Vaasan yliopisto
UNIVERSITY OF VAASA

NIINA KINNUNEN

Tietoturvaohjeistusten noudattamisen motivaatio ja sen muuttuminen

ACTA WASAENSIA 331

TIETOTEKNIIKKA 13

Esitarkastajat Professori Mikko Siponen
Tietojenkäsittelytieteiden laitos
PL 35 (Agora)
40014 JYVÄSKYLÄN YLIOPISTO

Professori (emer.) Pertti Järvinen
33014 Tampereen yliopisto

Julkaisija	**Julkaisupäivämäärä**	
Vaasan yliopisto	Syyskuu 2015	
Tekijä(t) Niina Kinnunen	**Julkaisun tyyppi** Monografia	
	Julkaisusarjan nimi, osan numero Acta Wasaensia, 331	
Yhteystiedot Vaasan yliopisto Teknillinen tiedekunta Tieto- ja tietoliikennetekniikka PL 700 65101 Vaasa	**ISBN** 978-952-476-636-4 (painettu) 978-952-476-637-1 (verkkojulkaisu)	
	ISSN 0355-7339 (Acta Wasaensia 331, painettu) 2323-9123 (Acta Wasaensia 331, verkkojulkaisu) 1455-7339 (Acta Wasaensia. Tietotekniikka 13, painettu) 2342-0693 (Acta Wasaensia. Tietotekniikka 13, verkkojulkaisu)	
	Sivumäärä 234	**Kieli** Suomi
Julkaisun nimike Tietoturvaohjeistusten noudattamisen motivaatio ja sen muuttuminen		

Tiivistelmä

Viranomaistahot ovat asettaneet tietoturvalle kunnianhimoisia tavoitteita. Työntekijät ovat tärkeässä asemassa yrityksen tietoturvan onnistumisessa. Motivaatio vaikuttaa työntekijöiden tapaan suhtautua työpaikkansa tietoturvaohjeisiin ja tapaan toimia ohjeiden mukaisesti. Koska työntekijän motivaatio on keskeistä yrityksen tietoturvan toteutumiselle ja yleisemminkin tietoturvan toteutumiselle, selvitetään tässä tutkimuