärjestelmiä käyttäjien väärinkäytöksiä vastaan (Siponen ja Kajava, 1998). Siponen (2000) väittää, että tietoturvatietoisuutta lisäämällä vähennettäisiin käyttäjälähtöisiä virheitä.

Tietojärjestelmän väärinkäyttö, tietojärjestelmän hyväksikäyttö tai tietokonerikos tietojenkäsittelyn yhteydessä voidaan määritellä Foltz'in, Cronan'in ja Jones'in (2005) mukaan luvattomaksi, harkituksi ja havaituksi tietojärjestelmän väärinkäytöksi, joka sisältää laitteet, ohjelmistot, datan ja palvelut. Tietokoneen väärinkäyttö voidaan määritellä myös loukkaukseksi, tai välittömäksi loukkauksen uhaksi tietoturvapoliittikkaa, hyväksytyjä käyttösääntöjä, turvallisuuskäytäntöjä kohtaan. Väärinkäytöksi katsotaan palvelunestoa, haittakoodin tekemistä tai levittämistä ja luvattonta tai asiatonta tietokoneen käyttöä. Tietojärjestelmän väärinkäytöstapauksissa on suurelta osin kyse laillisten käyttäjien tunnusten ja salasanojen väärinkäytöstä tai laillisten käyttäjien tahattomista teoista (Wiant, 2005).

Petos ja vilppi ovat yhä kasvavia ongelmia tietojenkäsittelyssä. Termit voidaan määritellä tietojenkäsittelyn ja ohjelmistojen luvattomaksi syötteen tai syötteen muuttamiseksi, luvattomaksi tietojenkäsittelyn tai ohjelmistojen tulosten estämiseksi, hävittämiseksi tai kavaltamiseksi (Mills, 1995).

Tietoturvan hallintajärjestelmän voidaan sanoa olevan tietoturvallisuuden johtamis- ja hallintajärjestelmän, joka on luonteeltaan viitekehys ja on riippuvainen organisaatiokohtaisesti tietoturvariskien merkityksestä ja tietoturva-asioiden kehitysvaiheesta organisaatiossa (VAHTI 6/2006, s.17). Se voidaan myös määritellä tietoturvallisuuskulttuuriksi joka on osa organisaation turvallisuuskulttuuria (Schlienger, 2003). Tietoturvan hallintajärjestelmä on järjestelmä, jossa etupäässä hallinnollisilla toimilla varmistetaan, että oikeat tekniset ratkaisut valitaan, otetaan käyttöön ja käytetään oikein (Pfleeger, 2007). Tietoturvallisuuden hallinta ja varsinkin sen aloittaminen on monimutkaista ja resursseja vaativaa toimintaa. Toiminnan organisoimisen apuna on hyvä käyttää jotain yleisesti hyväksyttyä standardia, vaikka ei hakisikaan toiminnalleen sertifiointia. Standardeista saa hyviä tarkastuslistoja toiminnan jäsentämiseksi. Yksi tällainen yleisesti käytetty standardi on British Standard 7799, josta käytetään myös nimeä Code of Practice for Information Security. BS 7799³ on Iso-Britannian Standardointiinstituutin julkaisema suositus organisaation tietoturvallisuuden hallintajärjestelmäksi (Solms, 1998).

Kohdennetulla koulutuksella tarkoitetaan tässä tutkimuksessa sitä, että koulutuksen sisällön suunnittelussa otetaan huomioon käyttäjien asema organisaatiossa, sekä organi-

³ Nykyään ISO 27001

saation erityispiirteet kun suunnitellaan koulutuksen sisältöä. Tutkimusta, jossa olisi tutkittu yksinomaan kohderyhmälle räätälöityä tietoturvakoulutusta, ei löytynyt. Tietoturvakoulutusta käsittelevissä tieteellisissä artikkeleissa kohderyhmän ominaispiirteiden huomioon ottamista koulutuksen sisältöä suunnitellessa kuitenkin painotetaan.

Seuraavassa alaluvussa tarkastellaan laajemmin ja tarkemmin tietoturvaa koskevaa tutkimusta. Ensiksi käsitellään muutamia artikkeleita tietoturvasta ja tietoturvatietoisuudesta yleensä. Seuraavaksi käsitellään tutkimusta, jonka aiheena on ollut tietoturvan hallinta. Viimeisenä esitellään tietoturvakoulutukseen liittyvää tutkimusta. Vaikka varsinaista viranomaisorganisaatiota koulutuksen kohdeorganisaationa käsittelevää tutkimusta ei erilaisista elektronisista tietokannoista hakusanoilla löytynyt kuin yksi lähde, niin sen sijaan tietoturvasta, tietoturvatietoisuudesta ja tietoturvakoulutuksesta, sekä valistuksesta löytyi paljon artikkeleita. Samoin nykyään julkaistaan paljon tutkimuksia ja pidetään useita konferensseja, jotka käsittelevät tietoturvan asemaa informaatiojärjestelmissä (Siponen ja Oinas-Kukkonen, 2007).

3.2 Tietoturva ja tietoturvatietoisuus

Huolimatta siitä, että organisaatiot kehittävät ja toteuttavat lukuisia suojaustoimenpiteitä on tietojärjestelmän väärinkäyttö jatkuvasti kasvava ongelma (Lee ja Lee, 2002.) Kun vuosina 1997–1999 enimmillään 50 % organisaatioista oli joutunut tietoturvaloukkauksien kohteeksi, niin kaksi vuotta myöhemmin luku oli noussut huomattavasti. Vuosina 2001–2003 luku oli enimmillään jo 90 % (Pahnila et al., 2007). Suurin riskitekijä tietoturvalle on ihminen, joko organisaation ulkopuolelta tai sisältä. Vaikeimmin torjuttava väärinkäyttötapa tulee nimenomaan organisaation sisältä. Vaikka lähes kaikki organisaatiot ovat huolissaan ulkoisesta uhasta, niin eri tutkimukset osoittavat että 50 – 70 % väärinkäytöksistä on organisaatioiden sisäisiä (Stanton et al., 2004, vrt. D’Arcy ja Hovav, 2007). Lee ja Lee (2002) esittelevät artikkelissaan Computer Security Institutin tutkimuksen vuodelta 2001, jossa tutkimukseen osallistuneet yritykset olivat kärsineet yhteensä 378 miljoonan dollarin menetykset tietokoneen väärinkäytön seurauksena. Väärinkäytöksistä 60 % oli nimenomaan väärinkäytöksen kohteeksi joutuneessa organisaatiossa työskentelevien tekemiä. Rikkomukset saattavat olla tahallisia tai tahattomia. Ne johtuvat vääränlaisesta turvallisuuskulttuurista, puutteellisesta ohjauksesta tai vääristä teknisistä ratkaisuista. Väärinkäytökset voivat johtua myös välinpitämättömyydestä tai laiskuudesta (Aytes ja Conolly, 2003).

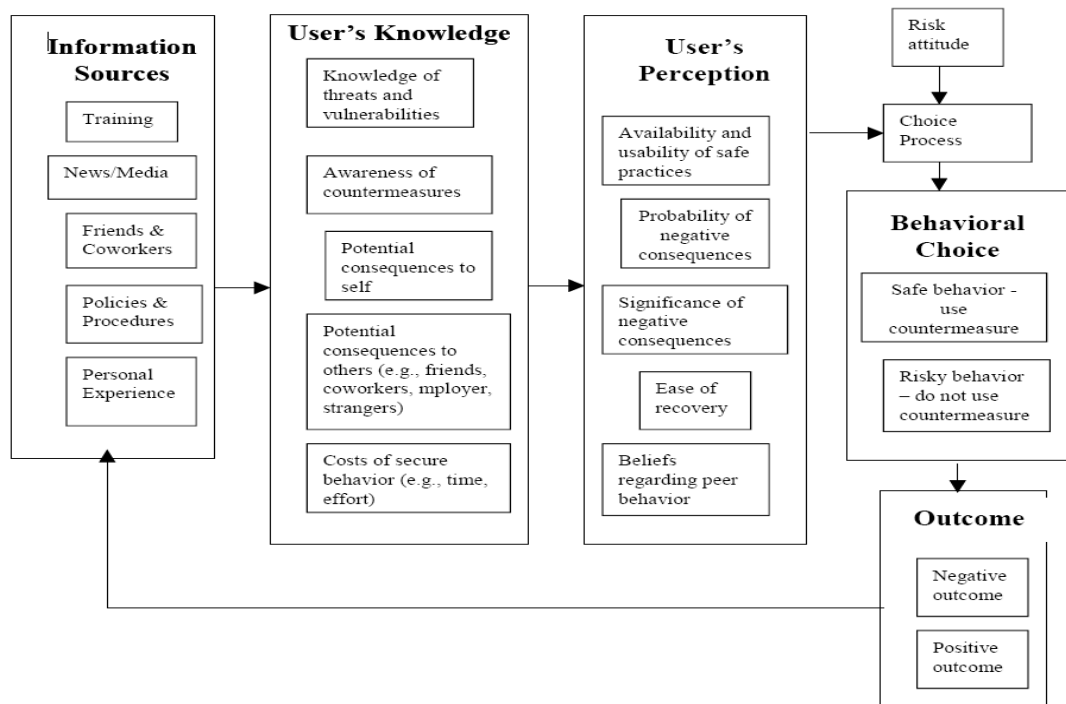
Tietoturvan toteutumisessa ohjeiden noudattaminen on tekniikan lisäksi yksi avainkysymyksistä. Kuten myöhemmin luvussa 3.1.3 esiteltävässä McCombsin ja Vakilin (2006) tutkimuksesta käy ilmi, motivaatiolla ja uskomuksilla on keskeinen osa tietoturvan toteutumisessa. Samoin motivaatiolla ja uskomuksilla on keskeinen osa kun selitetään käyttäjän tietoturvaohjeiden noudattamista. Normatiiviset uskomukset siitä mitä työkaverit ajattelevat tietoturvasta, tai mitä esimiehet vaativat työntekijältä tietoturvan noudattamisessa vaikuttavat määräysten noudattamiseen (Pahnila et al., 2007). Organisaation johdolle on usein tärkeämpää että työntekijät noudattavat ohjeita, kuin se ovatko he tietoturvatietoisia. On eri asia olla tietoinen tietoturvasta kuin noudattaa tietoturvaohjeita. Ohjeita noudatetaan jos ne nähdään normina toiminnalle. Liian harvoin organisaatiot kuitenkin suojelevat itselleen tärkeää tietoa normatiivisin vaatimuksin (Layton, 2005).

Pahnila et al. (2007) esittelevät teoreettisen mallin, joka perustuu useisiin käyttäytymistieteissä käytettyihin malleihin. Mallin pääfaktorit, kuten asenne sääntöjen noudattamista kohtaan, aikomus noudattaa sääntöjä ja niiden noudattaminen, perustuvat perustellun toiminnan teoriaan (*Theory of Reasoned Action*, TRA). Asenteet ilmaisevat henkilön positiivisia tai negatiivisia tuntemuksia erilaisiin ärsykkeisiin. TRA-teorian mukaan mitä suurempi aikomus henkilöllä on toteuttaa teko, sen todennäköisemmin se toteutetaan. Tämä pätee myös tietoturvasäännösten noudattamiseen. Malli kuvaa työntekijän tietoturvasäännösten noudattamista. Empiiristen tulosten mukaan tietoturvan informaation laadulla on huomattava merkitys ohjeiden noudattamisessa. Asenteilla, normatiivisilla uskomuksilla ja tavoilla on myös huomattava merkitys, kuten myös uhan tuntemuksella. Tässä tutkimuksessa esitellyiden tulosten perusteella rangaistuksilla on merkitystä, vain jos ne tehdään näkyviksi ja sellaisiksi, että ne seuraavat välittömästi rikettä. Yllättävää kyllä, palkitsemisella ei havaittu olevan merkittävää vaikutusta toimintaan (Pahnila et al., 2007).

Sen sijaan Puhakaisen (2006) tutkimuksen mukaan palkitseminen, kuten rankaiseminenkin, näyttää vaikuttavan tietoturvaohjeiden noudattamiseen. Myös tämän tutkimuksen toisen koulutuksen jälkeen suoritetun kyselyn vastauksista käy ilmi, että vastaajat pohtivat mahdollisia tietojärjestelmän väärinkäytön seurauksia rangaistuksen mahdollisuus mielessään. Puhakaisen tutkimuksessa esitellään vielä kaksi muuta pääelementtiä tietoturvatietoisuuden lisäämiseen: 1) tietoturvatietoisuuskoulutus ja 2) tietoturvan markkinointi (Puhakainen 2006).

Hilmer, Richardson ja Courtney (2003) ovat myös tutkimuksessaan käsitelleet rangaistuksen ja palkitsemisen problematiikkaa. Heidän mielestään epäeettinen toiminta saattaa vaikuttaa moniin ihmisiin sekä organisaation sisä- että ulkopuolella. Epäeettisten päätösten seurauksena saattaa koko organisaation olemassaolo olla uhattuna. Tästä syystä (varsinkin jos epäeettisen toiminnan seuraukset ovat isoja ja kauaskantoisia) organisaatiossa täytyy tehdä selväksi, että eettinen toiminta on osa organisaatiokulttuuria (Hilmer, et al., 2003).

Aytes ja Conolly (2003) esittävät mallin, jossa he kuvaavat käyttäjän toimintaa. Malli korostaa tekijöitä jotka riippuvat siitä, miten käyttäjät havaitsevat riskit ja mitä toimenpiteitä siitä seuraa. Aytes ja Conolly (2003) korostavat, että kun aiemmissa tutkimuksissa keskityttiin siihen, miten tekniikan avulla vähennetään tietoturvariskejä, niin nykyään on selvää, että tekniikka ei yksin riitä. Tähän he esittävät kaksi syytä: riskit muuttuvat ihmisen toiminnan seurauksena ja toimenpiteet, joiden tarkoitus on suojata riskeiltä, riippuvat siitä miten ajantasaisina ihmiset niitä pitävät. Toisin sanoen tietoturva on riippuvainen ihmisen toimista. Iteratiivinen malli, jonka Aytes ja Conolly (2003) esittelevät, koostuu kuudesta komponentista. Nämä pääkomponentit ovat: 1) informaation lähde, 2) käyttäjän tiedot, 3) käyttäjän havaintokyky, 4) valintaprosessi, 5) todellinen käyttäytyminen ja lopuksi 6) prosessin tulokset, jotka muodostavat uuden informaation mallin käyttöön (kuva 3).



Kuva 3. Malli, joka kuvaa käyttäjän toimintaan vaikuttavia tekijöitä (Aytes ja Conolly, 2003).

Tehokas tietoturvatietoisuus edellyttävät organisaatiolta jatkuvaa ponnistelua. Tietoturvatietoisuuden lisäksi tietoturvan hallintaan oleellisesti kuuluvat suojaustoimet käsittävät sekä menettelytapaohjeita, että teknisiä kontroleita. Teknisten ratkaisuiden tulisi suojata järjestelmää väärinkäytöksiltä. Niiden teho riippuu kuitenkin käyttäjien tietoisuudesta (D'Arcy ja Hovav, 2007). Inhimillisen tekijän huomioon ottaminen tietoturvaratkaisuissa ei ole edennyt samaa tahtia teknisten ratkaisujen kanssa. Käyttäjäkontrollilla, joka käsittää hallinnollisia ja ohjeellisia ratkaisuja, pyritään varmistamaan että käyttäjät ovat riittävän tietoisia tekemään turvallista työtä. Epäsuhta teknisten ratkaisujen ja hallinnollisten ratkaisujen välillä näkyi vuonna 2003 siten, että 83 % liiketoiminnasta vastaavista ilmoitti tekniikan olevan tärkein kustannuserä tietoturvallisuuden menoista ja vain 35 %:lla oli säännöllisiä tietoturvatietoisuus- tai tietoturvakoulutusohjelmia (Wiant, 2005).

Usein puhuttaessa tietoturvatietoisuudesta tarkoitetaan aikomusta tai halua ohjeiden noudattamiseen. Lee ja Lee (2002) väittävät, että tietoturvapoliitikat, tietoturvaohjeet ja tietoturvatietoisuuden parantamiseen tähtäävät ohjelmat eivät odotuksista huolimatta lisää tietoturvaohjeiden noudattamista. Tieteellisissä tutkimuksissa on yritetty löytää keinoja vähentää tietoturvarikkomuksia esittelemällä parempia tietoturvapoliitikoita ja turvallisempia tietojärjestelmiä. Näyttää kuitenkin siltä, että suoritettut toimenpiteet ovat olleet riittämättömiä. Halu tai aikomus ohjeiden noudattamiseen ei pelkästään riitä, vaan tarvitaan lisätoimia aikomuksen muuttamiseksi toiminnaksi. Käyttäjät tekevät rationaalisia päätöksiä maksimoidakseen toiminnan hyödyt ja minimoidakseen mahdolliset kustannukset. Tätä lähtökohtaa käytetään yleisesti kriminologisessa tutkimuksessa. Yleinen rangaistusteoria (*General Deterrence Theory, GDT*) on jonkin verran käytetty teoria tietoturvaohjeiden noudattamista tutkittaessa (esim. Lee ja Lee, 2002; Siponen et al., 2007). Se on antanut järkevä pohjan yritettäessä ymmärtää tietoturvarikkomuksia. GDT:ssä lähdetään siitä oletuksesta, että havainto rangaistuksen suuruudesta suhteessa saavutettuun hyötyyn ehkäisee väärinkäyttötapaauksia. Tämä ei ole kuitenkaan

johtanut toivottuun tulokseen, koska organisaatiot vievät harvoin sanktioita käytännön tasolle (Lee ja Lee, 2002). Lee ja Lee (2002) esittelevät kokonaisvaltaisen mallin, jolla selitetään tietokoneella tapahtuvaa väärinkäyttöä organisaatiossa. Edellä esitellyn GDT:n lisäksi he laajentavat suunnitellun toiminnan teoriaa (*The Theory of Planned Behaviour, TPB*) lisäämällä siihen teorian sosiaalisesta siteestä (*Social Bond Theory, SBT*) ja sosiaalisesta oppimisesta (*Social Learning Theory, SLT*).

Lee ja Leen (2002) esittelemässä mallissa on kolme elementtiä, jotka vaikuttavat asenteiden kautta. Sosiaalisessa siteessä on neljä muuttujaa; 1) *kiintyminen* tai leimautuminen johonkin vertaisryhmään, 2) *sitoutuminen* yhteisiin arvoihin tai sääntöihin, 3) *osallistuminen*, jolla havainnoidaan yksilön toiminnan suuntautumista (mitä enemmän yksilön toiminta suuntautuu tavanomaisiin aktiviteetteihin, sitä todennäköisemmin hän ei tule osallistumaan epätoivottavaan toimintaan) ja 4) *uskomukset* väärinkäytösten seuraamuksista.

Sosiaalisen oppimisen teorian mukaan yksilö toimii epärehellisesti epärehellisten seurassa. Rikoksenteelijät siirtävät kanssaihmisilleen arvojaan ja roolimallejaan ja siten lisäävät rikollisuutta. Suoritettujen tutkimusten mukaan sosiaalinen side vaikuttaa negatiivisesti aikomukseen ryhtyä tietokoneen väärinkäyttöön. Sen sijaan sosiaalisen oppimisen kautta käyttäjät saattavat oppia epätoivottua tietokoneen käyttöä, jos he ovat kanssakäymisissä sellaisten henkilöiden kanssa, jotka pitävät tietokoneen väärinkäyttöä hyväksyttävänä. Lopuksi kokonaisvaltaisen tietokoneen väärinkäyttöä käsittelevän mallin mukaan yleinen rangaistusteoria (GDT) vaikuttaa alentavasti aikomukseen ryhtyä tietokoneen väärinkäyttöön, varsinkin jos organisaatiossa on toimeenpantu rangaistuksia ja niistä on raportoitu työntekijöille (Lee ja Lee, 2002).

Vaikka sanktioiden ja toisaalta palkitsemisen vaikutuksia tietoturvaohjeiden noudattamiseen on jonkin verran tutkittu, niin motivaation ja etiikan vaikutuksen tutkimusta tarvitaan lisää. Varsinkin empiiristä tutkimusta tarvittaisiin selvittämään mitä keinoja tarvitaan varmistamaan, että käyttäjät sitoutuvat tietoturvaohjeiden noudattamiseen (Siponen ja Oinas-Kukkonen, 2007). Monilla organisaatioilla on olemassa eettiset säännöt tai jokin muu julkilausuma, johon organisaation arvot perustuvat. Niitä pidetään tärkeinä, jopa välttämättöminä ohjenuorina koko organisaation toiminnan kannalta. Todellisuus on kuitenkin osoittanut, että tämä toive ei usein toteudu käytännössä. Käytäntö on osoittanut, että usein yhteys organisaation tavoitteiden ja todellisen käyttäytymisen välillä on katkennut eri syistä. On osoitettu, että työntekijän päätös sääntöjen noudattamiseen perustuu usein eettiseen päätöksentekoon. Tähän päätöksentekoprosessiin saattaa vaikuttaa esimiesten taholta tulevat odotukset, työtyytyväisyys, ja sitoutuminen työnantajaan. Henkilökohtaiset arvot, pelko rangaistuksista, ja lojaalisuus lisäävät sitoutumista sääntöjen noudattamiseen. Sen sijaan itsekeskeisyys, tyytymättömyys, ja ympäristön vaikutus, kuten työkaverien painostus ja ohjailu tai tilaisuuden luoma mahdollisuus saattavat johtaa sääntöjen rikkomiseen (Embse, Desai ja Desai, 2004.)

Roper, Grau ja Fisher (2005) väittävät, että negatiivisella motivoinnilla eli rangaistuksen korostamisella on vähemmän tehoa kuin positiivisella motivoinnilla. Käyttämällä negatiivista motivointia ei voida olla varmoja tuloksista, sillä ihmiset mieluummin huijaavat välttääkseen rangaistuksen, kuin saavuttaakseen palkkion. Negatiivisen ja positiivisen motivoinnin yhdistämiselläkin on saavutettavissa parempia tuloksia, kuin pelkällä negatiivisella motivoinnilla. Ihmiset harkitsevat tekojensa seurauksia. Lisäksi he arvioivat ja kokevat seuraukset eri tavoin. Siksi mitä paremmin tunnetaan kohderyhmä, sitä paremmin pystytään valitsemaan, kumpaa motivointia käytetään. Käytetäänpä sit-

ten negatiivista, tai positiivista motivointia, ne on tehtävä näkyviksi. Jos jotain luvataan tai uhataan, se on toteutettava. Positiivinen motivointi on sikäli ongelmattomampaa, sillä julkinen kiitos tai palkitseminen ei aiheuta juridisia ongelmia kuten julkinen rankaiseminen. Lisäksi sanktiot saattavat aiheuttaa sen, että tahattomat väärinkäytökset salataan. Tietoturvan noudattamisesta kannattaa tehdä palkitsevaa ja riittävän helppoa (Roper et al., 2005).

3.3 Tietoturvan hallinta

Tietoturvan hallintajärjestelmä on järjestelmä, jonka avulla organisaation johto saa tietoa tietoturvan tasosta ja jonka avulla ohjataan toimintaa haluttuun suuntaan. Tietoturvan hyväksyttävä taso edellyttää oikein asetettuja ohjaustoimia sekä hallinnollisia, että teknisiä ratkaisuja hyväksikäyttäen. Tietoturvan kannalta oleellisten keinojen havaitsemis- ja määrittelyprosessi on monimutkainen ja paljon resursseja vaativaa. Tietoturvan hallintaprosessin apuna kannattaa käyttää yleisesti hyväksytyjä tietoturvastandardeja, vaikka ei tavoiteltaisikaan sertifikaattia. Hallintajärjestelmän tarkoituksena tulee olla tietoturvan jatkuva parantaminen, sillä BS 7799 standardin periaatteiden mukaisesti jokaisella organisaatiolla tieto on arvokasta ja sitä tulee suojella (Hong, Chao ja Tang, 2003.) Organisaatiossa on tietoturvan hallinnan kannalta neljä kriittistä osa-alueita, joiden kuntoon laitolla saavutetaan organisaation turvallisuuden minimitaso. Ensimmäiseksi tietoturvan kohteen ja aktiviteetin täytyy perustua organisaation johdon määrittelemälle toiminta- ajatukselle ja toiseksi sillä täytyy olla johdon näkyvä tuki. Kolmanneksi organisaatiolla täytyy olla selkeä käsitys sitä mahdollisesti kohtaavista riskeistä ja niitä vastaava turvallisuustaso. Neljänneksi tietoturvan täytyy olla hyvin markkinoitua kaikille työntekijöille ja yhteistyökumppaneille. Tämä tapahtuu viemällä tietoturvapoliitiikan sisältö ja tietoturvaohjeistus käytäntöön organisaation joka tasolla koskien myös yhteistyökumppaneita (Solms, 1999.)

Tietoturvaohjelmaa aloitettaessa on tärkeää tutkia mitä organisaatiossa on jo ehkä tehty tietoturvatietoisuuden eteen. On tutkittava, mitkä ovat organisaation vahvuudet ja mitkä ovat sen heikkoudet tietoturvan suhteen. On myös syytä tutustua organisaation henkilökuntaan; ketkä suhtautuvat myönteisesti ja ketkä kielteisesti tietoturvaan, minkälainen asenneilmasto henkilökunnan keskuudessa on ja minkälainen tietoturvatietoisuus organisaatiossa sillä hetkellä vallitsee. Tietoturvaohjelmissa kannattaa käyttää jo olemassa olevia kanavia. Jos esimerkiksi organisaatiossa on olemassa toimiva koulutusjärjestelmä, sitä kannattaa hyödyntää. Tärkein perusta tietoturvan kehitystyölle löytyy kuitenkin organisaation politiikoista, ohjeista ja standardeista. Ne täytyy ensimmäisenä saattaa ajan tasalle, ennen kuin muita tietoturvatietoisuutta parantamaan tähtääviä ohjelmia kannattaa aloittaa (Desman, 2006).

Turvallisuuskulttuurin muodostumiseen vaikuttavat organisaation sisäiset ja ulkoiset muuttajat. Organisaation tavoitteet ja toiminnalliset päämäärät muokkaavat sääntöjä, käyttäytymisnormeja ja ajattelua organisaation sisällä (Choudhry, Fang ja Mohamed, 2006.) Tästä on väistämättä seurauksena se, että erilaisessa toimintaympäristössä toimivilla organisaatioilla on erilainen organisaatiokulttuuri. Koska tietoturvallisuus on osa organisaatiokulttuuria, niin eri organisaatioilla on myös erilainen tietoturvakulttuuri (Schlienger ja Teufel, 2003.)

Tietoturvan saavuttamiseen on löydettävissä neljä tarkoituksenmukaista välinettä; 1) tietojärjestelmien pääsynvalvonnan hallinta, 2) turvallinen tiedonvälitys, 3) tietoturvan

hallinta ja 4) tietoturvan kehittäminen. Edellä mainittujen seikkojen hallinta voidaan jakaa organisationaaliseen-, sanalliseen eli käsitteelliseen ja tekniseen tasoon. Avainkysymys on se, kuinka tietojärjestelmiä tulisi hallinnoida ja kehittää tietoturvallisuuskannat huomioon ottaen. Tällöin tulee ottaa huomioon kolme tietoturvan yleistä päävaatimusta. Ensimmäiseksi informaatio tulee suojella niin, että oikeudettomilla ei ole mahdollisuutta sen muokkaamiseen (eheys). Toiseksi, informaation tulee olla saatavilla niille, joilla siihen on oikeus (saatavuus). Kolmas tiedon turvaamisen taso, luotettavuus, varmistetaan suojaus - ja estotoimenpiteillä (Siponen ja Oinas-Kukkonen, 2007).

Verkkoliiketoiminta ja asioiminen viranomaisten kanssa verkossa ovat lisänneet vaatimusta todentaa verkkoasioinnin osapuolten tekemät toimet. Kiistämättömyys on siis neljäs tietoturvan ulottuvuus, jota tietoturvan hallinta koskee. Tietojärjestelmien kehittämisessä tietoturvalliseen suuntaan on kysymys siitä, löydetäänkö oikeat vaatimukset tietoturvalliselle järjestelmälle. Erilaiset tarkastuslistat ja tutkimukset antavat suuntaa tietoturvan kehitystyölle, vaikka eivät annakaan eväitä tietoturvavaatimusten mallintamiseen tai havaitsemiseen. Pikemminkin ne määrittelevät tietoturvahallinnan periaatteita (Siponen ja Oinas-Kukkonen, 2007).

Viimevuosiin asti tietoturvakriittisten tekijöiden systematisointiin ja mittaamiseen ei ole ollut välineitä. Tämä tekee tietoturvan hallinnasta vaikeaa ja siksi helposti turvaudutaan yksinomaan teknisiin ratkaisuihin. Tekniikka ei kuitenkaan yksin auta estämään väärinkäytöksiä, sillä vain kymmenestä kahteenkymmeneen prosenttia tietoturvaongelmista ovat teknisiä, loput kahdeksankymmentä prosenttia johtuu inhimillisistä tekijöistä. Inhimillisten tekijöiden minimoimiseksi organisaation tulee luoda sellainen turvallisuuskulttuuri, jossa yksittäisen käyttäjä ymmärtää organisaation tavoitteet ja voi sitoutua niihin (Torres et al., 2006, vrt. Schlienger, 2003.) Torres et al. (2006) esittelevät mittarit, jolla selvennetään tietoturvan hallintaprosessin sisällä olevia muuttujia, kuten projektien suorittamisessa, tietoturvatoimien toteutustasossa tai riskienhallintaprosessissa tapahtuvia toimia. Lopuksi esitellään tietoturvatoimien tehon mittaamiseen soveltuva malli.

Inhimillisistä tekijöistä on kysymys myös silloin, kun organisaation auktorisoitu käyttäjä toimii tietoturvaohjeiden vastaisesti, usein tietämättään. D’Arcy ja Havav (2007) esittelevät tutkimuksessaan tällaista tietoturvan kannalta ongelmallista tilannetta: tietojärjestelmän sisäistä väärinkäyttöä. Vuoden 2002 väärinkäytöksistä 70 % oli organisaatioissa työskentelevien tietojärjestelmän käyttöluvan omaavien työntekijöiden aiheuttamia. Usein kyseessä oli tyytymätön työntekijä. D’Arcy ja Havav (2007) vertaavat neljän tekijän vaikutusta tietoturvatietoisuuteen. Vertailtavat tekijät olivat: tietoturvapolitiikka, tietoturvakoulutus, päätemonitorointi⁴, sekä tekniset ratkaisut. Tietoturvakoulutuksella oli eniten vaikutusta tietoturvatietoisuuteen. Tietoturvapolitiikalla ja teknisillä toimilla oli myös merkittävä vaikutus. Yllättävää kyllä, monitoroinnilla oli vähiten vaikutusta. D’Arcy ja Havav (2007) tulivat siihen johtopäätökseen, että käyttäjät ovat niin valistuneita, etteivät pelkät tekniset ratkaisut riitä. He edellyttävät näyttöä siitä, että organisaatiossa ollaan tosissaan tietoturvan suhteen. Artikkelin kirjoittajien mielestä tehokas tietoturvan hallinta edellyttää kombinaatiota kaikista edellä esitellyistä tietoturvaan vaikuttavista tekijöistä.

⁴ Päätemonitoroinnilla tarkoitetaan tässä tarkkailua, jolla käyttäjän toimet tallentuvat muistiin. Monitorointi käsittää sähköpostin, internetin ja sovellusten käytön, sisältäen tietoturvatarkastukset.

D'Arcy ja Havav (2007) esittävät väitteen, että liiallinen huomion kiinnittäminen tekniikkaan saattaa selittää sen, että tietojärjestelmien väärinkäyttö on edelleen huomattava ongelma. Monet organisaatiot suhtautuvat tietoturvaan kuitenkin nimenomaan teknisenä kysymyksenä. Kuitenkin jos organisaatiot ottaisivat tietoturvan enemmän asennekuin teknisenä kysymyksenä, ne säästäisivät kustannuksia (Layton, 2005). Tämän ongelman ratkaisemiseksi tutkijat ovat esitelleet tehokkaampia keinoja vähentää tietojärjestelmään kohdistuvia rikkomuksia. Tehokkaammat tietoturvapoliitikat, huolellisemmin toteutetut tietoturvaohjelmat ja turvallisemmat tietojärjestelmät tähtäävät tähän. Molempia, sekä teknisiä että hallinnollisia ratkaisuja tarvitaan vähentämään tietoturvarikkomuksia (Lee ja Lee, 2002). Erilaisten ratkaisujen pelkkä olemassaolo ei takaa turvallista tietojärjestelmää. Käyttäjien tulee ottaa ne käyttöön ja noudattaa niitä (D'Arcy ja Havav, 2007).

Tehokas tietoturvan hallinta edellyttää tekniikan lisäksi suunnittelua, harjoittelua, koulutusta ja johtamista (McIlwraith, 2006). Koulutus (*education*) ja harjoittelu (*training*) poikkeavat toisistaan siten, että kun koulutus vastaa kysymykseen ”miksi”, niin harjoittelu vastaa kysymykseen ”miten” (Layton, 2005). Usein tietoturvakoulutuksesta puhuttaessa näitä kahta termiä ei erotella. Varsinkin suomalaisessa tietoturvatermologiassa tietoturvakoulutus sisältää molemmat merkitykset.

Huomattava yhteys ehkäisevien tietoturvasovellusten ja tietoturvaohjeiden noudattamisen aikomuksen välillä on empiirisesti todettu olevan seurausta siitä, että tekniikka toimii myös pelotteena. Tämä edellyttää kuitenkin sitä, että henkilökunta on tietoinen tekniikasta ja on perillä sen toiminnasta ja merkityksestä tietoturvan suhteen. Usein käyttäjät eivät kykene yhdistämään teknisten ratkaisujen, kuten monitoroinnin ja kiinni jäämisen riskin yhteyttä. Siksi organisaatioiden tulee parantaa käyttäjien tietoisuutta tietoturvan parantamiseen käytettyjen tekniikoiden ja tietoturvapoliitikoiden merkityksestä (D'Arcy ja Havav, 2007).

Belsis, Kokolakis ja Kiountouzis (2005) laajentavat tietoturvan hallintaa tiedon hallinnan (*knowledge management*) suuntaan. Kyse on inhimillisestä tekijästä tietoturvan hallinnassa, jonka minimoimiseksi organisaation tulee luoda sellainen turvallisuuskulttuuri, jossa yksittäinen käyttäjä ymmärtää organisaation tavoitteet ja voi sitoutua niihin (vrt. Torres et al., 2006). Belsis et al. väittävät, että lähes kaikkia tietoturvan hallinnassa käytettyjä keinoja voidaan tarkastella kriittisesti. Niiden teho voidaan kyseenalaistaa jatkuvasti kasvavien väärinkäytösten ja niistä aiheutuvien kasvavien kustannusten valossa. Tietoturvatyökalut ja -mekanismit eivät ole riittäviä suojaamaan tietojärjestelmiä niiden inhimillisen ja organisatorisen luonteen vuoksi. Tietoturvan hallinta sisältää monia aktiivitenttejä, joiden tarkoituksena on minimoida organisaation toimintaan kohdistuvia tietoriskejä. Tällaisen toiminnan ylläpitäminen edellyttää erikoistunutta tietoturvaalueen osaamista. Toisena tärkeänä tekijänä tietoturvan hallinnassa kirjoittajat näkevät säännöistä, tavoitteista ja ohjeista käytävän viestinnän. Yleensä tietoturvapoliitikoita on käytetty tähän tehtävään. Tietoturvapoliitikat edustavat kuitenkin luontihetkensä teknistä ja tiedollista tasoa. Niinpä tietoturvan hallinnassa tarpeellinen palaute jääkin usein pelkästään teknisten lokitietojen varaan. Belsis et al. väittävät, että menestyksekkäs tietoturvan hallinta riippuu kaikkien osapuolten, työntekijöiden ja johtohenkilöiden, osallistumisesta tietoturvan analysointiin, suunnitteluun ja käyttöönottoon. Belsis et al. (2005) väittävät myös, että useimmilla johtoon kuuluvilta puuttuu vaadittava tietomäärä tietoturvan tehokkaaseen hallintaan. Vaikka artikkelissa myönnetään tiedon puutteen vaikutukset tietoturvaan, ei koulutus kuitenkaan ole väline tiedon hallintaan, vaan tieto nähdään enemmänkin piilossa olevana voimavarana, jonka esiintuomiseen teknisillä ja

organisatorisilla tekijöillä on vaikutusta. Sitä, miten tuo tieto organisaatioon saadaan, ei artikkelissa mainita (Belsis et al., 2005).

Torres et al. (2006) väittävät, että tietoturvan hallinnassa on kyse tekniikasta, prosessista ja ihmisistä (vrt. Siponen ja Oinas-Kokkonen, 2007). Artikkelissa tuodaan esille myös väite, että tietoturvasta puuttuu yleisesti hyväksytty kehys (*Framework*), teoria ja päämäärä, sekä keinot jolla mitataan tehtyjen toimien tehoa. He esittelevät artikkelissaan keinot (*Controls*) joilla tietoturvaa hallitaan. Niitä ovat: tekniset -, viralliset - ja epäviralliset kontrollit. Tietoturvan hallintaprosessissa on tärkeää, että se perustuu myös johonkin tieteellisesti hyväksytyyn periaatteeseen ja että siinä otetaan organisaation tarpeet huomioon. Usein organisaatioiden tarpeet unohtuvat kun seurataan ”tietoturva-guruja” heidän oppeihinsa sokeasti luottaen (Siponen ja Baskerville, 2001.) Tietoturvakoulutuksella, joka sitoo käyttäjät osaksi tietoturvaa, on keskeinen osa tietoturvan hallintaprosessissa. Ilman tietoturvakoulutusta tietoturvan hallinta ei onnistu. (Schlienger ja Teufel, 2003.)

3.4 Tietoturvakoulutus

Useissa tietoturvakoulutusta käsitelleissä tutkimuksissa lähestymistapa oli koulutettavat ja heidän erityispiirteet huomioon ottavaa (vrt. Torres et al., 2006 ja Schultz, McCoy ja Fowler, 2004). Chaston (1994) kuitenkin varoittaa korostamasta liikaa koulutettavien erityispiirteitä. Hänen mielestään perinteinen suora lähestymistapa työntekijöiden tietoihin, taitoihin ja asenteisiin koulutuksen suhteen jättää organisaation tarpeet taka-alalle. Myös Schultz (2004) kritisoi perinteistä tietoturvakoulutusta samasta syystä. Hänenkään mielestä siinä ei välttämättä paneuduta koulutettavalle organisaatiolle ominaisiin ongelma-kohtiin. On turha uhrata voimavaroja niihin tietoturvan osa-alueisiin, jotka organisaatiossa ovat jo kunnossa. Sen sijaan on tehokkaampaa painottaa niitä seikkoja, joiden on havaittu olevan lisäpanostuksen tarpeessa, tai ovat organisaation kannalta muutoin kriittisiä. Koulutustapahtumien sisältöä suunniteltaessa on syytä välttää yleistämistä ja ”jokaiselle jotain” - ajattelua, joka on usein tietoturvakoulutuksen ongelmana (Schultz et al., 2004).

McCombs ja Vakili (2006) esittelevät tutkimuksessaan tutkimusmenetelmän, joka perustuu oppijakeskeisyyteen. Opetustavan, jossa koulutettava on keskeisessä osassa he määrittelevät perspektiiviksi opettamiseen, joka yhdistää yksilön ominaisuudet parhaisiin opetusmenetelmiin. Learner-Centered Psychological Principles- niminen malli sisältää neljätoista periaatetta (*Principles*). Ne ovat kehyksessä, joka puolestaan koostuu neljästä määrittelyjoukosta (*Domain*). Määrittelyjoukkoja ovat: 1) metatiedollinen ja tiedollinen, 2) tunnetilan huomioonottava, 3) motivaatioon perustuva, sekä 4) kehittyvä ja sosiaalinen. Teorian avainkohtina mainitaan kyky kohdata koulutettavien tarpeet. Tähän päästään löytämällä strategiat koulutettavien tarpeiden hahmottamiseen. On hahmotettava myös koulutettavien kykyjen ja mielenkiinnon eroavaisuudet. Lisäksi on räätälöitävä koulutusstrategiat koulutettavien erilaisia henkilökohtaisia kontrollitarpeita ja valintoja ajatellen. Oppijakeskeinen opetusmalli on hyvä tuntee, sillä samojen lainalaisuuksien kanssa ollaan tekemisissä myös tietoturvaopetuksessa. Useita edellä esiteltyiden periaatteiden mukaisia aiheita käsitellään myös tietoturvaopetusta esittelevissä tieteellisissä tutkimuksissa (Liite A).

Kuten Solms (1999) esitti, tietoturvan hallintaan kuuluu tietoturvan markkinointi (vrt. Puhakainen, 2006). Tähän liittyen McCoy ja Fowler (2004) esittelevät tuotemarki-

noinnille tyypillisen brändäyksen tietoturvakoulutuksen yhteydessä. Samoin kuin Schultz et al. (2004) McCoy ja Fowler (2004) kritisoivat ”jokaiselle - jotain” - koulutustyyliä. Heidän mielestään koulutusohjelman pitää olla joustava, joka pystyy vastaamaan muuttuviin olosuhteisiin heti kun tarve vaatii. Heidän esittelemä ohjelma koostuu kiinteästä vuosittain evaluoitavasta ohjelmasta ja kuukausittain vaihtuvista teemoista. Koulutusmuodoksi valitaan kullekin kohderyhmälle parhaiten sopiva. Niitä ovat esimerkiksi verkossa tapahtuva tai perinteinen luokkahuoneessa toteutettu opetus.

Edellä mainittu kaikille samanlainen koulutus on merkki siitä, että se perustuu kapea-alaiseen turvallisuusnäkökulmaan, jolloin fokus ei ole ihmisessä. Tietoturvakoulutus saatetaan toteuttaa vain sen vuoksi, että sillä täytetään jokin vuosittainen koulutusnormi. Tietoturvakoulutuksen sisällön saattaa myös määrittellä tarjolla oleva materiaali tai kouluttaja. Tällaisen tarjonta-, tai määräyspainotteisen koulutuksen vaarana on ”juuri jokaiselle jotain” – tyylinen samaa levyä vuodesta toiseen pyörittävä koulutus (Roper et al., 2005). Tietoturvaohjelmat täytyy suunnitella ottaen huomioon organisaation luonne (Layton, 2005). Kouluttajan täytyy myös tunnustaa organisaation kulttuuri, jossa työskentelee (McIlwraith, 2006). Koulutuksen tulisi olla tarvepainotteista ja jo koulutusta suunniteltaessa olisi mietittävä näkökulmaa. Fokus voi olla joko sisällössä tai vaikutuksessa. Sisältönäkökulmaan perustuva koulutus ei ole niin tehokasta kuin vaikutusnäkökulmaan perustuva, jossa koulutettaville kerrotaan kuinka heidän tulisi toimia (Roper et al., 2005). Roper et al. (2005) väittävät, että vaikutusnäkökulman huomioon ottava koulutus on myös vähemmän aikaa vievää, kuin sisältönäkökulman huomioon ottava tietoturvakoulutus.

Vaikutusnäkökulmaan perustuva koulutus tuo tarpeen koulutuksen räätälöintiin (Roper et al., 2005). Opetuksen räätälöinnillä (*tayloring*) varmistetaan siitä, että jokainen koulutettava saa oikeanlaiset ohjeet juuri siihen tilanteeseen, jossa hän joutuu toimimaan. Esimerkiksi organisaation johdolla on erilainen rooli tietoturvan suhteen, kuin työntekijäportaalla. Roper et al. (2005) esittelevät TEAM-mallin (Roper et al., 2005 s. 22–24), jossa on neljä elementtiä joilla puututaan organisaation tietoturvaongelmiin. Harjoittelu (*training*), koulutus (*education*), tietoisuus (*awareness*), tai motivointi (*motivation*) ovat keinoja joilla tuotetaan halutun tyyppisiä vaikutuksia kohderyhmässä. Esimerkiksi jos ihmiset eivät näe jossain tietoturvaohjeessa järkeä, käytetään koulutusta. Jos ihmiset eivät koskaan ajattele tekojensa seurauksia, niin tietoturvatietoisuuden lisääminen lisää ihmisten tietoisuutta tekojensa seurauksista (Roper et al., 2005).

Motivointi vaikuttaa ihmisten uskomuksiin ja sitä kautta asenteisiin (vrt. Ajzen 2005). Asenteilla ja motivaatiolla on siten keskenään yhteys. Jos motivoidaan jotain ryhmää, on hyvä tuntea heidän asenteensa (Roper et al., 2005). Tärkeimmät tekijät tehokkaalle tietoturvalle ovat ihmiset - heidän asenteensa ja käsityksensä oikeasta ja väärästä (Layton, 2005). Toisaalta ihmisten asenteiden mittaaminen on vaikeaa ja joskus tarpeetonta (Siponen, 2000).

Tietoturvan hallinnasta vastaavat uskovat, että työntekijät noudattavat koulutuksen jälkeen ohjeita. Kuinka voidaan olla varmoja ohjeiden noudattamisesta, sillä puheet ja teot usein poikkeavat toisistaan? Jos käyttäjille annetaan kelvolliset argumentit ja he kokevat ohjeet oikeudenmukaisiksi, seuraa siitä positiivisia vaikutuksia käyttäjän aikomukseen noudattaa tietoturvaohjeita (Siponen, 2000). Siponen (2000) väittää myös, että koulutettavat eivät ole halukkaita välittömästi koulutuksen jälkeen noudattamaan ohjeita. Tämä lisää tarvetta tietoturva-asioiden esillä pitämiseen myös koulutuksen jälkeen,

sillä jatkuva, asteittainen tietoturvan parantaminen on tehokkaampaa, kuin yritys saada kerralla kaikki kuntoon (Layton 2005).

Koulutuksen tulee siis vahvistaa oikeanlaisia käyttäytymismalleja ja antaa selkeä kuva organisaation tietoturvapoliitikasta ja tavoitteesta turvallisuuden osalta. Vääränlainen ja väärin suunnattu koulutus rapauttaa tietoturvatyön uskottavuutta sekä myös saattaa antaa johdolle virheellisen kuvan organisaation tietoturvan tilasta. Pelkkä koulutus ja koulutuskertojen lukumäärä ei takaa tietoturvatietoisuuden syntyä. Liian usein, varsinkin ulkopuolisten kouluttajien, jotka eivät ymmärrä organisaation ja koulutettavien erikoispiirteitä, koulutustilaisuudet ovat tylsiä ja täynnä latteuksia tietoturvasta. Tietoturvakoulutuksessa pitäisi sitä vastoin tuoda koulutettaville esiin kuinka opetettavat asiat tulee toteuttaa käytännössä ja kuinka niiden tulisi vaikuttaa jokapäiväiseen työskentelyyn. Tietoturvan noudattamisen hyödyn havaitsemisen sijasta kuulijat saattavat suhtautua kielteisesti esiteltäviin asioihin jos he eivät koe saavan opetukselta mitään uutta (Schultz et al., 2004.) Lisäksi koulutettavat tulisi saada osallistumaan tietoturvatyöhön. Heille ei saisi syntyä tunnetta, että he ovat ulkopuolisia. Siksi ihmisille täytyisi saada syntymään tunne, että tietoturvaongelmat ovat myös heidän ongelmiaan ja että he pystyvät teoillaan vaikuttamaan niihin (McIlwraith, 2006.)

Ihmiset toimivat kuitenkin usein vastoin ohjeita. Vaikka tiedetään tietoturvalliset toimintatavat, toimitaan niitä vastaan. Lee et al. (2003) ovat artikkelissaan selvittäneet työhön kuulumattoman tietokonetyöskentelyn taustoja. Tietoturvaohjeiden noudattamattomuus voi olla tietoinen valinta. Usein tietoturvatietoisuuden puuttuminen liitetään epäeettiseen toimintaan. McNamara, Richardson ja Courtney (2003) tuovat tutkimuksessaan esille sen, kuinka etiikan pettämisellä saattaa olla mittaamattomia seurauksia organisaatiolle ja mahdollisesti laajemmallekin. Heidän mielestään, varsinkin jos epäeettisen käytöksen vaikutukset ovat laajoja, tulisi tällaisen käytöksen seuraukset tehdä näkyviksi (McNamara et al., 2003). Organisaation turvallisuuskulttuurin tulisi olla niin vahva, että siihen ei kuuluisi epäeettiset toimintatavat. Jokaisen työntekijän tulee ymmärtää organisaation tavoitteet ja pystyä sitoutumaan niihin (Torres et al., 2006). Ihmiset eivät aina kuitenkaan noudata tietoturvaohjeita, vaan huolimatta siitä, että ovat vastuullisia toimijoita toimivat vastuuttomasti (Siponen, 2005).

Edellisen perusteella voidaan väittää, että organisaation täytyy ryhtyä toimiin, jotka ottavat eettisen aspektin paremmin huomioon. Tietojärjestelmien väärinkäyttöä yritetään selittää työntekijästä johtuvilla tekijöillä, työolosuhteilla, tai tilanteen tuomilla mahdollisuuksilla. Työntekijästä johtuvia tekijöitä, jotka tuottavat epätoivottua käytöstä voivat olla esimerkiksi rahan ahneus, itsekkyyys, piittaamattomuus, tai poliittiset vaikuttimet. Henkilö, joka kokee tulleen väärin kohdelluksi, tai aliarvostetuksi työnantajan taholta saattaa kostaa kokemansa tietojärjestelmää sabotoimalla. Useimmin tietojärjestelmän väärinkäyttöön kuitenkin ryhdytään, kun ympäristö tarjoaa mahdollisuuden siihen. Tietoturvan teknisiä, sekä lakeihin ja säädöksiin perustuvia kontrolleja tarvitaan, mutta mikäli käyttäjä haluaa vahingoittaa työnantajaansa, eivät tekniset suojaukset tai muut vastatoimet voi sitä estää, sillä tekniikka ei kykene tunnistamaan ongelman moraalista ulottuvuutta. Ilman formaalisia sääntöjä ja ohjeita organisaatio altistuu käyttäjien mielivalalle. Tietoturvakoulutuksella lisätään henkilökunnan tietoturvatietoisuutta ja ymmärrystä siitä, mitä tietojärjestelmän väärinkäytöstä saattaa seurata. Kontrollit, ohjeet ja säännöt ovat tehotomia ilman käyttäjien hyväksyntää ja ymmärrystä. Päinvastoin, säännöt ja kontrollit edellyttävät täydellistä käyttäjien hyväksyntää läpi koko organisaation. Formaalisten sääntöjen ja ohjeiden lisäksi organisaatiot tarvitsevat eettistä tiedostamista myös epämuodollisella tasolla. Tämän johdosta ihmiset organisaation

sisällä tarvitsevat eettistä koulutusta. Eettisellä koulutuksella ei estetä täysin epätoivottavaa käytöstä, mutta sillä kyetään vähentämään sitä (Kesar ja Rogerson, 1997).

Dark ja Winstead (2005) väittävät, että tekniikkaa opettavat henkilöt ovat tottumattomia ja kykenemättömiä opettamaan eettisiä kysymyksiä. Liian usein tietoturvakoulutusta hoitavat epäpätevät henkilöt (McIlwraith 2006). Hyvin helposti opetetaan vain oikean ja väärän käyttäytymisen seurauksia, kun kyse on jostain syvemmästä. Lait määrittelevät oikean ja väärän. Se, mikä on laissa määritelty oikeaksi, ei merkitse sitä, että oikea olisi totta ja väärä olisi valhetta. Moraalisesti oikean ajattelun oppiminen on jatkuva prosessi, jota saattaa olla vaikea istuttaa tavalliseen koulutusmuottiin (Dark ja Winstead 2005).

Dark ja Winstead (2005) väittävät, että konstruktivisen filosofian mukaan tieto ei ole siirrettävissä, vaan se on pikemminkin rakennettavissa. Konstruktivistisen opetusperiaatteen mukaisesti koulutus on tarkoituksen etsimistä. Koulutuksen tarkoitus, joka syntyy kokemuksesta, on tehokas, koska se on perusluonteeltaan henkilökohtaisen havainnoinnin tulosta. Sosiaalinen konstruktivismi pitää sisällään myös ajatuksen, että koulutus on luonteeltaan yhteistyötä usean näkökulman välillä ja edellyttää siksi kokonaisuuksien ja sen osien hahmottamista. Tarkoituksen etsiminen on dynaaminen prosessi ja edellytys oppimiselle. Konstruktivinen koulutusprosessi, jonka tulisi keskittyä ensisijaisesti käsitteisiin ja yleisiin faktoihin, sisältää jännitteitä ristikkäisten uskomusten, ideoiden, asenteiden ja käytöstapojen välillä. Siksi hyvässä opetuksessa kouluttaja ymmärtää koulutettavien arvomaailmaa (Dark ja Winstead, 2005). Tietoturvakoulutus edellyttää myös edellä mainitun kohteen taustan tuntemuksen lisäksi kouluttajalta kokemusta työskentelystä vaihtelevassa tietoturva-ympäristössä. Tähän päästään jatkuvalla opiskelulla (Roper et al., 2005).

3.5 Johtopäätökset teorioista

Tietoturvatutkimusta viranomaisorganisaatioista ei löytynyt. Tämän tutkimuksen kannalta tärkeitä teoreettisia kysymyksiä on kuitenkin käsitelty edellä esitellyissä tutkimuksissa. Niissä on esitelty tietoturvan hallintaprosessia, tietoturvakoulutusta ja tietoturvan perusteorioita. Jos teoreettisen tutkimuksen pohjaa olisi laajennettu vielä nykyistä enemmän käyttäytymistieteiden, kuten kasvatustieteen tai psykologian suuntaan, olisi erilaisia ja käyttökelpoisia pedagogisia teorioita koulutuksen tueksi löytynyt enemmänkin. Esimerkkinä edellisestä esiteltiin (Learner-Centered Psychological Principles), joka sopisi hyvin myös tietoturvaopetuksen teoriaksi (vrt. Lambert, 2000, tai McCombs, 2005).

Vaikka viranomaisorganisaatioita tutkimuskohteena käyttävää tietoturvan hallintaan ja koulutukseen liittyvää tutkimusta ei löytynyt, on aiemman tutkimuksen läpikäyminen ollut tälle tutkimukselle hyödyllistä. Tietoturvan hallinta ja koulutus ovat loppuen lopuksi samanlaisia kaikissa organisaatioissa. Niissä artikkeleissa, joissa käsiteltiin koulutusta, aihetta lähestyttiin myös kohderyhmäkeskeisesti (vrt. Dark ja Winstead 2005; Layton, 2005; McIlwraith, 2006; McCoy ja Fowler, 2004; Roper et al., 2005; Schultz, 2004; Torres et al., 2006; Puhakainen, 2006, sekä McCombs ja Vakili, 2006). Koska erilaisessa toimintaympäristössä toimivilla organisaatioilla on erilainen organisaatiokulttuuri ja koska tietoturvallisuus on osa organisaatiokulttuuria, niin eri organisaatioilla on myös erilainen tietoturvakulttuuri (Schlienger ja Teufel, 2003.) Tästä on johto-

päätöksenä se, että tämä tulisi ottaa huomioon eri toimintaympäristössä toimiville organisaatioille tietoturvakoulutusta suunniteltaessa.

Yksi tämänkin tutkimuksen kannalta huomionarvoinen seikka on syytä esitellä tarkemmin. Vaikka sanktioiden vaikutusten arvioiminen ei ole tämän tutkimuksen tutkimusongelma, on sillä tässä tapauksessa koulutuksen vaikutuksen arvioinnin kannalta merkitystä. Läpikäydyistä artikkeleista käy ilmi selvästi se, että sanktioiden vaikutusten arvioimisessa on vielä tutkittavaa, sillä eri tutkijoilla, ja jopa samoilla tutkijoilla eri tutkimustapauksissa on erilaisia tuloksia sanktioiden vaikutuksesta (vrt. Crano ja Prislin 2006; D'Arcy ja Hovav 2007; Folz ja Jones 2005; Lee ja Lee 2002; McNamara et. al., 2003; Pahlila et al., 2007; Puhakainen 2006, sekä Siponen, 2000).

4. Empiirinen tutkimus tietoturvakoulutuksen vaikutuksista

Edellisissä luvuissa esiteltiin tutkimuksen tutkimusmalli, joka perustui Puhakaisen (2006) väitöskirjassa esittelemään UCIT-mallin (Puhakainen, 2006, s. 74–76) ja tieteellisissä artikkeleissa esiintyneitä tutkimuksia tietoturvan eri osa-alueista. Kirjallisuuskatsauksen tarkoituksena oli selvittää, mitä tutkimuksessa mukana olleista käsitteistä tiedetään ja millä tavalla tietoturvaan vaikuttavia seikkoja oli aiemmin tutkittu. Näiden seikkojen avulla asetettiin empiirisen tutkimuksen tulkintakehys (empiirinen tutkimusmalli).

4.1 Empiirisen tutkimuksen tulkintakehys

Tutkimuksessa haluttiin selvittää empiirisesti tietoturvakoulutuksen vaikutuksia pelastuslaitoksen henkilökunnan aikomukseen noudattaa tietoturvaohjeita ja sitä kuinka koulutus koettiin, sekä sitä soveltuiko koulutusmalli pelastuslaitoksessa annetun tietoturvakoulutuksen koulutusmalliksi. Tätä tarkoitusta varten tieteellisten tutkimusten joukosta etsittiin sopiva tulkintakehys, jota silmällä pitäen mittarit rakennettiin. Tähän tutkimukseen analyysin tulkintakehyksiksi valittiin suunnitellun toiminnan teoriasta (*A Theory of Planned Behaviour*, TPB) ja teknologian hyväksyttävyyssmallista (*Technology Acceptance Model*, TAM) johdettuja malleja (Kuvat 4 ja 5).

TPB- ja TAM- malleja, tai niistä johdettuja malleja on käytetty vastaavissa tutkimuksissa teoreettisina malleina analysoitaessa suhtautumista tietoturvaan tai koulutusmallien hyväksyttävyyttä (Taulukko 1). Alla olevassa taulukossa esitellään tässä tutkimuksessa käytettyjä lähteitä, joissa TPB tai TAM-malli tai niistä johdettu malli ovat olleet tutkimuksen viitekehystenä, tai niillä on muuten ollut tärkeä asema tuloksia analysoitaessa.

Taulukko 1. Kirjallisuuskatsauksessa esitellyt tutkimukset, joissa TPB, TAM- mallia tai niiden johdannaisista on käytetty analyysin välineenä

Lähde	TAM	TPB	TAM- mallin tai TPB:n johdannainen
Crano ja Prislin (2006)		X	
Davis ja Venkatesh (1996)	X		
Siponen (2000)	X	X	
Lee ja Lee (2002)		X	
Rawstorne et al. (2000)	X	X	
Kuo ja Hsu (2001)			X
Lee et. al. (2005)			X
Puhakainen (2006)			X
Pahnila et al. (2007)			X

Ajzenin (2005) suunnitellun toiminnan teoriassa (*The Theory of Planned Behaviour, TPB*) selitetään asenteen ja käyttäytymisaikomuksen suhdetta. Teoriassa tutkitaan, milloin ihminen aikoo käyttäytyä asenteensa mukaisesti ja milloin ei. Suunnitellun toiminnan teoria on yksi eniten sovellettu malli osoittamaan syysuhteita ihmisten käyttäytymiseen (Lee ja Lee, 2002). TPB on Ajzenin ja Fishbeinin vuonna 1975 esittelemän perustellun toiminnan teorian (*Theory of Reasoned Action, TRA*) laajennus. TRA mallista puuttuvat TPB-malliin verrattuna käyttäytymisen sisäiset ja ulkoiset rajoitteet, sekä koetut käyttäytymistä kontrolloivat tekijät. Ajzenin (2005) mukaan asenne on yksi tekijä, joka määrittää käyttäytymisaikomusta. Myös tutkittavan uskomukset sosiaalisista odotuksista, eli subjektiiviset normit ja havaitut vaikutusmahdollisuudet, joita tutkittava uskoo olevan käytössään vaikuttavat osaltaan tutkittavan käyttäytymisaikomukseen.

Henkilön osaaminen tai koettu osaaminen voivat myös rajoittaa käyttäytymistä. TPB-mallissa nämä käyttäytymisen sisäiset ja ulkoiset rajoitteet ovat käyttäytymistä kontrolloivia tekijöitä. Ihminen suunnittelee käyttäytyvänsä asenteensa mukaisesti. Toiminta riippuu siitä, mitä hänelle merkitykselliset toiset ihmiset tai organisaatiot häneltä hänen oman havaintonsa mukaan odottavat ja onko hän motivoitunut noudattamaan heidän odotuksiaan. Toiseksi ihmisen toimintaan vaikuttaa se, miten hän arvioi omat toimintamahdollisuutensa toiminnan suhteen. Tällöin arvioidaan onko toiminta turhaa vai onko toimintaan ryhtyminen oikeasti valittavissa oleva asia. Edellinen perustuu oletukselle, että ihmisillä on mielekäs tapa toimia ja he ottavat huomioon kaiken mahdol-

lisen informaation ja harkitsevat suoraan, tai epäsuoraan toimiensa seuraamuksia. Yksilön aikomus käyttäytymiseen on välittömin ilmenemismuoto tuosta toiminnasta (Ajzen, 2005).

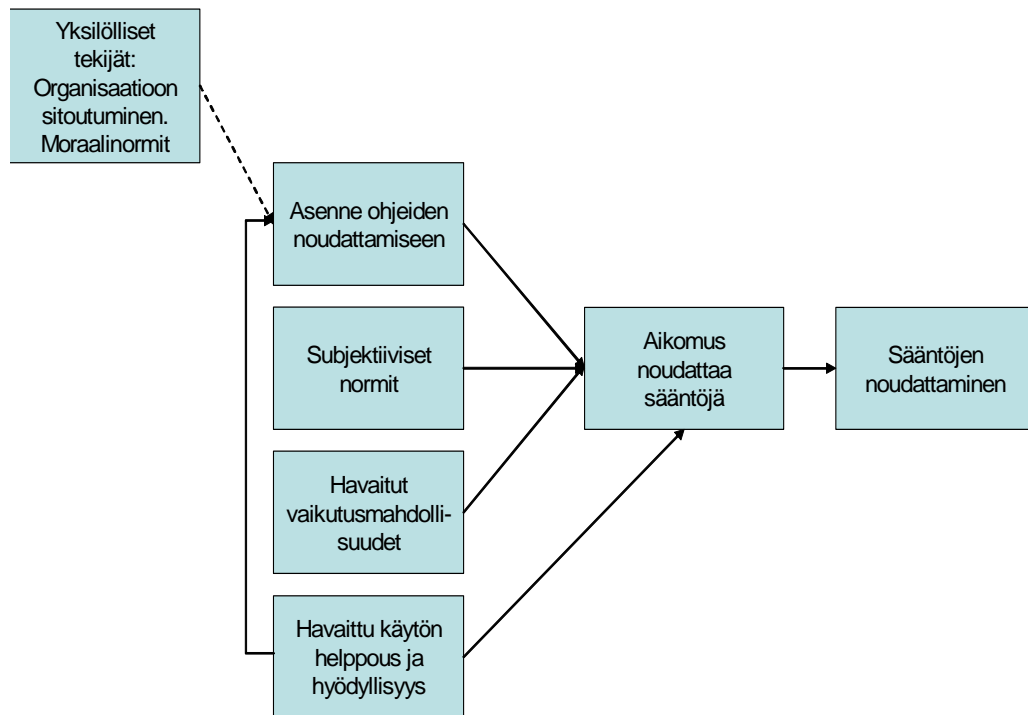
Ajzenin (2005) mukaan TPB:n muuttujista yksi, tai kaksi riittää selittämään toimintaa. Teorian mukaan asenteiden, subjektiivisten normien ja havaittujen toiminnan kontrollien suhteellinen painoarvo riippuu tutkittavasta aikomuksesta. Joillakin aikomuksilla asenteet selittävät enemmän toimintaa, kuin esimerkiksi normit, toisilla aikomuksilla taas havaitut toiminnan kontrollit nousevat tärkeimmäksi selittäjäksi. Lisäksi muuttujien suhteellinen painoarvo vaihtelee eri ihmisillä tai ryhmillä. Havaittu toiminnan kontrolli vaikuttaa vahvimmin motivaation kautta aikomukseen. Jos ihminen uskoo, ettei hänellä ole mahdollisuutta tai hänen ei kannata toimia aikomuksensa mukaisesti, ei hänelle siten synny toiminnan aikomustakaan vaikka omaisikin asenteen aikomusta kohtaan, tai hän kokisi sosiaalista painostusta toiminnan suuntaan (Ajzen, 2005).

Davisin vuonna 1985 esittelemä teknologian hyväksymismalli (*Technology Acceptance Model*, TAM) selittää sen miksi käyttäjät hyväksyvät tietyllä teknologialla toteutetun palvelun. Tämäkin malli on kehitetty Ajzenin ja Fishbeinin vuonna 1975 esittelemästä TRA- mallista. Perustellun toiminnan teorian avulla selitettiin ulkoisten muuttujien vaikutusta ihmisten aikomukseen käyttää tietokoneita. Yksi ulkoisista muuttujista oli koulutus. Davisin ja Venkatesh'in (1996) mukaan TAM- malli on osoittautunut käyttökelpoiseksi ennustettaessa käyttäjien aikomuksia hyödyntää joitain teknisiä palveluita.

Toisaalta TAM-mallia voi käyttää myös selitettäessä, sitä miksi käyttäjät ottavat käyttöönsä organisaatioiden sääntöjen vastaisia toimintamalleja tietokoneen käytössään (Lee, Lim ja Wong, 2005). TAM- mallissa keskeisessä osassa ovat käytön havaittu helppous ja hyödyllisyys (Davis ja Venkatesh, 1996). Havaittu hyödyllisyys tarkoittaa ihmisen käsitystä siitä, miten jonkin tietyn systeemin käyttö parantaa hänen tilannettaan. Havaittu käytön helppous puolestaan tarkoittaa yksilön käsitystä siitä että systeemin käyttö ei edellytä lisäponnisteluja (Puhakainen, 2006). Käytön helppouteen ja hyödyllisyyteen vaikuttaa muun muassa ohjeiden saatavuus ja selkeys. Käytännön kannalta tämä merkitsee sitä, että tietoturvapoliitikat tulee olla nopeasti ja helposti saatavilla ja että niistä saatava informaatio on käyttäjän tarpeisiin sopivaa (Pahnila, Siponen ja Mahmood, 2007). Tutkimusten mukaan hyödyllisyys koetaan helppoutta tärkeämmäksi tekijäksi uusien käytäntöjen käyttöönotossa (Davis ja Venkatesh, 1996). Tämä olisi syytä pitää mielessä koulutuksen sisältöä suunniteltaessa. Tämän tutkimuksen empiriaosassa koulutuksen sisältöä suunniteltaessa hyödyllisyyden korostaminen oli yksi painopistealueista. TAM-mallin rakenteen yksinkertaisuuden vuoksi sitä on helppo soveltaa erilaisissa yhteyksissä. Mallin vahvuutena koettu yksinkertaisuus on myös sen heikkous, sillä perusmalli on niin pelkistetty, ettei se tuota tarpeeksi yksilöityä tietoa tekijöiden taustalla vaikuttavista ulkoisista osatekijöistä. Mallia onkin kehitetty edelleen tuomalla siihen näitä edellä mainittuja ulkoisia osatekijöitä (vrt. Ainsworth, 2006).

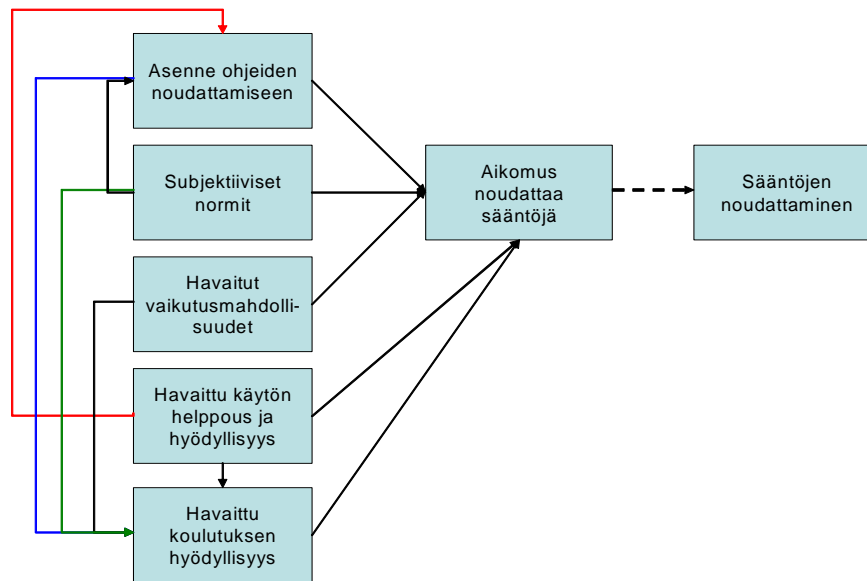
Ennen koulutusta suoritetun kyselyn datan analysointiin käytetty tulkintakehys (Kuva 4) käsittää viisi luokkaa: (1) yksilölliset tekijät, (2) asenne ohjeiden noudattamista kohtaan, (3) Subjektiiviset normit (4) havaitut vaikutusmahdollisuudet ja (5) havaittu käytön helppous ja hyödyllisyys. Kuten aiemmin mainittiin, Ajzen (2005) väittää, että ihmisten toiminta riippuu siitä, mitä heille merkitykselliset toiset ihmiset tai ryhmät heidän omien havaintojensa mukaan heiltä odottavat ja ovatko he motivoituneet noudattamaan näitä odotuksia. Muuttujat, kuten organisaatioon sitoutuminen tai moraalinormit ovat tekijöitä, jotka vahvistavat tai heikentävät ihmisten asenteita toimintaa kohtaan

(Ainsworth, 2006). Tulkintakehykseen otettiin mukaan yksilöllisten tekijöiden luokka Ainsworthin (2006) tutkimusta mukaillen. Koska työtyytyväisyyttä kartoittava tutkimus oli tehty erillään tästä tutkimuksesta, ei tulosten vaikuttavuutta voitu arvioida SEM-analyysin avulla. Siitä syystä yksilöllisten tekijöiden luokka on yhdistetty malliin katkoviivalla.



Kuva 4. Analyysin tulkintakehys ennen koulutusta.

Koulutuksen jälkeen suoritetun kyselyn datan analysointiin käytettävään tulkintakehykseen lisättiin koulutuksen hyödyllisyyttä kuvaava luokka (Kuva 5). Tulkintakehyksissä esiteltyjä muuttujien yhteyksiä toisiinsa on tarkasteltu SEM-analyysin avulla.



Kuva 5. Analyysin tulkintakehys koulutuksen jälkeen.

Tutkimusmalleista johdetaan työn tutkimuskysymykset malleissa esiintyvien muuttujaluokkien mukaisesti. Yllä esitellyissä malleissa käytetyt avainkäsitteet selvitetään seuraavassa tarkemmin.

Aikomus

Toimintaa voi ennustaa huomattavan tarkasti aikomuksesta. Yksilön aikomuksen toimintaa kohtaan voi puolestaan ennustaa asenteista toimintaa kohtaan, subjektiivisista normeista, sekä havaituista vaikutusmahdollisuuksista (havaituista toiminnan kontroleista) (Ajzen, 2002). Aikomuksen ja toteutuneen toiminnan välistä ennustettavuutta tutkittaessa on havaittu, että aikomus ennustaa n. 28 prosenttisesti toimintaan ryhtymistä. Yli 70 % selittämättömiä muuttujia on nähty pulmalliseksi, mutta ongelmalle on löydetty selitykseksi se, että vahva aikomus ennustaa paremmin toimintaa, kuin heikko aikomus toiminnan puutetta (Grano ja Prislin, 2006).

Asenne tietoturvan noudattamista kohtaan

Suunnitellun toiminnan teoria (TPB) perustuu olettamukseen, että yksilöt yleensä käyttäytyvät mielekkäästi ja ottavat huomioon kaiken käytettävissä olevan sisäisen, tai ulkoisen informaation harkitessaan toimintansa seurauksia. Asenne merkitsee johonkin sosiaalisesti merkitykselliseen kohteeseen, henkilöön, instituutioon, tai tapahtumaan liittyvä myönteistä tai kielteistä suhtautumistapaa. Teorian mukaan asenteet toimintaa kohtaan määräytyvät uskomuksista (*behavioral beliefs*) kyseessä olevan toiminnan seurauksista. Jokainen toimintaa koskeva uskomus yhdistyy tiettyyn toiminnan aiheuttamaan tulokseen, tai ominaisuuteen kuten hyötyyn tai haittaan. Siten asenteeseen toimintaa kohtaan vaikuttavat uskomukset toimintaa seuraavista vaikutuksista. Esimerkiksi vähäsuolainen dieetti (toiminta) vähentää verenpainetta (uskomus vaikutuksesta) (Ajzen, 2005).

Subjektiiiviset normit

Subjektiiivisilla normeilla tarkoitetaan yksilön havaitsemaa sosiaalista painetta, jolla on vaikutusta toiminnan toteutumiseen (Lee ja Lee, 2002). Ainsworth (2006) väittää, että ihmisillä on oletuksia, siitä kuinka muut odottavat heidän toimivan. Ajzenin (2005) mukaan tällöin puhutaan normatiivisista uskomuksista. Tällöin on kyse yksilön uskomuksista sen suhteen, mitä toiset yksilöt tai ryhmät pitävät hyväksyttävänä tai paheksuttavana toimintana. Yleisesti ottaen ihmiset, jotka mieltävät itsensä jonkin ryhmän jäseniksi kokevat sosiaalista painetta käyttäytyä ryhmän tavoin tai noudattaa sen mieltämiä. Tällaisia yksilölle merkittäviä käyttäytymiseen vaikuttavia ihmisiä saattaa löytyä perheen jäsenten, työkavereiden, ystävien tai esimiesten joukosta.

Havaitut käyttäytymistä kontrolloivat tekijät (havaitut vaikutusmahdollisuudet)

Yksilön osaaminen tai koettu osaaminen voivat myös rajoittaa käyttäytymistä. TPB-mallissa nämä käyttäytymisen sisäiset ja ulkoiset rajoitteet, tai havaitut vaikutusmahdollisuudet, ovat käyttäytymistä kontrolloivia tekijöitä. Näiden tekijöiden taustalla olevien uskomusten läsnäolo tai puuttuminen vahvistaa, tai heikentää toimintaan ryhtymistä. Nämä uskomukset voivat perustua kokemukseen mutta useimmiten vaikuttavana tekijänä on toissijainen informaatio. Mitä enemmän määriteltyjä resursseja tai mahdollisuuksia yksilö ajattelee omaavansa ja mitä vähemmän negatiivisia tekijöitä havaitaan, sitä suurempi havaittu kontrolli toimintaa kohtaan tulee olemaan (Ajzen, 2005).

Havaittu hyödyllisyys ja käytön helppous

Vaikka Davisin 1985 luomalla teknologian hyväksymismallilla yleensä selitetään sitä, miksi käyttäjät hyväksyvät tietyllä teknologialla toteutetun palvelun, voidaan TAM-mallia käyttää myös selitettäessä, sitä miksi käyttäjät ottavat käyttöönsä organisaatioiden sääntöjen vastaisia toimintamalleja tietokoneen käytössään (Lee, Lim ja Wong, 2005). Tässä tutkimuksessa ei selittävänä tekijänä ole sääntöjen vastainen toiminta, vaan TAM-mallin mukaisella käytön helppouden ja hyödyllisyyden kokemisella pyritään ennustamaan tietoturvaohjeiden noudattamista. Tässä tutkimuksessa TAM-mallin avulla selitetään, sekä käyttäjien suhtautumista tietoturvaohjeisiin, että heidän havaintoja ja koulutuksen hyödyllisyydestä.

TAM-mallissa koettu käytön helppous tarkoittaa sitä, missä määrin henkilö kokee järjestelmän käytön (tai tässä tapauksessa tietoturvaohjeiden noudattamisen) olevan vaivatonta. Käytön helppoudella on mallin mukaan voimakas vaikutus myös koettuun hyödyllisyyteen (Davis ja Venkatesh, 1996). TAM-mallissa havaittu hyödyllisyys ja käytön helppous on erotettu toisistaan omiksi kokonaisuuksiksi, missä käytön koettu helppous vaikuttaa palvelun hyödylliseksi kokemiseen. Koettu hyödyllisyys ja koettu käytön helppous vaikuttavat käyttöaikomuksiin asenteen kautta, vaikka koetulla hyödyllisyydellä on käyttöaikomuksiin myös suora vaikutus. Asenne toimintaa kohtaan on luonteeltaan henkilökohtainen ja se voi olla joko positiivinen tai negatiivinen. Toisin sanoen positiivinen suhtautuminen asennetta kohtaan ilmenee aikomuksena käyttää järjestelmää (Davis ja Venkatesh, 1996).

Yksilölliset muuttujat

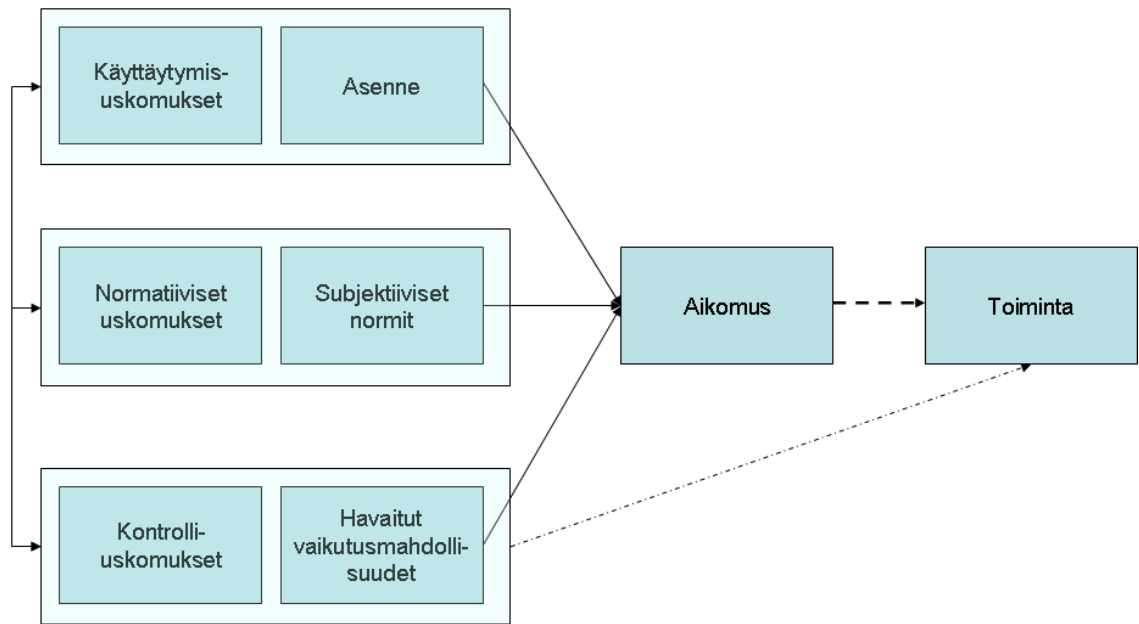
Yksilölliset muuttujat kuvaavat tässä sitä, mitkä tekijät katsotaan vaikuttavan yksilön asenteeseen ohjeiden noudattamista kohtaan. Asenteisiin vaikuttavia tekijöitä on monia, kuten sukupuoli, ikä, koulutus, sosiaalinen asema tai kasvatusta. Moraalinormeilla on todettu olevan vaikutusta eettiseen käyttäytymiseen aikomukseen tietotekniikassa. Sitoutumisen työnantajaan puolestaan uskotaan olevan selitys siihen, miten vahvasti työntekijät haluavat noudattaa sääntöjä (Ainsworth, 2006). Yksilölliset muuttujat ovat tässä mallissa mukana siitä syystä, että niiden avulla voidaan selittää asenteen vahvaa vaikutusta aikomukseen toteuttaa tietoturvaohjeita ennen koulutusta.

Sitoutuminen organisaatioon on työntekijän työssä viihtymiseen vaikuttava tekijä ja on yhteydessä työn mielekkyyden kokemiseen. Työ koetaan mielekkääksi jos tunnetaan, että tehtävä työ on tärkeää. Useiden tutkimusten valossa työhönsä tyytyväinen ihminen on todennäköisimmin sitoutunut työnantajaansa, kuin ihminen, joka on tyytymätön työhönsä. Työtyytyväisyys ennakoii sitoutumista voimakkaammin, kuin esimerkiksi ikä, sukupuoli, virka-asema, palkka, tai uraodotukset (Ahuja, Chudoba, George, Kacmar ja McKnight, 2002). Sitoutuminen on yksi osa sosiaalisia siteitä. Sosiaaliset siteet estävät yksilöä ryhtymästä epätoivottavaan toimintaan organisaatiota kohtaan. Sosiaalisen siteen teoria olettaa, että kaikilla ihmisillä on taipumus rikolliseen toimintaan elleivät sosiaaliset siteet estä sitä (Lee ja Lee, 2002).

Ainsworthin (2006) mukaan työntekijän moraalinnormit vaikuttavat hänen aikomukseensa epätoivottavan toiminnan suhteen. Siposen (2000) mukaan on mahdollista saavuttaa moraalinen vastuuntunto, jos turvallisuustoimenpiteet nähdään työntekijän kannalta moraalisesti hyväksyttävänä. Pidemmällä aikavälillä vastuuntunnon tulisi muuttua sisäiseksi. Ulkoiset normit ja määräykset, jos ne ovat pakottavia ja jyrkkiä, saatetaan kokea painostavina ja ne saattavat aiheuttaa vastustusta, tai jopa epätoivottavaa käyttäytymistä (Siponen, 2000).

Uskomukset (beliefs)

Ihmiset päätyvät toteuttaa aikomuksensa uskomustensa perusteella. Uskomusten toimintaan ryhtymisen surauksista ei tarvitse perustua totuuteen. Ne voivat olla epärationaalisia, perustua ennakkoluuloihin tai olla virheellisiä. Tästä huolimatta, kun uskomukset ovat muotoutuneet, niin ne muodostavat tiedollisen perustan asenteille, subjektiivisille normeille ja havaituille käyttäytymistä kontrolloiville tekijöille ja lopulta aikomukselle ja toiminnalle (Kuva 6). Asenteet toimintaa kohtaan määräytyvät uskomuksista (*behavioral beliefs*) kyseessä olevan toiminnan seurauksista. Jokainen toimintaa koskeva uskomus yhdistyy tiettyyn toiminnan aiheuttamaan tulokseen, tai ominaisuuteen kuten hyötyyn tai haittaan (Ajzen, 2005). Subjektiiivisten normien taustalla olevia uskomuksia ovat yksilön uskomukset siitä, miten hänelle tärkeät ihmiset tai yhteisöt käsillä olevasta toiminnasta ajattelevat, tai miten heidän on uskottu toimineen samassa tilanteessa.



Kuva 6. Uskomukset tiedollisena perustana aikomukselle ja toiminnalle suunnitellun toiminnan teoriassa (Ajzen, 2005).

Havaittujen vaikutusmahdollisuuksien tai toiminnan kontrollien taustalla olevien uskomusten perusteella yksilöt päättävät, mitä toimintaan ryhtyminen heiltä edellyttää. Esimerkiksi tietoturvaohjeita noudatetaan, jos niiden noudattaminen havaitaan helpoksi (Ainsworth, 2006).

4.2 Mittarit ja menetelmät

Ennen koulutusta suoritetussa kyselyssä kysymykset jaettiin kahteen osaan. Ensimmäisen kyselyn ensimmäisen osan kysymyksillä (53 kpl) haluttiin selvittää vastaajien tietoturvan lähtötasoa ja suhtautumista tietoturvaohjeisiin. Kysymyksistä valittiin tähän tutkimukseen ne, jotka soveltuivat selittämään valitun tulkintakehyksen (kts. kuva 4, s. 30) muuttujia. Tulkintakehyksen muuttujia olivat; (1) asenne ohjeiden noudattamista kohtaan, (2) Subjektiiiset normit, (3) havaitut vaikutusmahdollisuudet, (4) havaittu käytön helppous ja hyödyllisyys, sekä (5) aikomus. Ensimmäisen kyselyn toisessa osassa kysyttiin niitä asioita, joita pelastuslaitoksen keskuskunnalle laadittu ohjeistus pitää sisällään. Tällä toisella kysymysosalla oli tarkoitus selvittää se, mitä vastaajat entuudestaan tiesivät ohjeessa käsitellyistä tietoturva-asioista. Kyselylomake on vastauksineen liitteessä C sivuilla 55–56. Tämän osion tuloksia käytettiin koulutuksen sisällön ja painopistealueiden suunnittelussa. Ensimmäisen osan 53 kysymystä oli laadittu seitsemänportaisella Likertin asteikolla ja toisen osan kysymykset olivat monivalintakysymyksiä.

Toinen kysely, jonka kysymykset laadittiin tulkintakehyksen (kts. kuva 5, sivu 30) muuttujia silmällä pitäen, tehtiin koulutuksen tehon mittaamiseksi ja toteutettiin viisiportaisella Likertin asteikolla. Toisen kyselyn väittämällä haluttiin selvittää vastaajien suhtautumista tietoturvaohjeiden noudattamiseen koulutuksen jälkeen ja heidän havaitsemansa koulutuksen hyödyllisyys. Tämän takia toisen kyselyn tulkintakehykseen lisättiin havaittu koulutuksen hyödyllisyys-muuttujaluokka.

Ennen koulutuksen aloittamista tehtiin suppea kysely kahdenkymmenen kahden pelastuslaitoksen tietohallinnosta vastaaville. Ennen kyselyä kaikille pelastuslaitoksille tehtiin soittokierros, jossa halukkuus kyselyyn varmistettiin ja sovittiin ehdot, millä tulokset saadaan julkaista. Kysymykset oli laadittu viisiportaisella Likertin asteikolla. Asteikko laadittiin siten, että skaala käsitti jyrkästi erimieltä väittämän kanssa olevan valinnan ja täysin samaa mieltä olevan vaihtoehdon. Asteikon keskellä vaihtoehdot merkitsivät standardin Likertin-asteikon mukaisesti sitä, että vastaajalla ei ole mielipidettä (1=täysin samaa mieltä, 2= osittain samaa mieltä, 3= ei samaa eikä eri mieltä, 4=jokseenkin eri mieltä, 5= täysin eri mieltä.). Kahdessa kyselyssä asteikko oli yhdestä viiteen ja yhdessä, eli ensimmäisessä, yhdestä seitsemään.

4.3 Summamuuttujien muodostaminen

Tämän tutkimuksen kyselytutkimuksessa käytettiin ensimmäisen kyselyn osalta valmiita kysymyksiä, jotka olivat Oulun yliopiston Fusion- projektin⁵ laatimia. Tämän tutkimuksen mittareina käytettiin siinä mielessä valmiita mittareita, että ne johdettiin mittareista, jotka olivat validoitu ja todettu luotettaviksi aiemmissa tutkimuksissa (kts taulukko 1, s. 28).

Liitteessä G esitellään ensimmäisen kyselyn summamuuttujien pohjana olevat kysymysryhmät, joiden avulla käsitteet operatonalisoiitiin. Kysymysryhmät muodostettiin TPB:n ja TAM-mallin muuttujien perusteella. Ensimmäisen kyselyn kysymyksistä muodostettiin muuttujat asenteelle, normeille, vaikutusmahdollisuuksille, käytön helppoudelle ja aikomukselle. Muuttujat laskettiin keskiarvona niitä selvittäneistä kysymyksistä. Ensimmäisen kyselyn kysymyksistä käytettiin niitä, jotka vastasivat tulkintakehyksen tarpeita. Aikomusta tietoturvan noudattamiseen selvitettiin ensimmäisellä kysymyksellä. Asenteeseen liittyvistä kysymyksistä asenne-muuttujan laskemiseen käytettiin ensimmäisessä kyselytutkimuksessa kysymyksiä 7, 8, 9, 10, 11, 12, 33, 34, ja 35. Normi-muuttujan laskemiseen käytettiin kysymyksistä numeroita 18, 19, 20, 21, 37, ja 38. Havaittuja vaikutusmahdollisuuksia selvitettiin kysymysten 13, 14, 26, 48, 49, ja 50 avulla. Havaittua käytön helppoutta ja hyödyllisyyttä selvittävä muuttuja saatiin kysymysten 26, 29, 30, 32 ja 47 perusteella.

Toinen kysymyspatteri oli suppeampi, kuin ensimmäinen. Samoin kuin ensimmäisen kyselytutkimuksen kohdalla kysymykset suunniteltiin sen perusteella, että ne vastaavat tulkintakehyksen tarpeita. Kysymysten suunnittelun apuna käytettiin valmiita TPB ja TAM-mallia testanneita tutkimuksia (mm. Ainsworth, 2006; Ajzen, 2005; Davis ja Venkatesh, 1996; Pahlila et al., 2007, sekä Puhakainen, 2006).

Myös toisen kysymyspatterin viisiportaiselle Likertinasteikolle laadituista kysymyksistä muodostettiin muuttujat asenteelle, normeille, vaikutusmahdollisuuksille, käytön helppoudelle ja aikomukselle. Toisen kyselytutkimuksen vastauksien tulkintakehykseen oli lisätty tietoturvakoulutuksen hyödyllisyyttä selvittävä muuttujaluokka. Muuttujat

⁵ Fusion- projekti on Oulun Yliopiston tietojenkäsittelytieteidenlaitoksen tietoturvaprosjekti, jossa on tutkittu tietoturvallisuuden keskeisimpiä ongelma-alueita. Keskeisimmät tutkimustulokset liittyvät tietoturvaohjeiden noudattamiseen.

laskettiin keskiarvona niitä selvittäneistä kysymyksistä. Liitteessä H esitellään ensimmäisen kyselyn muuttujien pohjana olevat kysymykset.

Aikomusta tietoturvan noudattamiseen selvitettiin kysymyksellä numero yksi. Asenteeseen liittyvistä kysymyksistä asenne-muuttujan laskemiseen käytettiin toisessa kyselytutkimuksessa kysymyksiä 10 ja 15. Normi-muuttujan muodostamiseen käytettiin kysymyksiä 8, 11 ja 20. Kysymysten 13 ja 14 avulla muodostettiin havaittuja vaikutusmahdollisuuksia selvittävä muuttuja. Havaittua käytön helppoutta ja hyödyllisyyttä selvittävää muuttuja tehtiin kysymysten 17, 18 ja 19 perusteella. Viimeisenä muodostettiin muuttuja koulutuksen hyödyllisyyden arvioimiseksi kysymysten 2, 3, 4, 5, 6 ja 7 avulla.

4.4 Tietoturvakoulutuksen käytännön toteutus ja aineiston kerääminen.

Empiirinen tutkimus toteutettiin pelastuslaitoksessa, jossa työskenteli tutkimuksen aikana noin 120 henkilöä 22 kunnassa. Tämän tutkimuksen aikana suoritettiin kolme kyselyä. Kyselyistä kaksi oli myös osa koulutusprosessia. Tämä tutkimusprosessi aloitettiin suorittamalla kysely pelastuslaitoksen ja sen isäntäkunnan henkilökunnalle, Ensimmäiseksi suoritettuna kyselyn tulosten perusteella saatiin selville koulutuksen painopistealueet ja koulutettavien suhtautuminen tietoturvaohjeiden noudattamiseen ennen koulutusta. Ennen koulutusta suoritettu kysely tehtiin pelastuslaitoksen isäntäkunnan koko henkilökunnalle ja kyselyn kysymyksiin vastattiin Oulun Yliopiston tietojenkäsittelytieteiden laitoksen palvelimella sijainneelle kyselylomakkeelle. Toisen kyselyn avulla selvitettiin koulutuksen vaikuttavuutta koulutuksen jälkeen. Tämän kyselyn tuloksia käytetään myös tulevan koulutuksen suunnittelussa. Kolmas kysely oli suunnattu pelastuslaitosten tietohallinnosta vastaaville ja sen tarkoitus oli muun muassa selvittää oliko vastaavanlaisia koulutusta suoritettu jossain muussa pelastuslaitoksessa.

Ensimmäisen kyselyn jälkeen tietoturvakoulutusta annettiin viidelle ryhmälle. Aiemmin esitellyn suunnitteluprosessin mukaisesti ensin määriteltiin opetukselliset tavoitteet. Siksi ensimmäisenä koulutettavana ryhmänä oli johdon ja hallinnon henkilökunta. Sisällöllisesti johdon koulutus jakaantui kahteen osaan: koulutustavoitteita käsitteeseen johdon seminaariin ja varsinaiseen johdon tietoturvakoulutukseen. Ennen koulutusta toteutettu riskikartoitus ja ensimmäinen kysely olivat pohjana koulutustavoitteita määriteltäessä. Ensimmäisessä kyselyssä oli kysymyspatteri, jolla suunnitteluprosessin mukaisesti kohderyhmän tiedot ja taidot selvitettiin (kts. liite D).

Koska koulutus oli osa vasta aloitusvaiheessa olevaa tietoturvan hallintaprosessia, tärkein painopiste päätettiin laittaa tietoturvasäädösten ja pelastuslaitoksen tietoturvapoliittikan esittelemiseen. Toisena tärkeänä seikkana pidettiin sitä, että henkilökunta tulee tietoiseksi tietoturvan merkityksestä pelastuslaitokselle. Kolmantena asiana koulutuksessa päätettiin käsitellä niitä seikkoja, joiden riskikartoituksessa ja kyselytutkimuksessa todettiin tarvitsevan huomiota. Esimerkiksi käyttäjätunnusten ja salasanojen oikeanlainen käyttö ja tietoturvaohjeiden tunnetuksi tekeminen vaativat huomiota.

Toisen koulutusryhmän muodostivat eri toimialueiden päällystö ja esimiehet. Tällaisia koulutustilaisuuksia järjestettiin yhteensä kolme kappaletta. Näissä koulutustilaisuuksissa esiteltiin pelastuslaitoksen johdon hyväksymä koulutuspaketti. Koulutuksessa korostettiin esimiesportaan vastuuta tietoturvan suhteen. Pelastuslaitoksessa ollaan ottamassa uusia johtamisjärjestelmiä käyttöön. Tämän seurauksena esimiehille tulee tieto-

tekniikan osalta lisää koulutusvastuuta. Tietotekniikan osuus päivittäisessä työskentelyssä tulee kasvamaan muutenkin huomattavasti, joten esimiesten on tietotekniikkakoulutusta suunnitellessaan osattava ottaa huomioon myös tietoturva. Kysymykset jaettiin koulutuksen jälkeen, tai lähetettiin sähköpostilla kaikille koulutukseen osallistuneille ja heitä pyydettiin lähettämään vastaukset kirjepostilla tutkimuksen tekijälle ilman lähettäjä tietoja.

Kolmantena ryhmänä koulutettiin miehistö. Miehistön osalta koulutus oli sisällöltään sama, kuin päällystön ja esimiesten, mutta siinä painotettiin tietoturvan merkitystä käytännön kannalta. Tässä koulutuksessa tietoturvan merkitys pyrittiin havainnollistamaan esimerkkien avulla. Tällä tavalla kohderyhmälle selvitettiin mitä tietoturva merkitsee pelastuslaitoksessa työskentelevälle ja mitä erityispiirteitä mahdollisesti siinä on.

Kaikissa koulutustilaisuuksissa pyrittiin asioita käsittelemään pelastusalan näkökulmasta. Koulutuksessa pyrittiin lähestymään ongelmakeskeisesti tietoturvaa. Riskikartoituksessa ja kyselytutkimuksessa esiin tulleita, sekä keskustelujen esiin nostamia asioita puitiin tietoturvasäädösten ja tietoturvaohjeiden kannalta siten, että asiat kytkettiin pelastusalan kontekstiin.

4.5 Aineiston koodaaminen

Hirsjarven et al. (2004) mukaan aineistosta päästään tekemään analyysia vasta esitöiden jälkeen. Kun mittarit ja menetelmät on valittu, sekä aineisto kerätty, sille suoritetaan vielä tietojen tarkastus, mahdollinen tietojen täydentäminen ja järjestäminen.

Tämän tutkimuksen aineistolle tehtiin tarkastus mahdollisten muusta joukosta huomattavasti poikkeavien vastausten varalta. Outlierit, eli muusta joukosta poikkeavat havainnot hankaloittavat väistämättä aineiston tulkintaa ja vaikeuttavat muuttujien välisen suhteiden havaitsemista. Poikkeamat saattavat johtua, joko vastaajan ymmärrettyä väärin asteikon napaisuuden tai siitä, että väittämiä ei ymmärretty oikein (Järvinen ja Järvinen, 2000). Toisistaan huomattavasti poikkeavia vastauksia aineistosta ei havaittu, joten aineisto voitiin syöttää SPSS- ohjelmistoon analysoitavaksi.

Kerätty aineisto analysoitiin käyttämällä kvantitatiivisen aineiston analysointiin suunniteltua SPSS (*Statistical Package for Social Sciences*) ohjelmaa. Ennen aineiston käsitteilyä SPSS ohjelmalla se järjestettiin ja sille tehtiin tarvittavat muokkaukset Microsoft Excelissä. Lisäksi ensimmäisen kyselyn tuloksista poistettiin ikä-, sukupuoli-, sekä virka-asematiedot, joita ei toisessa kyselyssä enää kysyty.

Tutkimuksen rajauksessa päädyttiin siihen, että koulutuksen kohdeorganisaatioksi otetaan pelastuslaitoksen henkilökunta. Koska kysymyslomakkeissa vastaajien työpaikkaa anonymiteetin takaamiseksi ei kysyty, jälkikäteen pelastuslaitoksen henkilökunnan vastauksia ei voitu eristää datasta. Tämän vuoksi ensimmäisen kyselytutkimuksen data ei sellaisenaan välttämättä ole täysin luotettava pelastuslaitoksen henkilökunnan tietoturvan lähtötason mittaajana. Pelastuslaitoksessa työskenteli kysymysten esittämisen aikaan naisia vain kolme, joten vastaajista jätettiin naiset ensimmäisen kyselyn tuloksista kokonaan pois.

4.6 Mittareiden luotettavuus ja pätevyys

Järvisen ja Järvisen (2000) mukaan mittaaminen riippuu mitta-asteikosta, mitattavasta kohteesta mittavälineestä ja mittaustavasta. Jokaisen tieteellisesti pätevän mittauksen vaatimuksena on luotettavuus (*reliability*) ja pätevyys (*validity*). Luotettavuus tarkoittaa tuloksien toistettavuutta eri mittauskerroilla ja pätevyys sitä, että kerätty data vastaa tutkimiskysymyksiin (Levin, 2004). Käytettyjen mittareiden luotettavuuden tarkastelu kuuluu tieteelliseen tutkimukseen. Mikään mittaaminen ei ole absoluuttisen luotettava, vaan luotettavuus on usein asteikkokysymys. Mittarin pätevyys on abstraktimpi asia, kuin sen luotettavuus, sillä tulos on pätevä vain siinä tapauksessa, että se mittaa vain sitä asiaa tai ilmiötä, jota se on asetettu mittaamaan. Siinä missä luotettavuus keskittyy tiettyyn mitattavaan ominaisuuteen ja pysyy stabiilina useiden mittauskertojen jälkeenkin, koskee pätevyys kriittistä yhteyttä mitattavan (teoreettisen) käsitteen ja todellisen mitaustuloksen välillä (Muijs 2004.) Tässä tutkimuksessa sisällön validiteettia parantaa se, että mittarien kokoamisessa oli käytetty aiemmin valideiksi todettuja mittareita.

Kyselyn kysymyksistä muodostettiin summamuuttujat vastaamaan tulkintakehysten muuttujia. Asteikon (mittarin) vastauksista voidaan muodostaa muuttujia, joita käytetään yläkäsitteenä. Tosin tutkijoiden kesken vallitsee erilaisia mielipiteitä siitä, voidaanko vastauksia summaamalla muodostettuja muuttujia pitää kvantitatiivisena muuttujana, josta voidaan tehdä vaativia tilastollisia tarkasteluja (Järvinen ja Järvinen, 2000.)

Kun käsitteitä halutaan empiirisesti mitata, niitä joudutaan operationaalistamaan, jolloin selvitetään miten kulloistakin mitattavaa käsitettä pyritään mittaamaan. Ongelmaksi muodostuu se, että käyttäytymistieteissä samasta käsitteestä saattaa löytyä useita operationaalisia vastineita. Tällöin puhutaan mittauksen validiusongelmasta (Hirsjärvi et al., 2004).

Valittu tiedonkeruutapa ja väline vaikuttavat osaltaan tulosten pätevyteen. Huonosti laaditut kysymykset eivät välttämättä anna vastauksia mitattavaan asiaan. Suoritetut kyselyt olivat Likertin asteikolla tehtyjä kyselyjä. Poikkeuksen teki ensimmäisen kyselytutkimuksen yhteydessä ollut käyttäjien tietoturvasoaa mittaava osio, joka sisälsi monivalintakysymyksiä tietoturvasoaa.

Menetelmänä kyselytutkimus on yksi yleisimmistä kvantitatiivisen tutkimusmenetelmän tiedonkeruutavoista. Kyselytutkimus voidaan toteuttaa monella eri tavalla, mutta luonteenomaista erityyppisille kyselytutkimuksille, kuten survey on, että aineistoa kerätään standardoidusti (Mujis, 2004.) Joustavuutensa vuoksi kyselytutkimus valittiin tämän tutkimuksen tutkimusaineiston keruumenetelmäksi.

Puute kyselytutkimuksessa on se, ettei tutkija voi sen avulla kontrolloida olosuhteita ja se on siten huomattavasti sopiva kausaalisuhteiden kuvaamiseen kuin kokeelliset menetelmät. Pitkittäistutkimuksella, keräämällä riittävän määrän sopivia muuttujia, ja huolellisella mallintamisella on kuitenkin mahdollista selvittää syy- ja seuraussuhteita ilmiöiden välillä (Hirsjärvi et al., 2004). Lisäksi kyselyjen avulla prosessien syvempää ymmärrystä tai käsitteellisiä eroavaisuuksia on vaikeampaa analysoida. Esimerkiksi surveyn heikkoudeksi on esitetty siinä suoritettavan itsearvioinnin epäluotettavuutta. On huomattu, että tutkimustulokset saattavat muuttua jos kyselyn avulla saatuja tuloksia verrataan ulkopuolisen arvioijan tuloksiin (Mujis, 2004.)

Hirsjärvi et al. (2004) väittävät, että kyselytutkimuksessa ei ole mahdollista varmistua vastausten luotettavuudesta, koska vastaajien rehellisyydestä ja huolellisuudesta ei voida olla varmoja ja toisinaan vastaamattomuus nousee suureksi. Lisäksi on epävarmaa ovatko vastausvaihtoehdot onnistuneita vastaajien näkökulmasta, tai ovatko vastaajat ylipäättään selvillä aihealueesta tai perehtyneitä kysyttävään asiaan. Voidaan olettaa, että tässä tutkimuksessa vastaajat antoivat totuuden mukaisia vastauksia, sillä heidän anonymiteettiä pyrittiin varmistamaan. Vastausvaihtoehtojen väärinymmärtämisen sijaan ei pystytty varmistamaan. Vastaamattomuus, joka oli suuri varsinkin ensimmäisen kyselyn aikana ja saatu palaute viittasivat vaikeaselkoiisiin kysymyksiin, mikä saattaa johtaa väärinymmärtämiseen. Toisen kyselyn aikana palautetta kysymysten vaikeudesta ei saatu, mutta osalla kysymyskaavakkeen saajista toisessakin kyselyssä kysymysten vaikeus saattoi olla syynä vastaamattomuuteen.

Järvinen ja Järvinen (2000) mainitsevat harhat eli ei-satunnaisvirheet, jotka ovat subjektiivisen tiedon vaikeasti tunnistettavia mittausvirheitä. Harha esiintyy, kun joku muuttuja, jota ei huomattu tai voitu mitata systemaattisesti, vinouttaa mittausprosessia. Subjektiivisuus aiheuttaa kyselyihin harhoja kahdella tavalla; 1) vastaajalta voidaan kysyä parasta ”arvausta”, tai 2) häneltä kysytään mielipiteitä tutkittavasta asiasta. Harha vaikuttaa pääasiassa tutkimuksen validiteettiin (Järvinen ja Järvinen, 2000.) Tämän tutkimuksen ensimmäisessä kyselyssä oli paljon subjektiiviseksi luokiteltavia kysymyksiä, jotka aiheuttivat vinoutta mittausprosessiin. Tämän lisäksi ensimmäisen kyselyn aineiston joukossa oli nolla-arvon saaneita vastauksia. Tulosten vinoudesta johtuen nolla-arvoja ei voitu koodata keskiarvoon, vaan ne jätettiin tuloksiin. Tämä aiheutti joidenkin kysymysten osalta hieman vääristymää Likert-asteikon toiseen päähän. Toisessa kyselyssä pyrittiin ottamaan huomioon ensimmäisen kyselyn puutteet. Toisen kyselyn puutteena voidaan pitää kvantitatiiviselle tutkimukselle erittäin pientä (32 kpl) otoskokoa ja käytettyjen kysymysten pientä määrää, jolloin mittarin yhtenäisyyden mittaaminen on ongelmallista.

Tässä tutkimuksessa PLS-menetelmää käytettiin yksittäisten ja latenttien muuttujien välisten yhteyksien tarkastelussa. Tässä tutkimuksessa käytettyjen yksittäiset muuttujat luokiteltiin SEM-mallinnuksen kohdalla formatiivisiksi muuttujiksi, jolloin latentin muuttujan indikaattorit selittävät ilmiötä, eikä formatiivisten muuttujien käyttö edellytä korrelaatiota muuttujien välillä (Bollen ja Lennox, 1991, 307). Toisin kuin reflektiivisten muuttujien kohdalla, multikolleneiarisuus on ongelma formatiivisten muuttujien kohdalla (Jarvis et al., 2003). Tosin aineistossa tätä ongelmaa ei havaittu. Formatiiivisten mittareiden luotettavuutta arvioitaessa ei voida käyttää perinteisiä menetelmiä (faktorilataukset ja reliabiliteettikerroin), vaan sisäistä koostumusta tarkastellaan latenttien muuttujien indikaattoreiden sisäisellä painoarvolla (*inner weight*) ja niiden tilastollisella merkittävyydellä (mm. Jarvis et al., 2003).

5. Empiirisen tutkimuksen tuloksien tarkastelu

Tässä luvussa käydään läpi tutkimuksessa käytetty tutkimusaineisto. Sukupuoli-, koulutus-, ikä, tai työtehtävätietoja ei tässä tutkimuksessa otettu mukaan analyysiin. Ensimmäisessä kyselyssä tietoja kysyttiin mutta ne pudotettiin aineistoa koodatessa pois, sillä niillä ei katsottu olevan merkitystä tutkimuksen kannalta. Ensimmäiseen kyselyyn vastanneita oli 142, mikä on noin 20 prosenttia henkilökunnasta. Kysely suoritettiin pelastuslaitoksen isäntäkunnan koko henkilökunnalle.

Tietoturvakoulutus annettiin pelastuslaitoksen henkilökunnalle ja siihen osallistui 46 % henkilökunnasta. Koulutusprosessin hitaudesta johtuen tähän tutkimukseen ei koko pelastuslaitoksen henkilökuntaa ehditty kouluttaa. Se vaikuttaa jonkin verran tämän opinnäytetyön tulosten luotettavuuteen, sillä pienen aineiston takia tulokset ovat vain suuntaa antavia. Kyselylomakkeet jaettiin kaikille koulutukseen osallistuneille, joista 31 eli n. 70 % vastasi.

Tässä tutkimuksessa suoritettiin ennen koulutusta kysely Suomen 22 pelastuslaitokselle. Kyselyn tarkoituksena oli saada tutkimukseen tausta-aineistoa mahdollisesti toteutetusta tietoturvakoulutuksesta pelastuslaitoksissa. Ennen kyselylomakkeiden lähettämistä suoritettiin soittokierros, jolloin yhdeksästätoista pelastuslaitoksesta tavoitettiin vastuhenkilö. Heistä kaikki suostuivat kyselyyn. Koska kyselyn päätarkoitus oli selvittää onko vastaavaa tutkimusta tai koulutusta tehty pelastuslaitoksissa ja miten tietohallinto laitoksissa oli järjestetty, niin tässä yhteydessä käsitellään tuloksia vain niiltä osin. Vastauksia tuli määräaikaan mennessä kuusitoista, eli 72,7 % kaikista pelastuslaitoksista ja 84.2 % tavoitetuista vastasi kyselyyn.

5.1 Käytetyt analyysimenetelmät

Oikein valittu data-analyysi on tärkeä tutkimusprojektin onnistumisen ja mittareiden luotettavuuden arvioinnin kannalta. Tutkimuksen alusta alkaen edessä oleva tutkimusaineiston analysointi kannattaa ottaa huomioon. Tutkimusprosessiin kuuluva datan analysointi saattaa vaatia etukäteisperehtymistä analysointitekniikoihin, tai analysoinnissa vaadittaviin työkaluihin. Tutkittavan aihealueen tutkimuskysymyksiä ei saa sovittaa analysointitekniikoihin sopiviksi tutkimusaineiston analysoinnin helpottamiseksi, vaan analysointitekniikan valinnan on perustuttava tutkimusongelman ja tutkimusmetodin kannalta tarkoituksenmukaisiin syihin (Brewerton ja Millard, 2001). Tässä tutkimuksessa aineiston analyysimetodien valintaan vaikuttivat työn kvantitatiivinen luonne ja tutkimuskysymykset. Analysointimeteodeista valittiin yleisen käytännön mukaisesti siten se, joka parhaiten toi vastauksia tutkimustehtävään (Hirsjärvi et al., 1997).

Tutkimuksen onnistumisen edellytys on oikeanlaisen tiedon löytyminen tutkimuskysymysten ratkaisemiseksi sekä se, että tiedonkeruun metodi soveltuu tutkimuksen tavoitteisiin. Käytännössä tiedonkeruun metodin valinta on iteratiivinen prosessi. Siihen vaikuttavat tutkimuksen aikataulu ja tutkimukseen käytettävien resurssien määrä, sekä metodin käyttökelpoisuus tutkimusongelmaa ajatellen (Brewerton ja Millard, 2001).

5.1.1 SEM-mallinnus ja PLS

Rakenneyhtälömallinnus (*Structural Equation Modeling, SEM*) on menetelmä, joka mahdollistaa monimutkaisten, yhden tai useamman riippumattoman muuttujan (*independent variable*) ja riippuvan muuttujan (*dependent variable*) välisten suhteiden tutkimisen. Muuttujat voivat olla faktoreita tai mitattuja muuttujia. SEM-mallinnuksesta käytetään sovellusalasta riippuen erilaisia nimityksiä kuten esimerkiksi kausaalinen mallinnus, polkuanalyysi, LISREL-mallinnus tai konfirmatorinen faktorianalyysi (*CFA*) (Metsämuuronen, 2002).

SEM-analyysi on yleensä tarkoitettu tilanteisiin, joissa tutkijalla on olemassa teoria muuttujien yhteyksistä toisiinsa. Tarkoituksena on siis aineiston avulla tutkia, saako teoria tukea. SEM-analyysin peruskysymys on siinä, saadaanko teoreettisen mallin perusteella sellainen kovarianssimatriisi, joka on yhtenevä aineiston perusteella havaitun kovarianssimatriisin kanssa (Metsämuuronen, 2002). Edellä mainittu koskee nimenomaan kovarianssipohjaista SEM-mallinnusta, josta esimerkkinä mainittakoon LISREL.

SEM-mallit yhdistävät faktorianalyysin, monen muuttujan regressioanalyysin (*multiple regression*) ja kovarianssianalyysin. SEM-mallit pystyvät myös käsittelemään monen muuttujan tai faktorin lineaarista riippuvuutta (*multicollinearity*) selitettävään muuttu-jaan (Metsämuuronen, 2002).

SEM-analyysi alkoi kehittyä 1960-luvun loppupuolella Karl Jöreskogin myötä. Tosin jo aiemmin polkuanalyysin ideaa kehitti Sewall Wright, joka julkaisi polkumallin jo vuonna 1918 (Bollen, 1989). 1970-luvun alussa Järeskog kehitti kovarianssipohjaisen LISREL-mallinnuksen, joka mahdollisti faktoreiden regressio-, polku- ja moniyhtälöesitykset (Bollen, 1989). Myös muita ohjelmia kehiteltiin, kuten esimerkiksi EQS ja AMOS (Metsämuuronen, 2002). 1970-luvun alussa Herman Wold kehitti regressiopohjaisen PLS-menetelmän (*Partial Least Square*) (Chin, 2005).

Oleellisimmat erot esimerkiksi kovarianssipohjaisen LISREL:in ja regressiopohjaisen PLS:n välillä ovat siinä, että LISREL on herkkä multikolleneiarisuudelle, jota taas PLS ei ole (poikkeuksena formatiiviset muuttujat). LISREL edellyttää vahvaa taustateoriaa, PLS on tässä suhteessa joustavampi. Yleensä LISREL edellyttää myös, että indikaattorit ovat reflektiivisiä, PLS-menetelmää taas voidaan käyttää sekä reflektiivisten että formatiivisten indikaattoreiden mallinnuksessa. LISREL myös edellyttää suurta havaintomäärää (>200), PLS-menetelmää voidaan käyttää huomattavasti pienemmällä havaintoaineistolla (Chin, 2005). ”*The results show that the PLS approach can provide information about the appropriateness of indicators at sample size as low as 20*” (Chin ja Newstead, 1999). LISREL-mallinnuksessa malli joudutaan indentifioimaan (Metsämuuronen, 2002), PLS-menetelmässä malli on aina indentifioituva (Chin, 2005).

Tässä tutkimuksessa PLS-menetelmää on käytetty yksittäisten ja latenttien muuttujien välisten yhteyksien tarkastelussa. SEM-mallinnuksen kohdalla tutkimuksessa käytettyjen mittareiden indikaattorit (yksittäiset muuttujat) on luokiteltu formatiivisiksi muuttujiksi. Toisin sanoen latentin muuttujan indikaattorit selittävät ilmiötä, päinvastoin kuin faktorirakenteessa. Tämä tarkoittaa myös sitä, että latentin muuttujan indikaattoreilla ei välttämättä ole sellaista keskinäistä riippuvuutta, että voitaisiin olettaa jonkin muuttujan vaihtelun johtavan myös muiden mittarin muuttujien vastaavaan vaihteluun. Formatii- visten muuttujien käyttö ei edellytä korrelaatiota muuttujien välillä. ”*Can have positive,*

negative or no correlation with one another” (Bollen ja Lennox, 1991, s. 307). Toisin kuin reflektiivisten muuttujien kohdalla, multikolleneisuus on ongelma formatiivisten muuttujien kohdalla (Jarvis et al., 2003). Tosin aineistossa tätä ongelmaa ei havaittu. Formatiiivisten mittareiden reliabiliteetin estimoinnissa ei voida käyttää perinteisiä menetelmiä (faktorilataukset ja reliabiliteettikerroin), vaan sisäistä konsistenssia tarkastellaan latenttien muuttujien indikaattoreiden sisäisellä painoarvolla (*inner weight*) ja niiden tilastollisella merkittävyydellä (mm. Jarvis et al., 2003).

5.1.2 Korrelaatioanalyysi

Muuttujien välisiä yhteyksiä tutkitaan tavallisesti korrelaatioanalyysin avulla. Useimmiten käytetty on Pearsonin tulomomenttikorrelaatiokerroin r (*Pearson's Product-Moment Correlation Coefficient*), jota yleisesti nimitetään vain korrelaatioksi (Heikkilä 2001; Metsämuuronen, 2002). Tämä vaatii vähintään välimatka-asteikollisen tasoiset muuttujat. Jos muuttujat ovat järjestysasteikollisia, voidaan käyttää Spearmanin tai Kendallin järjestyskorrelaatiokerrointa. Korrelaatiokertoimet vaihtelevat välillä -1 - $+1$ (Heikkilä, 2001).

Korrelaatiokertoimet esitetään yleensä korrelaatiomatriisina, jossa esitetään kaikkien tarkasteltavien muuttujien pareittain lasketut korrelaatiokertoimet. Korrelaatioanalyysin tuloksia voidaan käyttää pohjana jatkoanalyysille, kuten esimerkiksi pääkomponentti-, faktori- ja regressioanalyysille. Korrelaatiomatriisissa ei ole tietoa muuttujien arvoista vaan pelkästään niiden keskinäisistä riippuvuuksista (Metsämuuronen, 2002).

Selitysaste eli selityskerroin ilmoittaa, kuinka suuren osan selittävä muuttuja selittää selitettävän muuttujan vaihtelusta. Selitysaste saadaan korottamalla korrelaatiokerroin toiseen potenssiin. Korrelaatiokertoimen tilastollinen merkitsevyys voidaan testata. Nollahypoteesina on, että muuttujien välillä ei ole riippuvuutta. Jos korrelaatiokerrointa vastaava p :n arvo (*significance*) alittaa käytettävän merkitsevyystason, voidaan tarkastella myös korrelaation voimakkuutta ja suuntaa. On myös huomattava, että korrelaatio ei vielä ole todiste muuttujien välisestä kausaalisuhteesta (syy \rightarrow seuraus) (Heikkilä, 2001). Tässä tutkimuksessa korrelaatioanalyysissä käytettiin Spearman'in järjestyskorrelaatiokerrointa, koska kyseessä on järjestysasteikolliset muuttujat.

5.2 Suoritettujen kyselyjen vastausten analysointi

Tässä luvussa esitellään tämä tutkimuksen tuloksia. Kysymykset, sekä kyselylomakkeen kysymyskohtaiset keskiarvot ja hajonnat on esitetty ensimmäisen kyselyn osalta liitteessä B.. Toisen kyselyn tulokset löytyvät liitteestä C.. Pelastuslaitoksille osoitetun kyselyn tuloksia esitellään ensiksi heti tämän luvun alussa.

Pelastuslaitosten tietohallinnosta vastaavien keskuudessa tehdyn kyselyn perusteella selvitettiin esimerkiksi sitä, kokivatko vastaajat pelastuslaitoksen poikkeavan muusta kuntaorganisaatiosta tietoturvan suhteen (taulukko 2, s. 42). Tärkein syy kyselyyn oli kuitenkin se, että saataisiin selville, oliko vastaavaa tutkimusta tehty missään toisessa suomalaisessa pelastuslaitoksessa. Tätä kysyttiin pelastuslaitosten tietohallinnon parissa työskenteleviltä soittokierroksen yhteydessä, jossa kartoitettiin halukkuus kyselyyn osallistumiseen.

Taulukko 2. Tietoturvan suhteen pelastuslaitos poikkeaa muusta kunnallisesta organisaatiosta ($n= 16$).

Vastausvaihtoehto	Vastausten määrä	%	Kumulatiivinen - %
Täysin samaa mieltä	4	25,0	25,0
Jokseenkin samaa mieltä	6	37,5	62,5
Ei samaa eikä eri mieltä	1	6,3	68,8
Jokseenkin eri mieltä	5	31,3	100,0
Täysin eri mieltä	0	0	
	Yhteensä	16	100,0

Yllä olevassa taulukossa on esitelty saatujen vastausten % -jakaumat eri kysymysten mukaan. Puolet vastaajista oli sitä mieltä, että pelastuslaitokset poikkesivat muusta kunnallisesta organisaatiosta.

Pelastuslaitoksissa on myös otettu entistä enemmän käyttöön tietotekniikkaa. Erilaiset johtamisovellukset ovat tavallisia useimmissa pelastusyksiköissä. Tämä tuo henkilökunnan lisää vaatimuksia tietoturvan hallinnan suhteen (taulukko 3).

Taulukko 3. Tietoturvaosaamista vaaditaan pelastuslaitosten henkilökunnalta nykyään enemmän kuin ennen ($n= 16$).

Vastausvaihtoehto	Vastausten määrä	%	Kumulatiivinen- %
Täysin samaa mieltä	10	62,5	62,5
Jokseenkin samaa mieltä	4	25,0	87,5
Ei samaa eikä eri mieltä	2	12,5	100,0
Jokseenkin eri mieltä	0	0	
Täysin eri mieltä	0	0	
	Yhteensä	16	100,0

Taulukosta käy ilmi, että pelastuslaitosten tietohallinnossa työskentelevistä enemmistö (87,5 %) oli sitä mieltä että tietoturva tuo lisähaasteita henkilökunnalle. Tulos on ymmärrettävä, sillä esimerkiksi vuodesta 1999 vuoteen 2003 tietoturvaloukkaukset organisaatioita kohtaan olivat kasvaneet huomattavasti (Pahnila et al., 2007).

Kyselyssä kartoitettiin myös henkilökunnan tietoturvaosaamisen tasoa ja koulutuksen riittävyyttä. Näihin kysymyksiin vastattiin luottamuksellisesti, joten niitä ei tässä ana-

lyysissä käsitellä. Sen sijaan käsitys pelastusalan ulkopuolelta tulevan kouluttajan kyvystä ottaa huomioon pelastusalan erityispiirteet jakoi mielipiteitä (Taulukko 4).

Taulukko 4. Ulkopuolinen tietoturvakoulutus kykenee ottamaan huomioon pelastusalan erityispiirteet ($n= 16$).

Vastausvaihtoehto	Vastausten määrä	%	Kumulatiivinen %
Täysin samaa mieltä	0	0	0
Jokseenkin samaa mieltä	2	12,5	12,5
Ei samaa eikä eri mieltä	8	50,0	62,5
Jokseenkin eri mieltä	6	37,5	100,0
Täysin eri mieltä	0	0	
Yhteensä	16	100,0	

Kysymys jakoi vastaajien mielipiteet ja puolella vastaajista ei ollut asiaan mielipidettä. Kuitenkin yli kolmannes vastaajista (37,5 %) epäili alan ulkopuolelta saadun tietoturvakoulutuksen kykyä huomioida alan erityispiirteet. Pelastuslaitoksille osoitetun kyselyn tulokset vahvistivat käsitystä, että tällaiselle koulutusta ja sen vaikutusta arvioivalle tutkimukselle on tarvetta.

Ennen koulutusta pelastuslaitoksen henkilökunnalle suunnatun kyselyn tarkoitus oli selvittää, koulutettavien suhtautuminen tietoturvaan, sekä se minkälainen tietotaso vastaajilla oli tietoturvakysymyksistä. Kysymyssarja oli kaksiosainen, jonka toisen osion pääasiallisena tarkoituksena oli toimia koulutuksen suunnittelun apuna. Kysymyssarjan ensimmäisen osion vastausten pohjalta tehdyn analyysin perusteella tutkittiin, minkälainen oli vastaajien aikomus tietoturvaohjeiden noudattamista kohtaan ennen koulutusta ja mitkä muuttajat aikomukseen vaikuttivat.

Koulutuksen jälkeen suoritetussa kyselyssä ei selvitetty olivatko vastaajien tiedot parantuneet ensimmäisessä kyselyssä kysytyjen asioiden suhteen. Tähän oli kaksi syytä. Ensiksikin kysymyksillä olisi heti koulutuksen jälkeen mitattu lähinnä vastaajien muistamista käsitellyistä asioista ja toiseksi tuloksilla ei olisi merkitystä tutkimuskysymysten kannalta. Analyysissä käytetyn kyselyjen - ja SEM-mallin tulosten perusteella tutkittiin, kuinka vastaajat kokivat koulutuksen ja aikoivatko he noudattaa tietoturvaohjeita. Toisessa koulutuksen jälkeen suoritetussa kyselyssä oli kuitenkin yksi kysymys, jolla haluttiin testata koulutuksen tehoa myös käytännön tasolla. Ensimmäisen kyselyn perusteella kolmasosa vastaajista oli antanut päivittäin tai joskus tunnuksensa toisten käyttöön. Koulutuksen jälkeen suoritetussa kyselyssä vastaajia pyydettiin ottamaan kantaa väittämään; ”käyttäjätunnukset ovat henkilökohtaisia”. Kun ennen koulutusta vastaajilla oli puutteita salasanojen ja käyttäjätunnusten salassa pitämisen suhteen, niin toisessa kyselyssä 96,7 % vastaajista oli sen sijaan täysin (93,5 %) tai osittain (3,2 %) sitä mieltä, että käyttäjätunnukset ovat henkilökohtaisia. Tämän perusteella voidaan olettaa, että käytännön työssäkin koulutus tulee näkymään positiivisesti.

5.3 Formatiivisen SEM-mallinnuksen tulokset

Tässä alaluvussa analysoidaan, minkälaisia riippuvuuksia kyselyiden vastausten perusteella muodostettujen summamuuttujien välillä vallitsee. Näin voidaan arvioida sitä, minkälainen vaikutus kullakin muuttujalla suoraan tai välillisesti tietoturvaohjeiden noudattamisen aikomusta kohtaan on. Toiminnan perustuessa vapaaehtoisuuteen ihmisten käyttäytymistä on mahdollista ennustaa varsin täsmällisesti toimintaan kohdistuvan aikomuksen perusteella (Ajzen 2005; Davis ja Venkatesh, 1996).

Kuvissa 8 ja 9 sivuilla 48 ja 50 näkyy SEM-mallin tulokset, jotka kertovat, missä määrin muuttujat, jotka perustuvat kyselylomakkeen kysymyksiin selittävät vastaajien aikomusta noudattaa tietoturvaohjeita. Tämän tutkimuksen tutkimuskirjallisuudessa TPB ja TAM- malli, tai niiden johdannaiset, ovat olleet useassa analysointimenetelmänä kun on haluttu ennustaa, tai selvittää yksilön toimintaa, tai toiminnan aikomusta (kts Taulukko 2, sivu 32). Tämä johtuu siitä, että tietoturvatutkimusta tekevät ovat kokeneet ne päteviksi malleiksi (Siponen, 2000; Rawstone et al., 2000). Niiden etuna tämän tutkimuksen kontekstissa oli niiden muunneltavuus. Varsinkin TPB sallii vaihtoehtoisten muuttujien käytön mallissa (Ainsworth, 2006). Tämän perusteella tässä tutkimuksessa sen ensimmäisten kysymysten analysoinnin tulkintakehyksenä käytettyyn TPB:stä johdettuun malliin voitiin lisätä asennetta selittäviä muuttujia, sekä toista kysymyspatteria varten voitiin rakentaa kombinaatio TPB:stä ja TAM-mallista. Analysointimenetelmänä on tarkoituksen mukaista käyttää sellaista, joka parhaiten tuo vastauksia tutkimustehtävään (Hirsjärvi et al., 1997).

Tämän tutkimuksen tutkimusongelmina ovat tietoturvakoulutuksen teho ja koulutuksen hyödyllisyyden kokeminen. Tietoturvakoulutuksen yksi tehon mittari on se, kuinka koulutuksen jälkeen vastaajat suhtautuvat tietoturvaohjeiden noudattamiseen verrattuna siihen miten he kokivat asian ennen koulutusta. Tässä tutkimuksessa tietoturvaohjeiden noudattamisen havainnointia ei suoritettu. Sen sijaan vastaajilta kysyttiin aikomusta tietoturvaohjeiden noudattamiseen. TPB:ta on käytetty tutkimuksissa selvittämään aikomuksen ja toteutuneen toiminnan välistä ennustettavuutta, jolloin on havaittu, että aikomus ennustaa toimintaan ryhtymistä. Vahva aikomus ennustaa paremmin toimintaa, kuin heikko aikomus toiminnan puutetta (Grano ja Prislin, 2006).

Vaikka TAM-malli onkin yksi eniten käytetty teoreettinen pohja informaatioteknologian tuotteiden omaksumiselle ja käytölle, voidaan sitä hyödyntää myös muiden informaatioteknologian osa-alueiden, tässä tapauksessa tietoturvaohjeiden, käyttöön oton ennustamiseen (Lee et al., 2005). Tämän perusteella aiemmin esitellyt ja analyysissä käytetyt mallit soveltuivat hyvin tämän tutkimuksen tutkimusongelmien ratkaisun välineiksi. Analyysin perusteella voidaan päätellä, että tulokset koulutuksen tehosta ovat yhtäpitäviä vastaavien tutkimusten kanssa (taulukko 5).

Taulukko 5. Koulutuksen vaikutus tietoturvaohjeiden noudattamiseen tutkimuksessa käytettyjen lähteiden mukaan.

Lähde	Koulutuksen vaikutus tietoturvaohjeiden noudattamiseen
D'Arcy ja Hovav (2007)	Positiivinen
Dark ja Winstead (2005)	Positiivinen
Kesar ja Rogerson (1997)	Positiivinen
Lee ja Lee (2002)	Positiivinen
Pahnila et al. (2007)	Positiivinen
Puhakainen (2006)	Positiivinen
Siponen (2000)	Positiivinen
Solms (1999)	Positiivinen
Torres et. al. (2006)	Positiivinen

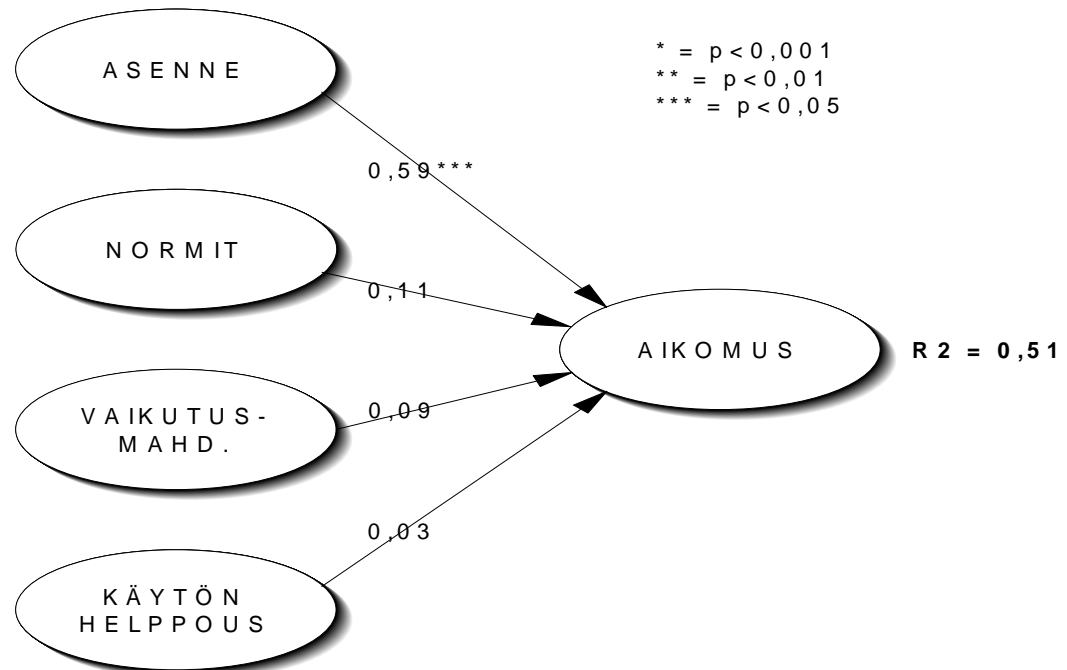
Yllä olevassa taulukossa on esitelty joidenkin tämän tutkimuksessa käytettyjen lähteiden tutkimustuloksia, tai mielipiteitä siitä mitä vaikutuksia koulutuksella on tietoturvaohjeiden noudattamiseen.

Vastaajien asenteiden, normien, vaikutusmahdollisuuksien sekä käytön helppouden samanaikaisia vaikutuksia tietoturvaohjeiden ja sääntöjen noudattamisen aikomusarvioihin tutkittiin rakenneyhtälömallinnuksen (*Structural Equation Modeling*, SEM) avulla. Mallinnus perustuu TPB-teoriaan ja TAM-malliin (kts. kuvat 4 ja 5, s. 30). Mallissa ympyrä-symbolit kuvaavat latentteja muuttujia, nuolet vaikutuksen suuntaa ja R² selitystasetta, beta-kertoimet vaikutuksen voimakkuutta ja beta-arvojen perässä olevat tähdet (*) vaikutuksen tilastollista merkitsevyyttä. Rakenneyhtälömallinnus tehtiin PLS Graph – ohjelmistolla.

Latentit muuttujat on rakenneyhtälömallinnuksessa määritelty formatiivisiksi⁶, ja latenttien muuttujien yksittäisten indikaattoreiden vaikutusta tarkastellaan niiden sisäisen painoarvon (*inner weight*) ja sen tilastollisen merkitsevyyden perusteella. Mallin tilastollisesti merkittäviä yhteyksiä estimoitii (*Bootstrap resampling*, samples = 500, iterations = 500) formatiivisten muuttujien painoarvon ja niiden tilastollisen merkittävyyden (t-jakauma, *t-statistic*) avulla. T-jakauman arvojen perusteella laskettiin tulosten p-arvot (*significance*). Laskennassa käytettiin Excel-funktiota TDIST (x; deg_freedom; tails).

⁶ Tarkoittaa sitä, että latentin muuttujan indikaattoreiden ei oleteta korreloivan keskenään.

Latenttien muuttujien yksittäisten indikaattoreiden sisäiset painoarvot esitetään liitteessä F. Seuraavalla sivulla kuvassa 7 esitetään SEM-mallin tulokset ennen koulutusta.

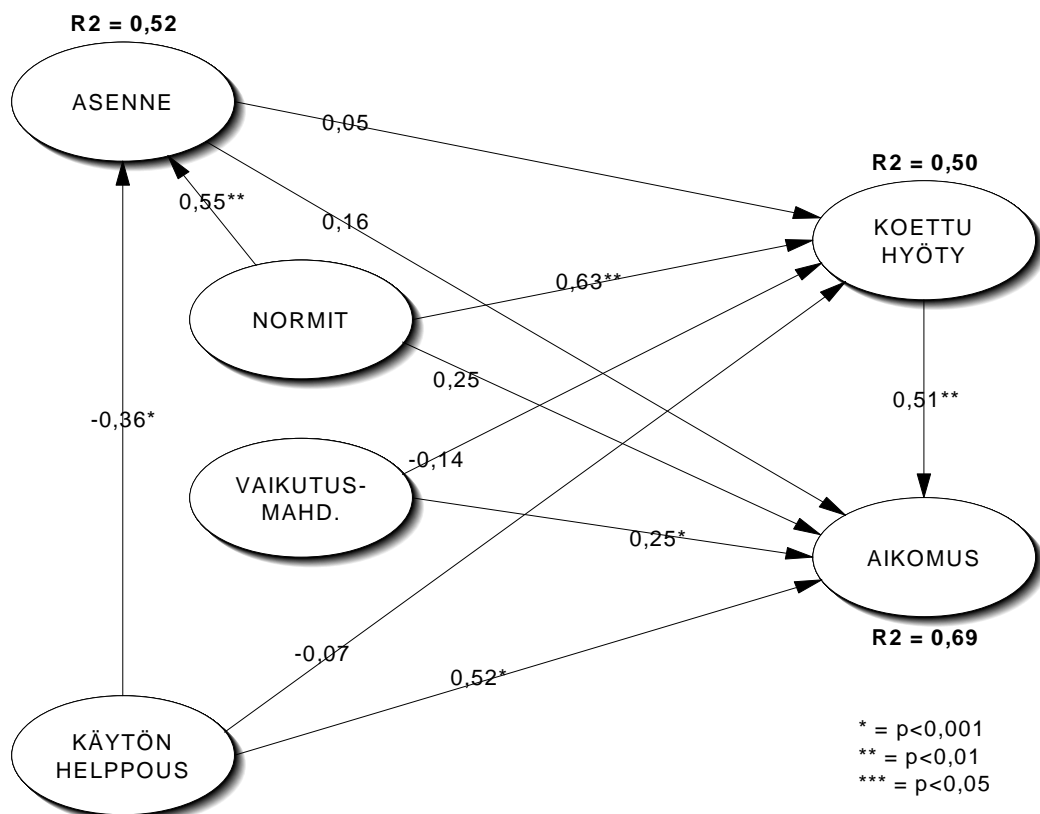


Kuva 7. Formatiivinen SEM-malli – tulokset ennen koulutusta.

Tulokset osoittavat, että vastaajan asennetekijät, subjektiiviset normit, vaikutusmahdollisuudet ja käytön helppous selittävät 51 % vastaajien aikomusarvioiden vaihtelusta, kun tilannetta tarkastellaan ennen tietoturvakoulutusta. Tilastollisesti merkitsevä vaikutus ($p < 0,001$) on pelkästään vastaajan asennetekijöillä. Tämä selittyy sillä, että ennen koulutusta vastaajilla oli vähän, jos ollenkaan tietoa organisaation tietoturvaohjeista. Vastaajilla ei siten voinut olla TPB:n muuttujien taustalla olevia selkeitä uskomuksia tietoturvaohjeista. Tämän vuoksi vastaajien on täytynyt muodostaa mielipiteensä jonkin muun tekijän perusteella. Ennen koulutusta tehdyn kyselyn vastausten analyysin kehyksenä käytetty malli ottaa huomioon vaihtoehtoiseen muuttujan vaikutuksen TPB-mallissa (kts. kuva 9). Vahva organisaatioanaalinen sitoutumisen aste toimii selityksenä voimakkaalle asenteen kautta ilmenevälle aikomukselle tietoturvaohjeiden noudattamiseen (Lee ja Lee, 2005; Ainsworth, 2006). Pelastuslaitoksen henkilökunnan keskuudessa vuonna 2005 suoritetun työilmapiiriä kartoittavan työtyytyväisyyskyselyn perusteella henkilökunta on työhönsä tyytyväisiä, mikä on edellytys sille, että työntekijä sitoutuu työnantajaan (Ahuja et al., 2002).

Positiivinen regressiokerroin ($\beta = 0,59***$) osoittaa, että asenteiden muuttuessa positiivisemmiksi aikomus noudattaa tietoturvaohjeita kasvaa tilastollisesti erittäin merkittävästi ($p < 0,001$). Asennetekijöistä merkittävin vaikutus on muuttujalla ”koen tietoturvaohjeiden noudattamisen miellyttävänä”. Muilla asenne-muuttujan indikaattoreilla (kts. liite F, taulukko 1) ei ole tilastollisesti merkitsevää vaikutusta vastaajien aikomusarvoihin. Huomion arvoista tuloksissa on myös se, että asennetekijöistä rangaistusten pelolla ei ole merkittävää vaikutusta tietoturvaohjeiden noudattamisen aikomuksiin ennen

koulutusta (kts. liite F, taulukko 1). Tulos ei ole kuitenkaan yllättävä, sillä rangaistuksen vaikuttavuudesta aikomukseen on aiemmissa tutkimuksissa saatu samansuuntaisia tuloksia silloin, kun rangaistuksia ei ole viety käytäntöön tai niillä ei ole todellista pelotevaikutusta. Samoin työntekijöille on ilmoitettava mahdolliset sanktiot ja niiden seuraukset ja heille on raportoitava toteutetuista rangaistustoimista, jotta sanktioilla olisi vaikutusta yksilön päätöksiin noudattaa ohjeita (D'Arcy ja Hovav, 2007 vrt. Lee ja Lee, 2002, Folz ja Jones, 2005, Siponen 2007; McNamara et al., 2003). Tämä perustuu yleisen peloteorian (*General Deterrence Theory, GDT*) mukaan siihen, että yksilöllä on taipumus maksimoida hyödyt ja minimoida haitat (Lee et al., 2005). Seuraavassa kuvassa 8 esitetään SEM-malli, jossa tilannetta tarkastellaan toteutetun koulutuksen jälkeen.



Kuva 8. Formatiivinen SEM-malli – tulokset koulutuksen jälkeen.

Asenne

Mielenkiintoinen tulos on se, että vaikka työntekijöiden asenteet tietoturvaa kohtaan muuttuisivatkin positiivisemmiksi, ei asennetekijöillä kuitenkaan ole enää koulutuksen jälkeen merkittävästi vaikutusta yksilön aikomuksiin noudattaa organisaation tietoturvaohjeita ja sääntöjä. Mahdollinen selitys asenne-muuttujan staattisuuteen on se, että koulutuksen jälkeen tehdyn kyselyn perusteella tilastollisesti merkitseviä aikomusta selittäviä muuttujia on useampia. Koulutuksen jälkeen vastaajilla on enemmän tietoa tietoturvaohjeiden sisällöstä ja tietoturvalainlyöntien mahdollisista vaikutuksista yksilöön ja koko organisaatioon. Tulosta asenteiden osalta saattaa selittää myös se, että

koulutuksen koettu hyöty suuntautuu koulutuksen jälkeen jossain määrin enemmän yksilötasolle kuin organisaatiotasolle. Asennetekijöistä merkittävin vaikutus on muuttujalla ”ohjeiden noudattaminen on järkevää” (kts. liite F, taulukko 2).

Asenteiden taustalla olevilla uskomuksilla (*behavioral beliefs*) on tutkimusten mukaan vahva merkitys ennustettaessa aikomusta, toisin kuin normeilla. (Ajzen, 2005). Tämän suuntaiseen tulokseen päädyttiin myös SEM mallin tuloksissa, joiden perusteella voitiin päätellä, että kuta tärkeämpänä vastaajat olettavat pelastuslaitoksen johdon pitävän tietoturvakoulutusta, sitä suurempi positiivinen vaikutus edellä mainituilla tekijöillä on nimenomaan vastaajien tietoturva-asenteisiin (kts. kuva 8, s. 47). Jos ihminen uskoo johonkin, hän ei ainoastaan kannata asiaa, vaan on myös motivoitunut toimimaan uskomustensa mukaisesti (Layton, 2005).

Käytön helppous

Tulokset osoittavat, että tietoturvaohjeiden käytön helppous ja subjektiiviset normit selittävät tilastollisesti merkitsevästi ($p < 0,01$) 52 % vastaajien asennetekijöiden vaihtelusta. Latentin muuttujan ”Käytön helppous” indikaattoreista merkittävin sisäinen painoarvo (*inner weight*) on muuttujalla ”ohjeet ovat helposti ymmärrettävissä” ja ”Normit”-muuttujan indikaattoreista muuttujalla ”pelastuslaitoksen johto pitää koulutusta tärkeänä” ja muuttujalla ”ohjeiden noudattamista jättämisestä voidaan rangaista” (kts. liite F, taulukko 2). Käytön helppouden negatiivinen regressiokerroin ($\beta = -0,36^*$) ja muuttujan ”ohjeita on helppo noudattaa” negatiivinen sisäinen painoarvo (kts. liite F, taulukko 2) viittaavat siihen, että parantamalla ohjeiden noudatettavuutta vaikutetaan positiivisesti siihen, että ohjeita on järkevä noudattaa. Siponen (2000) väittää, että jos ihmisille esitetään kelvolliset argumentit ja he kokevat ohjeiden noudattamisen oikeana, se vaikuttaa positiivisesti aikomukseen noudattaa ohjeita.

Mielenkiintoinen tulos on myös se, että ohjeiden helpon noudattamisen ja helpon ymmärrettävyyden välinen korrelaatio on erittäin vähäinen ($r = 0,003$). Tämä on jossain määrin yllättävää, mutta saattaa merkitä sitä, että tietoturvaohjeiden sisältöön ei sittenkään kyselyn jälkeen ole tutustuttu, vaan mielikuva sisällöstä muodostettiin ainoastaan koulutuksen perusteella, sillä usein ihmiset muodostavat käsityksensä ohjeista lukematta niitä (Foltz ja Jones 2005). Toisaalta selityksenä saattaa olla se, että halutaan noudattaa sääntöjä koska ymmärretään sen palvelevan organisaation etua. Käyttäytyminen on monin tavoin sidoksissa sosiaaliseen prosessiin ja yhteisöön. Tämä tapahtuu sosiaalisen älykkyyden avulla, joka pitää sisällään kriittisen ymmärryksen, jonka avulla yksilöllä on kyky nähdä ja ymmärtää sosiaalisia uskomuksia. Sosiaalinen älykkyys mahdollistaa yksilöä tunnistamaan sosiaalisesti oikean käyttäytymisen ja toimimaan yhteisen hyvän eteen (Dark ja Winstead, 2005).

Subjektiiviset normit

Muuttujan ”normit” positiivinen regressiokerroin ($\beta = 0,55^{**}$) osoittaa, että kuta ymmärrettävämpiä ohjeet ovat ja kuta tärkeämpänä pelastuslaitoksen johto pitää tietoturvakoulutusta, sitä suurempi positiivinen vaikutus edellä mainituilla tekijöillä on vastaajien tietoturva-asenteisiin. ”Normit”-muuttujan indikaattoreista myös muuttujan ”ohjeiden noudattamatta jättämisestä voidaan rangaista” sisäinen painoarvo on tilastollisesti merkitsevä, joka osoittaa, että rangaistuksen pelolla on merkittävää vaikutusta henkilöstön tietoturva-asenteisiin, kuten useissa tutkimuksissa on todettu (vrt. Crano ja Prislin

2006; D'Arcy ja Hovav 2007; Folz ja Jones 2005; Lee ja Lee 2002; McNamara et al., 2003; Pahlila et al., 2007; Puhakainen 2006, sekä Siponen, 2000).

Mielenkiintoista SEM-mallien tuloksissa on myös se, että organisaation normeilla ei ole merkittävää vaikutusta aikomuksiin noudattaa organisaation tietoturvaohjeita ja sääntöjä. Tämä saattaa vaikuttaa yllättävältä, mutta Crano ja Prislin (2006) väittävät, että subjektiiviset normit, joihin uskomustasolla (*normative beliefs*) organisaation normit yhtenä taustamuuttujana vaikuttavat, ovat TPB:n peruselementeistä heikoiten toimintaa ennustava muuttuja. Yksilölle tärkeät ihmiset, ryhmät tai organisaatiot kuitenkin vaikuttavat aikomukseen toimintaa kohtaan, mutta ei suoraan aikomukseen, vaan välillisesti asenteiden kautta (Crano ja Prislin, 2006).

Koettu hyöty

Tulosten mukaan vastaajan asennetekijät, normit, vaikutusmahdollisuudet, käytön helppous, sekä koettu tietoturvakoulutuksen hyöty selittävät 69 % vastaajien aikomusarvioiden vaihtelusta, kun tilannetta tarkastellaan toteutetun tietoturvakoulutuksen jälkeen. Tilastollisesti merkitsevä vaikutus on koulutuksen koetulla hyödyllä ($p < 0,01$), normeilla ($p < 0,01$) sekä tietoturvaohjeiden käytön helppoudella ($p < 0,05$). Käytön helppouden osalta positiivinen regressiokerroin ($\beta = 0,52^*$) osoittaa, että lisäämällä ohjeiden ymmärrettävyyttä ja ohjeiden helpolla noudatettavuudella voidaan merkittävästi vaikuttaa henkilöstön aikomuksiin noudattaa tietoturvaohjeita ja sääntöjä. Sen sijaan ohjeiden helpolla saatavuudella ja niiden noudattamisella on korrelaatioanalyysin tulosten mukaan jonkin verran tilastollisesti merkitsevää keskinäistä yhteyttä ($r = 0,37^*$). Tulos on yhdensuuntainen TAM-mallin kanssa. Mallissa koettu hyödyllisyys ja koettu käytön helppous vaikuttavat käyttöaikomuksiin asenteen kautta. (Davis ja Venkatesh 1996). Pahlila et al. (2007) puolestaan esittää, että tietoturvan näkyvyys vähentää tietojärjestelmän väärinkäyttöä ja lisää käyttäjän aikomusta noudattaa ohjeita. Organisaatioiden tulee parantaa käyttäjien tietämystä tietoturvapoliitikoista ja tehdä niistä helposti saatavia. Tämä parantaa ohjeiden noudattamista (D'Arcy ja Hovav, 2007.)

Asennetekijät, tietoturvaohjeiden käytön helppous, normit ja vaikutusmahdollisuudet selittävät 50 % tietoturvakoulutuksen koetun hyödyn vaihtelusta. Tilastollisesti merkitsevä ($p < 0,01$) vaikutus on ainoastaan normeilla ($\beta = 0,63^*$). ”Normit”-muuttujan indikaattoreista merkittävät painoarvo ovat muuttujilla ”pelastuslaitoksen johto pitää koulutusta tärkeänä” sekä ”ohjeiden noudattamatta jättämisestä voidaan rangaista” (kts. liite F, taulukko 2). Tulos on mielenkiintoinen, koska se osoittaa, että mikäli pelastuslaitoksen johto pitää koulutusta tärkeänä, niin koulutuksen koettu hyöty nähdään suuremmaksi. Tässä yhtenä mahdollisena selityksenä on se, että myös johto on osallistunut koulutukseen, jolloin se heijastuu positiivisena kokemuksena myös muihin koulutukseen osallistuneisiin henkilöihin? Koulutuksen jälkeen suoritetun kyselyn perusteella myös se, että rangaistuksen pelko lisää koulutuksen koettua hyötyä, on mielenkiintoinen, sillä tutkimusten mukaan rangaistuksen pelon tulisi lisätä aikomusta tietoturvallisten toimintatapojen noudattamiseen (Siponen, 2007). Toisaalta havaitaan myös se, että tietoturvakoulutus nousee merkittävimmäksi tekijäksi, kun tarkastellaan vastaajan aikomuksia tietoturvaohjeiden noudattamiseen. Mahdollinen selitys sanktioiden vaikutuksen esiintymiseen muodossa tai toisessa vasta toisen kyselyn tuloksissa voi olla siinä, että sanktioita käsiteltiin koulutuksessa. Yksilöt toimivat rationaalisesti ja arvioivat toimintaan ryhtymistä myös hyödyn ja haitan perusteella (Lee et al., 2005). Ilmeisesti tieto sanktioista koettiin hyödylliseksi kun arvioidaan toiminnan kustannuksia ja tämä lisäsi myös koulutuksen koettua hyötyä. Tietoturvakoulutuksessa kannattaa pitää esillä sanktioiden

mahdollisuutta, sillä niillä on vaikutusta asenteiden kautta aikomukseen. (Siponen, 2000).

Latentin muuttujan ”koettu hyöty” kaikilla sisäisillä indikaattoreilla (muuttujilla) on tilastollisesti merkitsevä sisäinen painoarvo (kts. liite F, taulukko 2). Hieman yllättäen muuttujalla ”työnantaja hyötyy koulutuksesta” on vähäisin, joskin tilastollisesti merkitsevä sisäinen painoarvo (kts. liite F, taulukko 2). Tulos viittaa siihen, että koulutuksen koettu hyöty suuntautuu jossain määrin enemmän yksilötasolle kuin organisaatiotasolle.

Aikomus

Merkittävin vaikutus ($p < 0,01$) aikomuksiin on tietoturvakoulutuksen koetulla hyödyllä ($\beta = 0,51^{**}$). Positiivinen regressiokerroin osoittaa, että kuta hyödyllisemmäksi koulutus koetaan, sitä todennäköisemmin aiotaan noudattaa organisaation tietoturvaohjeita ja sääntöjä.

Tuloksista voidaan siis havaita, että tietoturvakoulutus nousee merkittävimmäksi tekijäksi, kun tarkastellaan vastaajan aikomuksia tietoturvaohjeiden noudattamiseen. Selitysaste (R^2) on suuri (69 %), mutta tässä on huomioitava se, että pienen aineiston takia tulokset ovat vain suuntaa antavia. Tulokset kuitenkin antavat viitteitä siitä, että tietoturvakoulutuksella voidaan merkittävästi vaikuttaa yksilön aikomuksiin noudattaa organisaation tietoturvaohjeita ja sääntöjä. Mutta kysymys on vasta aikomuksista, ei siis siitä, noudattaako yksilö tietoturvaohjeita vai ei. Aikomuksen voimakkuudesta voidaan kuitenkin päätellä kuinka todennäköistä ohjeiden noudattaminen on (Pahnila et al., 2007).

Aiemmissä tutkimuksissa (esim. Grano ja Prislin, 2006) on selvitetty aikomuksen ja toteutuneen toiminnan välistä ennustettavuutta, jolloin on havaittu, että aikomus ennustaa n. 28 prosenttisesti toimintaan ryhtymistä. Toimintaa selittämättömien muuttujien suuri määrä on nähty ongelmaksi. Vahva aikomus ennustaa paremmin toimintaa, kuin heikko aikomus toiminnan puutetta. Vahvaan aikomukseen vaikuttavat nimenomaan asenteet, joihin yksilölle tärkeät ihmiset tai ryhmät myös vahvasti vaikuttava (Kuo ja Hsu, 2001.) On myös syytä pitää mielessä Siposen (2000) väite, että koulutettavat eivät ole halukkaita välittömästi koulutuksen jälkeen noudattamaan ohjeita. Tämä lisää tarvetta tietoturva-asioiden jatkuvaan esillä pitämiseen myös koulutuksen jälkeen, sillä jatkuva, asteittainen tietoturvan parantaminen on tehokkaampaa, kuin yritys saada kerralla kaikki kuntoon (Layton, 2005).

Vaikutusmahdollisuudet

Vaikutusmahdollisuuksien osalta, jossa suurin painoarvo on muuttujalla ”yksittäinen työntekijä voi parantaa tietoturvaa pelastuslaitoksissa”, positiivinen regressiokerroin ($\beta = 0,24^*$) tarkoittaa, että mikäli yksittäinen työntekijä pääsee vaikuttamaan organisaation tietoturvan kehittämiseen, on sillä positiivinen vaikutus työntekijän aikomuksiin noudattaa organisaation tietoturvaohjeita ja sääntöjä. Negatiivinen sisäinen painoarvo (kts. liite F, taulukko 2) puolestaan osoittaa, että henkilöstön vaikutusmahdollisuuksia organisaation tietoturvatyössä tulisi lisätä. Tulosten mukaan myös kehittynyt tietotekniikka edesauttaa henkilöstön aikomuksia noudattaa tietoturvaohjeita ja sääntöjä. Käyttäjät tulisi saada osallistumaan tietoturvatyöhön, eikä heille saisi syntyä tunnetta, että he ovat ulkopuolisia. Käyttäjille täytyisi tehdä selväksi, että tietoturvaongelmat ovat myös heidän ongelmiaan ja että he pystyvät teoillaan vaikuttamaan niihin (McIlwraith, 2006.)

6. Pohdinta ja johtopäätökset

Tutkimuksen tavoitteena oli selvittää pelastuslaitoksessa aloitettuun tietoturvan kehitystyöhön kuuluvan tietoturvakoulutuksen vaikutuksia käyttäjien aikomukseen noudattaa tietoturvaohjeita. Lisäksi ensimmäisenä alatutkimusongelmana selvitettiin sitä, kuinka koulutettavat kokivat tietoturvakoulutuksen. Koulutusmalliksi valittiin Puhakaisen (2006) väitöskirjassa esitelty malli (*The Universal Constructive Instructional Theory, UCIT*). Toisena alatutkimusongelmana oli siten selvittää kyseisen mallin sopivuus ja käyttökelpoisuus pelastuslaitoksen erityispiirteet huomioonottavan koulutuksen järjestämiseen. Tämän tutkimuksen kirjallisuuskatsauksessa selvitettiin sitä, mitä aiempi tutkimus oli saanut selville tutkimuksen kohteena olevista käsitteistä ja kuinka niitä oli tutkittu.

Tutkimusmetodiltaan tutkimus oli kvantitatiivinen, jossa kyselyillä kerättiin tutkimusaineistoa ennen ja jälkeen koulutuksen. Empiirisen tutkimuksen tutkimusmalliksi valittiin kaksi tulkintakehystä, jotka johdettiin suunnitellun toiminnan teoriasta (*The Theory of Planned Behaviour, TPB*) ja teknologian hyväksymismallista (*Technology Acceptance Model, TAM*). Mallissa olevien muuttujien välisiä keskinäisiä suhteita tutkittiin SEM-mallinnuksen ja korrelaatioanalyysin avulla.

Kirjallisuuskatsauksen perusteella erilaisissa toimintaympäristöissä toimivilla organisaatioilla on erilainen organisaatiokulttuuri. Koska tietoturvallisuus on osa organisaatiokulttuuria, niin eri organisaatioilla on myös erilainen tietoturvakulttuuri. Tämä tulisi ottaa huomioon tietoturvakoulutusta suunniteltaessa eri toimintaympäristöissä toimiville organisaatioille. Tämän perusteella kohderyhmän erityispiirteet huomioonottavalle koulutukselle pelastuslaitoksessa oli perusteita. Tietoturvakoulutuksella lisättiin henkilökunnan tietoturvatietoisuutta ja -ymmärrystä siitä, mitä tietojärjestelmän väärinkäytöstä saattaa seurata. Kontrollit, ohjeet ja säännöt ovat tehottomia ilman käyttäjien hyväksyntää ja ymmärrystä. Tehokkaat säännöt ja kontrollit edellyttävät täydellistä käyttäjien tukea läpi koko organisaation.

Organisaation tietoturvallisen toimintaympäristön varmistaminen riippuu monesta tekijästä. Kirjallisuudessa esitettyjen aiempien tutkimustulosten perusteella koulutuksella oli merkittävä vaikutus tietoturvaohjeiden noudattamiseen. Koulutuksen lisäksi tietoturvan hallintajärjestelmällä ja siihen liittyvillä toimilla oli myös vaikutusta käyttäjien aikomukseen noudattaa tietoturvaohjeita.

Teknisten suojaustoimenpiteiden lisäksi ohjeiden laatuun ja saatavuuteen kannattaa kiinnittää huomiota. Myös sanktioilla on merkitystä käyttäjän aikomukseen noudattaa ohjeita, mikä tulisi tutkimusten mukaan huomioida siten, että ohjeiden noudattamatta jättämisen seuraamukset tehtäisiin käyttäjille tunnetuksi. Vaikka sanktioiden vaikutusten arvioiminen ei ole tämän tutkimuksen tutkimuskysymys, todettiin sillä tässä tutkimuksessa olevan koulutuksen vaikutuksen arvioinnin kannalta merkitystä, kuten myös osa tutkimuskirjallisuudesta väittää.

Tämän tutkimuksen tutkimusongelmiin saatiin vastaukset. Tutkimuksen perusteella koulutuksella ja siinä esiin tuoduilla asioilla oli suoraan tai välillisesti positiivinen vai-

kutus vastaajien aikomukseen noudattaa tietoturvaohjeita, mikä on vastaus päätätkimusongelmaan.

Koulutettavat kokivat koulutuksen hyödylliseksi, mikä on vastaus ensimmäiseen alatutkimusongelmaan. Hieman yllättävä huomio tuloksissa oli se, että koulutuksen koettu hyöty suuntautui jossain määrin enemmän yksilötasolle kuin organisaatiotasolle. Toisaalta mikäli yksittäinen työntekijä pääsee vaikuttamaan organisaation tietoturvan kehittämiseen, on sillä positiivinen vaikutus työntekijän aikomuksiin noudattaa organisaation tietoturvaohjeita ja - sääntöjä ja siten positiivinen vaikutus koko organisaatioon. Henkilöstön vaikutusmahdollisuuksia organisaation tietoturvatyössä tulisi siten lisätä.

Aikomus noudattaa tietoturvaohjeita ennustaa todellista ohjeiden noudattamista. Tässä tutkimuksessa saadut tulokset vahvistavat siten Puhakaisen (2006) tutkimuksen tuloksia ja ovat yhdensuuntaisia aiempien tutkimusten kanssa. Tulosten perusteella voidaan siis todeta, että UCIT-mallin mukainen koulutus sopii myös pelastuslaitoksen kaltaisen viranomaisorganisaation koulutusmalliksi, kun ollaan aloittamassa tietoturvan hallintaprosessia. Tämä oli toinen alatutkimusongelmista. Tutkimuskohteena olleen UCIT-mallin kaltainen koulutusmalli on kuitenkin liian monimutkainen ja raskas pysyväksi koulutusmalliksi.

Pelastuslaitoksen johto oli näkyvästi mukana koulutuksen suunnittelussa ja järjestelyissä. Koko pelastuslaitoksen ylin johto osallistui ”rivijäsenenä” koulutukseen, mikä osaltaan viestitti asian tärkeyttä henkilökunnalle. Tulokset osoittavat, että kuta tärkeämpänä pelastuslaitoksen johto pitää tietoturvakoulutusta, sitä suurempi positiivinen vaikutus edellä mainitulla tekijällä on nimenomaan vastaajien tietoturva-asenteisiin. Johdon esimerkillä on siis tärkeä merkitys koulutuksen onnistumiselle, mikä kannattaa huomioida jatkossa myös muissa tärkeissä kehityshankkeissa.

Koulutus on tärkeä osa myös pelastuslaitoksen tietoturvan hallintaprosessia. Itse asiassa se oli ensimmäisiä toimia hallintaprosessin käynnistämisessä tämän tutkimuksen tutkimuskohteena olleessa pelastuslaitoksessa. Kuinka pysyviä koulutuksen vaikutukset ovat, sekä millä tavalla ja missä määrin tässä tutkimuksessa havainnoitu aikomus noudattaa tietoturvaohjeita aktualisoituu tietoturvalliseksi käyttäytymiseksi, ovat jatkotutkimuksen arvoisia aiheita. Mikä osa tietoturvan hallintaprosessin kehittämisestä aiheutuvalla tietoturva-asioiden esillä pitämisellä on tutkimushetken tietoturvatietoisuuden kasvuun, kannattaisi myös jatkossa tarkemmin tutkia.

Tämän tutkimuksen heikkoutena voidaan pitää kyselytutkimusten osalta sitä, että ensimmäisen kyselytutkimuksen kysymykset eivät olleet tätä tutkimusta varten suunniteltuja ja siksi ne eivät kaikin osin olleet käyttökelpoisia tätä tutkimusta silmällä pitäen. Ensimmäisen kyselyn ongelmana olivat harhat eli ei-satunnaisvirheet, jotka ovat subjektiivisen tiedon mittausvirheitä. Tämän tutkimuksen ensimmäisessä kyselyssä oli paljon subjektiiviseksi luokiteltavia kysymyksiä, jotka aiheuttivat vinoutta mittausprosessiin.

Toisessa kyselyssä pyrittiin ottamaan huomioon ensimmäisen kyselyn puutteet. Toisen kyselyn puutteena voidaan kuitenkin pitää kvantitatiiviselle tutkimukselle erittäin pientä (32 kpl) otoskokoa ja käytettyjen kysymysten pientä määrää, jolloin mittarin yhtenäisyys voidaan asettaa kyseenalaiseksi. Tutkimustulosten luotettavuutta saattaa heikentää myös se, että ensimmäisen kyselyn ja koulutuksen välinen aika venyi lähes kahteen vuoteen. Toisen kyselyn osalta on siten huomioitava se, että pienen aineiston takia tu-

lokset ovat vain suuntaa antavia. Ne kuitenkin antavat vahvoja viitteitä siitä, että tietoturvakoulutuksella voidaan merkittävästi vaikuttaa yksilön aikomuksiin noudattaa organisaation tietoturvaohjeita ja -sääntöjä.

Tämän tutkimuksen valossa tietoturvakoulutukselle pelastuslaitoksessa oli tarvetta ja sillä oli huomattava vaikutus vastaajien aikomukseen noudattaa tietoturvaohjeita. Tämän tutkimuksen tulosten perusteella suunnitelmallinen koulutus tuo siis tuloksia. Koulutuksen tuoman hyödyn ylläpitäminen vaatii kuitenkin lisäpanostusta. Siksi säännöllinen tietoturvakoulutus kannattaa sisällyttää osaksi tietoturvan hallintaprosessia.

Tämän tutkimuksen tieteellisenä kontribuutiona oli viranomaisorganisaation tuominen tietoturvatutkimuksen piiriin. Tällaista tutkimusta ei aiemmin ole pelastusalalla tehty, joten tässä tutkimuksessa esitellystä koulutusmallista ja saaduista tuloksista on hyötyä muillekin pelastuslaitoksille tietoturvakoulutusta suunniteltaessa.

Lähteet

- Ahuja, M., Chudoba, K. M., George, J. F., Kacmar, C. & McKnight, H. (2002). Overworked and isolated? Predicting the effect of work-family conflict, autonomy, and workload on organizational commitment and turnover of virtual workers. *Proceedings of the 35th Annual Hawaii International Conference on System Science*, 3586-3593.
- Ajzen, I. (2005) *Attitudes, Personality and Behaviour*. Berkshire England. McGraw-Hill Education.
- Aytes, K. & Conolly, T. (2003). A Research Model for Investigating Human behaviour Related to Computer Security. *Ninth Americas Conference on Information Systems* 2027-2030.
- Bailey, Ainsworth A. (2006) Retail employee theft: a theory of planned behavior perspective. *International Journal of Retail & Distribution Management* 34(11).
- Belsis, P., Kokolakis, S. & Kiountouzis, E. (2005). Information systems security from a knowledge management perspective. *Information Management & Computer Security* 13(3).
- Bollen, K. & Lennox, R. (1991). Conventional wisdom on measurement. A structural equation perspective. *Psychological Bulletin*, 110 (2), pp. 305-314.
- Bollen, K.A.1989. *Structural Equations with Latent Variables*. New York: John Wiley & Sons.
- Chaston, Ian (1994) Managing for Total Training Quality. *Training for Quality* 2(3): 11-14.
- Chin, W.W. & Newsted, P.R. (1999). *Structural Equation Modeling Analysis with Small Samples Using Partial Least Squares*. In R.H. Hoyle (eds.) *Statistical Strategies for Small Sample research*. Thousand Oaks, CA: Sage Publications.
- Chin, W.W. 2005. *Partial Least Squares SEM with PLS-graph: demonstration with examples form marketing & IT research*. C.T. Bauer College of Business, University of Houston.
- Choudhry, R M., Fang, D. & Mohamed, S. (2007). The nature of safety culture: A survey of the state-of-the-art. *Safety Science*, 45(10): 993-1012.
- Crano, W. D. & Prislin, R. (2006). Attitudes and persuasion. *Annual Review of Psychology* 57(): 345-374.
- D'Arcy, J. & Hovav, A. (2007). Deterring internal information systems misuse. *Communications of the ACM* 50(10): 113-117.

- Dark, M J. & Winstead, J. (2005). Using educational theory and moral psychology to inform the teaching of ethics in computing, *Proceedings of the 2nd annual conference on Information security curriculum development*, 27-31.
- Davis, F. & Venkatesh, V. (1996). A critical assessment of potential measurement biases in the technology acceptance model: three experiments. *International Journal of Human-Computer Studies*, 45(1): 19-45.
- Desman, M.B. (2002). *Building an Information Security Awareness Program*, Auerbach Publications, USA.
- Dibbern, J., Goles, T., Hirschheim, R. & Jayatilaka, B. (2004). Information systems outsourcing: a survey and analysis of the literature. *SIGMIS Database* 35(4): 6-102.
- Eaves, M. (1990). The Elaboration Likelihood Model and Proxemic Violations as Peripheral Cues to Information Processing. *Draft of chapter to appear in: Chaiken, S. & Trope, Y. (Eds.), Dual process theories in social psychology*. New York: Guilford Press.
- Embse, T J. von der, Desai, M S. & Desai, S. (2004). How well are corporate ethics codes and policies applied in the trenches? Key factors and conditions. *Information Management & Computer Security* 12(2).
- Foltz, C., Cronan, T. & Jones, T. (2005). Have you met your organization's computer usage policy? *Industrial Management & Data Systems* 105(2).
- Heikkilä, T. (2001). *Tilastollinen tutkimus*. Helsinki, Edita.
- Hilton, Thomas (2000). Information systems ethics: A practitioner survey. *Journal of Business Ethics* 28(4): 279.
- Hirschheim, R. & Klein, H. (1989). Four paradigms of information systems development. *Communications of the ACM* 32(10): 1199-1216.
- Hong, K-S., Chi, Y-P., Chao, L. & Tang, J-H. (2003). An integrated system theory of information security management. *Information Management & Computer Security* 11(5).
- Jarvis, C.B., Mackenzie, S.B. & Podsakoff, P.M. (2003). A Critical Review of Construct Indicators and Measurement Model Misspecification in Marketing and Consumer Research. *Journal of Consumer Research*, Vol.30.
- Kesar, S. & Rogerson, S. (1997). Developing ethical practices to minimise computer misuse. *International Symposium* 219-225.
- Kuo, F-Y & Hsu, M-H (2001). Development and Validation of Ethical Computer Self-Efficacy Measure: The Case of Softlifting. *Journal of Business Ethics* 32(4): 299-315.
- Lambert, N. (2000). Applications of Psychological Knowledge to Schooling. *Annual Conference of the American Psychological Association 108th, Washington, DC, USA*.

- Layton, T.P. (2005). *Information Security Awareness: The Psychology Behind the Technology*. AuthorHouse, USA.
- Lee, J. & Lee, Y. (2002). A holistic model of computer abuse within organizations. *Information Management & Computer Security* 10(2).
- Lee, O., Lim, K., Wong, W. (2005). Why Employees Do Non-Work-Related Computing: An Exploratory Investigation through Multiple Theoretical Perspectives. *Proceedings of the 38th Hawaii International Conference on System Sciences - 2005*
- Lewin, C. (2004). *Research Methods in the Social Sciences*. Sage Publications.
- McCombs, B. & Vakili, D (2005). A Learner-Centered Framework for E-Learning. *Teachers College Record* 107(8): 1582-1600.
- McCoy, C. & Fowler, R. (2004). You are the key to security: establishing a successful security awareness program. *Proceedings of the 32nd annual ACM SIGUCCS conference on User services, th, Baltimore, MD, USA*, 346-349.
- McGovern, M. (2002). Opening eyes: building company-wide IT security awareness. *IT Professional* 4(3): 52-54.
- McIlwraith, A. (2006). *Information Security and Employee Behaviour: How to Reduce Risk Through Employee Education, Training and Awareness*. Gower Publishing Limited, England.
- McNamara H., Richardson, S. & Courtney, J. (2003). Encouraging Ethical Behavior in Organizations: Punishment as Magnitude of Consequences. 2003 — *Ninth Americas Conference on Information Systems*, 2362-2366.
- Metsämuuronen, J. (2002). *Metodologia-sarja*. e-Kirja, International Methelp Ky, Helsinki.
- Mills, A. (1995) Inadequate security encourages the thief. *Industrial Management & Data Systems* 95(2).
- Millward, L. (2001). *Organizational research methods* [Elektroninen aineisto] : a guide for students and researchers. London: SAGE Thousand Oaks, California.
- Muijs, D. (2004) *Doing quantitative research in education with SPSS* [Elektroninen aineisto]. London: SAGE.
- Pahnila, S., Siponen, M. & Mahmood, A. (2007). Employees' Behavior towards IS Security Policy Compliance. *40th Annual Hawaii International Conference*, 156b-156b.
- Pfleeger, L., Trope L., Roland L. & Palmer, C. (2007). Guest Editors' Introduction: Managing Organizational Security. *Security & Privacy Magazine, IEEE* 5(3): 13-15.

- Puhakainen, P. & Siponen, M. (2005). Three design theories for IS security awareness. *Unpublished research paper, University of Oulu.*
- Puhakainen, P. A design theory for information security awareness. *Unpublished Ph.D. Thesis, Oulu, Finland, 2006.*
- Rawstorne, P., Jayasuriya, R. & Caputi, P. (2000). Issues in predicting and explaining usage behaviors with the technology acceptance model and the theory of planned behavior when usage is mandatory. *Proceedings of the twenty first international conference on Information systems, Brisbane, Queensland, Australia, 35-44.*
- Resch, C. (2004). Designing an information security system. Information Assurance Workshop, 2004. *Proceedings from the Fifth Annual IEEE SMC, 449-450. : .*
- Roper, C.A., Grau, J.A. & Fisher, L.F. (2006) Security Education, Awareness and Training: From Theory to Practice. *Elsevier Butterworth-Heinemann, Oxford, UK.*
- Schultz, E. (2004). Security training and awareness—fitting a square peg in a round hole. *Computers & Security, 23(1): 1-2.*
- Siponen, M. & Baskerville, R. (2001). A New Paradigm for Adding Security into IS development Methods. *Eighth Annual Working Conference on Information Security Management & Small Systems Security 99-111.*
- Siponen, M. & Kajava, J. (1998). Ontology of organizational IT security awareness—from theoretical foundations to practical framework. Enabling Technologies: Infrastructure for Collaborative Enterprises, 1998. (WET ICE '98) *Proceedings., Seventh IEEE International Workshops 327-331.*
- Siponen, M. & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *SIGMIS Database 38(1): 60-80.*
- Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security 8(1): 31-41.*
- Siponen, M. (2004). A Pragmatic Evaluation of the Theory of Information Ethics. *Ethics and Information Technology 6(4): 279-290.*
- Solms, R. von (1998). Information security management (3): the Code of Practice for Information Security Management (BS 7799). *Information Management & Computer Security 6(5): 224-225.*
- Solms, R. von (1999). Information security management: why standards are important. *Information Management & Computer Security 7(1).*
- Spillers, W. R. & Newsome, S. L. (1990). Another look at design theory. *Systems, Man and Cybernetics, IEEE Transactions on 20(2): 528-530.*
- Stanton, J., Stam, K., Mastrangelo, P. & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security, 24(2): 124-133.*

- Torres, J., Sarriegi, J., Santos, J. & Serrano, N. (2006). Managing Information Systems Security: Critical Success Factors and Indicators to Measure Effectiveness. *Information Security*: 530-545.
- VAHTI 6/2006 (2006). Tietoturvatavoitteiden asettaminen ja mittaaminen. Valtiovarainministeriö, Hallinnon kehittämisosasto, Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI, Lainattu 20.1.2008, saatavilla: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/53828/name.jsp
- VAHTI 6/2003 (2003). Opas julkishallinnon tietoturvakoulutuksen järjestämiseksi. Valtiovarainministeriö, Hallinnon kehittämisosasto, Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI, Lainattu 20.1.2008, saatavilla: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/53763/name.jsp
- Wiant, T. (2005). Information security policy's impact on reporting security incidents. *Computers & Security*, 24(6): 448-459.

Liite A. Oppijakeskeisen opetuksen teoria.

Taulukko 1. Oppijakeskeisen opetuksen teorian neljä aihealuetta ja neljätoista periaatetta. (McCombs ja Vakili 2006).

Periaate	Aihealue	Selite
	Tiedolliset ja metatiedolliset tekijät	
<i>Periaate 1</i>	Oppimisprosessin luonne	Vaikeiden asioiden oppiminen on tehokkainta jos se on mielekäs kokonaisuus tietoa ja kokemusta.
<i>Periaate 2</i>	Oppimisprosessin tavoitteet	Menestyvä oppija pystyy ajan ja opetuksen avustamana luoda tarkoituksenmukaisen ja johdonmukaisen tiedon kuvan.
<i>Periaate 3</i>	Tietämyksen rakenteet	Menestyvä oppija sitoo uuden informaation olemassa olevaan tietoon ymmärrettävällä tavalla.
<i>Periaate 4</i>	Strateginen ajattelu	Menestyvä oppija voi luoda ja käyttää ajattelunvalikoimaa ja järkeviä strategioita saavuttaakseen monimutkaiset oppimistavoitteet
<i>Periaate 5</i>	Ajattelun ajattelu	Korkein järjestysmalli valvomaan ja valikoimaan niitä henkisiä operaatioita, jotka helpottavat kriittistä ja luovaa ajattelua.
<i>Periaate 6</i>	Oppimisen konteksti	Oppiminen on riippuvainen ympäristötekijöistä, kuten kulttuurista, teknologiasta ja opetuskäytännöistä.
	Motivaatioon ja mielialaan mukautuvat tekijät	
<i>Periaate 7</i>	Motivaation ja tunteen vaikutus oppimiseen	Oppijan motivaatioon vaikuttaa henkinen tila, uskomukset, kiinnostukset, tavoitteet ja tapa ajatella.
<i>Periaate 8</i>	Luontainen motivaatio oppimiseen	Sisäiseen motivaatioon vaikuttaa sopiva asian uutuus(uutuudenviehätys) ja vaikeus, suhteessa henkilökohtaiseen kiinnostukseen.
<i>Periaate 9</i>	Motivaation vaikutus tuloksiin	Ilman motivaatiota oppija ei vapaaehtoisesti ponnistele päämäärän eteen vaan tarvitaan pakkoa.

(jatkuu)

Taulukko 1. Oppijakeskeisen opetuksen teorian neljä aihealuetta ja neljätoista periaatetta McCombs ja Vakili (2006). (jatkuu)

	Kehitys- ja sosiaaliset tekijät	
<i>Periaate 10</i>	Oppimisen kehitysvai- kutukset	Oppiminen on sitä tehokkaampaa, mitä enemmän fyysisesti, henkisesti, emotionaalisesti ja sosiaalisti merkittävää kehitystä tapahtuu edellä mainittujen alueiden sisällä ja välillä.
<i>Periaate 11</i>	Sosiaaliset vaikutukset oppimiseen	Oppimiseen vaikuttaa sosiaaliset kontaktit, henkilökohtaiset suhteet ja kommunikointi oppijien välillä.
	Yksilöllisyys- /eroavaisuustekijät	
<i>Periaate 12</i>	Oppiminen ja moninai- suus	Oppiminen on tehokasta jos oppijan kielelliset, kulttuuriset ja sosiaaliset taustat otetaan huomioon.
<i>Periaate 13</i>	Yksilölliset oppimiserot	Oppijoilla on yksilölliset toimintatavat, lähestymistavat ja kyvyt oppimiseen. Tähän vaikuttaa kokemus ja perimä.
<i>Periaate 14</i>	Normit ja arviointime- netelmät	Tavoitteiden asettaminen riittävän korkealle ja haasteellisiksi, sekä oppijan ja oppimisprosessin arvioiminen ovat rinnakkaisia menetelmiä.

Liite B. Ensimmäisen kyselyn kysymykset.

	Vastausten määrä	Minimi	Maksimi	keskiarvo	keskihajonta
K1: Aion noudattaa tietoturvaohjeita.		3	7	6,48	,805
K2: Aion suositella toisille tietoturvaohjeiden noudattamista.	141	1	7	6,30	1,315
K3: Aion auttaa muita tietoturvaohjeiden noudattamisessa.	141	1	7	5,97	1,402
K4: Noudatan tietoturvaohjeita.	141	2	7	6,16	1,019
K5: Suosittelen toisille tietoturvaohjeiden noudattamista.	141	0	7	6,09	1,457
K6: Autan muita tietoturvaohjeiden noudattamisessa.	141	0	7	5,47	1,901
K7: Koen tietoturvaohjeiden noudattamisen positiivisena asiana.	141	0	7	6,42	1,225
K8: Koen positiivisena asiana kun muut noudattavat tietoturvaohjeita.	141	0	7	6,35	1,208
K9: Koen tietoturvaohjeiden noudattamisen miellyttävänä.	141	0	7	5,53	1,346
K10: Tietoturvaohjeiden noudattamisesta on tullut minulle tapa.	141	0	7	5,28	1,619

(jatkuu)

Liite B. (jatkuu)

K11: Tietoturvaohjeiden noudattamisesta on tullut minulle luonnollista.	141	0	7	5,29	1,681
K12: Tietoturvaohjeiden noudattaminen on minulle itsestään selvää.	141	0	7	5,45	1,571
K13: Olen liian kiireinen noudattamaan tietoturvaohjeita.	141	0	7	2,95	2,018
K14: Minulla on riittävä tietämys tietoturvaohjeiden noudattamiseksi.	141	0	7	3,90	1,870
K15: Tarvitsen enemmän ohjausta esimieheltäni työhöni liittyvissä tietoturvatehtävissä.	141	0	7	4,04	2,010
K16: Tarvitsen enemmän ohjausta tietoturvahenkilöstöltä työhöni liittyvissä tietoturvatehtävissä.	141	0	7	4,60	2,107
K17: Tukea on saatavilla jos kohtaan vaikeuksia tietoturvaohjeiden noudattamisessa.	141	0	7	5,27	1,631
K18: Ylimmän johdon mielestä minun tulisi noudattaa tietoturvaohjeita.	141	0	7	6,03	1,463
K19: Esimieheni ovat sitä mieltä, että minun tulisi noudattaa tietoturvaohjeita.	141	0	7	6,00	1,468

(jatkuu)

Liite B. (jatkuu)

K20: Läheiset työtoverini ovat sitä mieltä, että minun tulisi noudattaa tietoturvaohjeita.	141	0	7	5,64	1,552
K21: Organisaationi tietoturvahenkilöstö on sitä mieltä, että minun tulisi noudattaa tietoturvaohjeita.	141	0	7	6,24	1,378
K22: Tietoturva-asioita markkinoidaan laajasti organisaatiossani.	141	0	7	3,71	1,486
K23: Tietoturva-asiat eivät ole näkyvästi esillä organisaatiossani.	141	0	7	4,09	1,707
K24: Tietoturvaongelmat ovat esillä julkisuudessa.	141	0	7	4,88	1,589
K25: Hyviä tietoturvakäytäntöjä markkinoidaan julkisuudessa.	141	0	7	4,40	1,505
K26: Tietoturvaohjeet ovat tarvittaessa saatavilla nopeasti.	141	0	7	3,55	1,744
K27: Tietoturvaohjeiden tiedonmäärä on tarpeisiini sopiva.	141	0	7	4,09	1,764
K28: Tietoturvaohjeissa on riittävästi informaatiota.	141	0	7	4,12	1,772

(jatkuu)

Liite B. (jatkuu)

K29: Tietoturvaohjeita on helppo ymmärtää.	141	0	7	3,76	1,647
K30: Tietoturvaohjeet ovat merkityksellisiä työtehtävieni kannalta.	141	0	7	5,03	1,713
K31: Tietoturvaohjeet ovat riittävän ajan tasalla työtehtävieni kannalta.	141	0	7	4,63	1,595
K32: Löydän tietoturvaohjeista tarvitsemani tiedon nopeasti.	141	0	7	3,57	1,679
K33: Jos en noudata tietoturvaohjeita, minua rangaistaan.	141	0	7	2,77	1,792
K34: Jos en noudata tietoturvaohjeita, siitä seuraa ankara rangaistus.	141	0	7	2,47	1,634
K35: Jos en noudata tietoturvaohjeita, rangaistus seuraa välittömästi.	141	0	6	2,16	1,447
K36: Tuntisin syyllisyyttä jos en noudattaisi tietoturvaohjeita.	141	0	7	5,30	1,595
K37: Minulle koituisi ongelmia, jos työtoverini huomaisivat, että en noudata tietoturvaohjeita.	141	0	7	3,60	1,834
K38: En ajattele seurauksia jättäessäni noudattamatta tietoturvaohjeita.	141	0	7	2,26	1,643

(jatkuu)

Liite B. (jatkuu)

K39: Tietoturvarikkomus organisaatiossani olisi minulle vakava ongelma.	141	0	7	4,16	1,946
K40: Tietoturvarikkomus olisi organisaatiolleni vakava ongelma.	141	0	7	4,78	2,111
K41: Tietoturvarikkomukset tulevat yhä vakavammiksi.	141	0	7	4,98	1,967
K42: Voin joutua tietoturvarikkomuksen kohteeksi.	141	0	7	5,08	1,882
K43: Organisaationi voi joutua tietoturvarikkomuksen kohteeksi.	141	0	7	5,32	1,791
K44: Organisaationi kohtaa yhä vakavampia tietoturvaongelmia.	141	0	7	4,54	1,854
K45: Organisaationi tieturvahenkilöstö pitää tietoturvarikkomukset vähäisinä.	141	0	7	3,74	1,949
K46: Organisaationi tieturvaohjeet pitävät tietoturvarikkomukset vähäisinä.	141	0	7	3,77	1,697
K47: Organisaationi tieturvaohjeiden noudattaminen pitää tietoturvarikkomukset vähäisinä.	141	0	7	4,37	1,844

(jatkuu)

Liite B. (jatkuu)

K48: Pystyn noudattamaan tietoturvaohjeita itsenäisesti.	141	0	7	4,83	1,873
K49: Pystyn soveltamaan tietoturvaratkaisuja jos saan apua tarvittaessa.	141	0	7	5,48	1,751
K50: Pystyn soveltamaan tietoturvaratkaisuja jos joku näyttää niiden toiminnan minulle.	141	0	7	5,70	1,708
K51: Jos noudatan tietoturvaohjeita, saan materiaallisen palkinnon.	141	0	7	1,80	1,521
K52: Jos noudatan tietoturvaohjeita, saan arvostusta.	141	0	7	2,85	1,955
K53: Jos noudatan tietoturvaohjeita, saan kiitosta esimiehiltäni.	141	0	7	2,60	1,899

Liite C. Toisen kyselyn kysymykset

	vastausten lukumäärä	Minimi	Maksimi	Keskiarvo	Keskihajonta
K1. On hyvä, että kouluttaja tuntee pelastusalan.	31	3	5	4,08	,494
K2. Koulutus oli hyödyllistä	31	4	5	4,77	,439
K3. Tietoja voi hyödyntää työtehtävissä	31	4	5	4,38	,506
K4. Aihe oli ajankohtainen	31	4	5	4,92	,277
K5. Aihe toi lisätietoa	31	4	5	4,69	,480
K6. Työnantaja hyötyy koulutuksesta	31	4	5	4,54	,519
K7. Työntekijä hyötyy koulutuksesta	31	4	5	4,77	,439
K8. Pelastuslaitoksen johto pitää koulutusta tärkeänä	31	4	5	4,69	,480
K9. Aion noudattaa tietoturvaohjeita	31	4	5	4,77	,439
K10. Ohjeiden noudattaminen on järkevää	31	4	5	4,92	,277
K11. Ohjeiden noudattamatta jättämisestä voidaan rangaista	31	4	5	4,85	,376

(Jatkuu)

Liite C. (jatkuu)

K12. Käyttäjätunnukset ovat henkilökohtaisia	31	4	5	4,92	,277
K13. Kehittynyt tietotekniikka suojelee pelastuslaitosta tietoturvauhilta	31	1	5	3,23	1,536
K14. Yksittäinen työntekijä voi parantaa tietoturvaa pelastuslaitoksessa	31	1	4	1,85	1,068
K15. Tietoturvasta hössötetään liikaa	31	1	4	1,62	,870
K16. Riittää, että esimieheni tuntevat ohjeet	31	1	4	1,92	1,256
K17. Ohjeet ovat helposti saatavissa	31	2	4	3,46	,776
K18. Ohjeita on helppo noudattaa	31	2	5	3,69	,947
K19. Ohjeet ovat helposti ymmärrettävissä	31	2	5	3,62	1,044
K20. En välitä, mitä muut ajattelevat ohjeiden noudattamisesta	31	1	2	1,46	,519

Liite D. Ensimmäisen kyselyn toinen osio

Kysymys		Kysymys	
1. Onko työnantajallasi tietoturvalu- litiikka?		2. Kaupungin tietoturvasta vastaa:	
Kyllä		Ylin johto	
Ei		Atk-tuki	
En tiedä		Käyttäjät	
3. Toisen tunnuksien käyttö on:		4. Olen tallentanut omia pelejä, kuvatiedostoja tai ohjelmia työkoneeseeni:	
Sallittua poikkeustapauksissa		Usein	
Sallittua aina työasioissa		Joskus	
Aina kiellettyä		En koskaan	
5. Tietojärjestelmän käyttöoikeuden taso riippuu:		6. Mitä teet jos oikeutesi eivät riitä, mutta töiden hoito vaatii tietojärjestelmän jokin osan käyttöä?	
Työkokemuksesta		Pyydän työkaveria avaamaan koneen tunnuksillaan	
Työtehtävästä		Neuvottelen esimieheni kanssa lisäoikeuksista	
Tietokoneen käyttötaidosta		Soitan atk-tukeen ja pyydän lisää oikeuksia	
7. Onko etätyö luvanvaraista?		8. Etätyössä voin käyttää omia ohjelmia	
Kyllä		Kyllä	
Ei		En	
En tiedä		En tiedä	

(jatkuu)

Liite D. (jatkuu)

9. Mikä seuraavista vaikuttaa tietoaineiston tietoturvalliseen käsittelyyn?		10. Kuka vastaa salassa pidettävän asiakirjan luokittelusta ja merkinnästä?	
Käsittelijän työtehtävä		Asiakirjan laatija tehtävänsä mukaisesti	
Aineiston tietoturvaluokitus		Arkiston hoitaja tehtävään määrättyinä	
Laatijan työtehtävä		Atk- osasto	
11. Mitä seuraavista ei tarvitse tehdä salassa pidettävää aineistoa lähetettäessä?		12. Miten salassa pidettävä aineisto hävitetään?	
Varmistua vastaanottajan oikeudesta käsitellä salassa pidettävää aineistoa		Samoin, kuin muukin aineisto	
Aineiston luokituksen merkitsemistä		Laittamalla se tiedon suojausvaatimusten mukaisiin tietoturva-aineiston keräyslaatikkoihin tai silppuriin	
Ilmoittaa tietohallinnolle lähetyksestä		Annetaan esim. siivojalle hävitettäväksi	
13. Mitä tarkoittaa "Puhtaanpöydän -periaate"?		14. Työntekijän vaihtolovelvollisuus koskee mm. hänen tietoonsa tulleita yksityisiä viestejä. Mikä muu alla olevista kuuluu vaihtolovelvollisuuden piiriin?	
Luokitellusta aineistosta siivottua työpöytä		Vahingossa saatuja toiselle tarkoitettuja sähköposteja	
Puhdasta, kaikista työpapereita vapaata työpöytä		Kaikkea sähköpostiliikennettä, myös roskapostia	
Hyvää järjestystä työpöydällä		Työtiloissa nähtyjen ulkopuolisten nimet	
15. Kenelle saa tarvittaessa luovuttaa henkilökohtaiset käyttöoikeudet ja salasanat?		16. Kuka saa asentaa ja päivittää ohjelmia ja laitteita?	
Esimiehelle		Jokainen saa omaa työasemaansa	
Työkaverille		Atk-tuki, tai tuen nimeämä käyttäjä	
En kenellekään		Asiantunteva työkaveri	
Atk- tuelle			

(jatkuu)

Liite D. (jatkuu)

17. Mihin tietovarastojen tietoja saa käyttää?		18. Jos käytät julkisia päätteitä tai toisen henkilön tietokonetta, niin mitä sinun ei tarvitse tehdä lopetettuasi työskentelyn?	
Käytölle ei ole rajoituksia		Kirjautua ulos	
Omien työtehtävien hoitoon		Vaihtaa salasana	
Kaikkiin organisaation töihin		Tyhjentää selaimen välimuisti	
19. Mikä näistä on hyvä salasana?		20. Milloin täytyy käyttää salausta, kun lähetetään tietoa Internetin kautta?	
Matti45		Aina	
Musti		Lähetettäessä salassa pidettävää tietoa	
Ko1ri2PAllo		Se on jokaisen omassa harkinnassa	
21. Mitä täytyy tehdä, jos saa sähköpostissa roskapostia?		22. Missä virka sähköpostia ei saa käsitellä?	
Tuhota se avaamatta		Omilla laitteilla ja ohjelmilla	
Ilmoittaa tietohallintoon ja pyytää joku tuhoamaan se		Organisaation laitteilla	
Vastata ja pyytää lopettamaan lähettäminen		Muilla julkishallinnon laitteilla ja ohjelmilla	
23. Missä tilanteessa töissä voi käyttää muuta sähköpostijärjestelmää tai osoitetta kuin virkasähköpostia?		24. Käytän työkonetta yksityisasioiden hoitamiseen:	
Jos siihen on tietohallinnon lupa		Päivittäin	
Ei koskaan		Joskus	
Silloin kun virkaposti ei toimi		En koskaan	

(jatkuu)

Liite D. (jatkuu)

25. Olen luovuttanut tunnukseni, tai avoimen päätteen työkaverille:		26. Olen itse pyytänyt tai minulle on annettu jonkun toisen tunnukset, tai avoin pääte:	
Päivittäin		Päivittäin	
Joskus		Joskus	
En koskaan		En koskaan	
27. Lukitsen aina työasemani kun poistun sen ääreltä:			
Aina			
Joskus			
En koskaan			
En osaa lukita työasemaani			

Liite F. Formatiivisen SEM-mallinnuksen validoinnin tulokset.

Taulukko 1. Validoinnin keskeiset tulokset ennen koulutusta.

Latentti muuttuja	indikaattori	Sisäinen painoarvo
Asenne	Koen tietoturvaohjeiden noudattamisen positiivisena asiana.	0.3227**
	Koen positiivisena asiana kun muut noudattavat tietoturvaohjeita.	0.0647
	Koen tietoturvaohjeiden noudattamisen miellyttävänä	0.5096***
	Tietoturvaohjeiden noudattamisesta on tullut minulle tapa	0.1378
	Tietoturvaohjeiden noudattamisesta on tullut minulle luonnollista	0.1162
	Tietoturvaohjeiden noudattaminen on minulle itsestään selvää.	0.1392
	Jos en noudata tietoturvaohjeita, minua rangaistaan.	0.1505
	Jos en noudata tietoturvaohjeita, siitä seuraa ankara rangaistus	-0.2367*
	Jos en noudata tietoturvaohjeita, rangaistus seuraa välittömästi	0.0604
	Normit	Ylimmän johdon mielestä minun tulisi noudattaa tietoturvaohjeita
Esimieheni ovat sitä mieltä, että minun tulisi noudattaa tietoturvaohjeita		0.2008
Läheiset työtoverini ovat sitä mieltä, että minun tulisi noudattaa tietoturvaohjeita.		0.0196
Organisaationi tietoturvahenkilöstö on sitä mieltä, että minun tulisi noudattaa tietoturvaohjeita		0.1103
Minulle koituisi ongelmia, jos työtoverini huomaisivat, että en noudata tietoturvaohjeita		0.1040*
En ajattele seurauksia jättäessäni noudattamatta tietoturvaohjeita.		-0.6928***

(jatkuu)

Taulukko 1. (jatkuu)

Vaikutus	Olen liian kiireinen noudattamaan tietoturvaohjeita	-0.5771**
	Minulla on riittävä tietämys tietoturvaohjeiden noudattamiseksi.	0.6001**
	Tietoturvaohjeet ovat tarvittaessa saatavilla nopeasti	-0.1611
	Pystyn noudattamaan tietoturvaohjeita itsenäisesti.	-0.0563
	Pystyn soveltamaan tietoturvaratkaisuja jos saan apua tarvittaessa.	0.0499
	Pystyn soveltamaan tietoturvaratkaisuja jos joku näyttää niiden toiminnan minulle.	0.4557*
Helppous	Tietoturvaohjeet ovat tarvittaessa saatavilla nopeasti.	-0.6821*
	Tietoturvaohjeita on helppo ymmärtää.	0.1546
	Tietoturvaohjeet ovat merkityksellisiä työtehtävieni kannalta.	0.8044***
	Löydän tietoturvaohjeista tarvitsemani tiedon nopeasti.	0.5851**
	Organisaationi tietoturvaohjeiden noudattaminen pitää tietoturvarikkomukset vähäisinä.	0.0560

Taulukko 2. Validoinnin keskeiset tulokset koulutuksen jälkeen.

Latentti muuttuja	indikaattori	Sisäinen painoarvo
Asenne	Ohjeiden noudattaminen on järkevää	0.10084***
	Tietoturvasta hössötetään liikaa	0.0842
Normit	Pelastuslaitoksen johto pitää koulutusta tärkeänä	0.4752*
	Ohjeiden noudattamatta jättämisestä voidaan rangaista	-0.3003*
	En välitä, mitä muut ajattelevat ohjeiden noudattamisesta	0.5495**
Vaikutus	Kehittynyt tietotekniikka suojelee pelastuslaitosta tietoturvauhilta	0.7491**
	Yksittäinen työntekijä voi parantaa tietoturvaa pelastuslaitoksessa	-0.5755*
Helppous	Ohjeet ovat helposti saatavissa	0.2589
	Ohjeita on helppo noudattaa	-0.6900*
	Ohjeet ovat helposti ymmärrettävissä	0.7270*
Hyödyllisyys	Koulutus oli hyödyllistä	0.2713***
	Tietoja voi hyödyntää työtehtävissä	0.2327***
	Aihe oli ajankohtainen	0.2510***
	Aihe toi lisätietoa	0.1818***
	Työnantaja hyötyy koulutuksesta	0.1378*
	Työntekijä hyötyy koulutuksesta	0.2598***

Liite G. Ensimmäisen kyselyn summamuuttajat

Taulukko 1. Asennemuuttujan muodostamiseen käytettyjen kysymysten keskiarvot ja –hajonnat.

	Kysymys	Minimi	Maksimi	Keskiarvo	Keskihajonta
Asenne	7. Koen tietoturvaohjeiden noudattamisen positiivisena	3	7	6,42	1,225
	8. Koen positiivisena asiana kun muut noudattavat tietoturvaohjeita	1	7	6,35	1,208
	9. Koen tietoturvaohjeiden noudattamisen miellyttävänä	3	7	5,53	1,346
	10. Tietoturvaohjeiden noudattamisesta on tullut minulle luonnollista.	1	7	5,28	1,619
	11. Tietoturvaohjeiden noudattaminen on minulle itsestään selvää	1	7	5,29	1,681
	12. Jos en noudata tietoturvaohjeita, minua rangaistaan.	2	7	5,45	1,571
	33. Jos en noudata tietoturvaohjeita, minua rangaistaan.	1	7	2,77	1,792
	34. Jos en noudata tietoturvaohjeita, siitä seuraa ankara rangaistus	1	7	2,47	1,634
	35. Jos en noudata tietoturvaohjeita, rangaistus seuraa välittömästi.	1	6	2,16	1,447

Taulukko 2. Normimuuttujan muodostamiseen käytettyjen kysymysten keskiarvot ja –hajonnat.

	Kysymys	Minimi	Maksimi	Keskiarvo	Keskihajonta
Normit	18. Ylimmän johdon mielestä minun tulisi noudattaa tietoturvaohjeita	1	7	6,03	1,463
	19. Esimieheni ovat sitä mieltä, että minun tulisi noudattaa tietoturvaohjeita	1	7	6,00	1,468
	20. Läheiset työtoverini ovat sitä mieltä, että minun tulisi noudattaa tietoturvaohjeita	1	7	5,64	1,552
	21. Organisaationi tietoturvahenkilöstö on sitä mieltä, että minun tulisi noudattaa tietoturvaohjeita	1	7	6,24	1,378
	37. Minulle koituisi ongelmia, jos työtoverini huomaisivat, että en noudata tietoturvaohjeita	1	7	3,60	1,834
	38. En ajattele seurauksia jättäessäni noudattamatta tietoturvaohjeita	1	7	2,26	1,643

Taulukko 3. Havaittujen vaikutusmahdollisuuksia kuvaavan muuttujan muodostamiseen käytettyjen kysymysten keskiarvot ja – hajonnat.

	Kysymys	Minimi	Maksimi	Keskiarvo	Keskihajonta
Havaitut vaikutusmahdollisuudet	13, Olen liian kiireinen noudattamaan tietoturvaohjeita.	1	7	2,95	2,018
	14, Minulla on riittävä tietämys tietoturvaohjeiden noudattamiseksi.	1	7	3,90	1,870
	26, Tietoturvaohjeet ovat tarvittaessa saatavilla nopeasti.	1	7	3,55	1,744
	48, Pystyn noudattamaan tietoturvaohjeita itsenäisesti.	1	7	4,83	1,873
	49, Pystyn soveltamaan tietoturvaratkaisuja jos saan apua tarvittaessa.	2	7	5,48	1,751
	50, Pystyn soveltamaan tietoturvaratkaisuja jos joku näyttää niiden toiminnan minulle.	2	7	5,70	1,708

Taulukko 4. Havaitun käytön helppoutta kuvaavan muuttujan muodostamiseen käytettyjen kysymysten keskiarvot ja – hajonnat.

	Kysymys	Minimi	Maksimi	Keskiarvo	Keskihajonta
Havaittu käytön helppous ja hyödyllisyys	26. Tietoturvaohjeet ovat tarvittaessa saatavilla nopeasti.	1	7	3,55	1,744
	29. Tietoturvaohjeita on helppo ymmärtää.	1	7	3,76	1,647
	30. Tietoturvaohjeet ovat merkityksellisiä työtehtävieni kannalta.	1	7	5,03	1,713
	32. Löydän tietoturvaohjeista tarvitsemani tiedon nopeasti.	1	7	3,57	1,679
	47. Organisaationi tietoturvaohjeiden noudattaminen pitää tietoturvarikkomukset vähäisinä.	1	7	4,37	1,844

Liite H. Toisen kyselyn summamuuttujat

Taulukko 1. Asennemuuttujan laskemiseen käytettyjen kysymysten keskiarvot ja – hajonnat toisen kyselytutkimuksen analyysissä.

Asenne	Kysymys	Minimi	Maksimi	Keskiarvo	Keskihajonta
	10. Ohjeiden noudattaminen on järkevää	4	5	4,81	,402
	15. Tietoturvasta hössötetään liikaa	1	5	1,84	1,157

Taulukko 2. Normimuuttujan laskemiseen käytettyjen kysymysten keskiarvot ja – hajonnat toisen kyselytutkimuksen analyysissä.

Normit	Kysymys	Minimi	Maksimi	Keskiarvo	Keskihajonta
	8. Pelastuslaitoksen johto pitää koulutusta tärkeänä	3	5	4,65	,551
	11. Ohjeiden noudattamatta jättämisestä voidaan rangaista	4	5	4,68	,475
	20. En välitä, mitä muut ajattelevat ohjeiden noudattamisesta	1	4	1,58	,807

Taulukko 3. Havaittujen vaikutusmahdollisuuksien laskemiseen käytettyjen kysymysten keskiarvot ja – hajonnat toisen kyselytutkimuksen analyysissä.

Havaitut vaikutusmahdollisuudet	Kysymys	Minimi	Maksimi	Keskiarvo	Keskihajonta
	13. Kehittynyt tietotekniikka suojelee pelastuslaitosta tietoturva-uhilta	1	5	3,55	1,457
	14. Yksittäinen työntekijä voi parantaa tietoturvaa pelastuslaitoksessa	1	5	4,39	1,022

Taulukko 4. Havaitun käytön helppouden laskemiseen käytettyjen kysymysten keskiarvot ja – hajonnat toisen kyselytutkimuksen analyysissa.

	Kysymys	Minimi	Maksimi	Keskiarvo	Keskihajonta
Havaittu käytön helppous	17. Ohjeet ovat helposti saatavissa	1	5	3,26	,999
	18. Ohjeita on helppo noudattaa	2	5	3,61	,844
	19. Ohjeet ovat helposti ymmärrettävissä	2	5	3,74	,773

Taulukko 5. Havaitun koulutuksen hyödyllisyyden laskemiseen käytettyjen kysymysten keskiarvot ja – hajonnat toisen kyselytutkimuksen analyysissa.

	Kysymys	Minimi	Maksimi	Keskiarvo	Keskihajonta
Havaittu koulutuksen hyödyllisyys	2. Koulutus oli hyödyllistä	4	5	4,58	,502
	3. Tietoja voi hyödyntää työtehtävissä	4	5	4,55	,506
	4. Aihe oli ajankohtainen	3	5	4,71	,588
	5. Aihe toi lisätietoa	1	5	4,45	,888
	6. Työnantaja hyötyy koulutuksesta	4	5	4,58	,502
	7. Työntekijä hyötyy koulutuksesta	3	5	4,58	,564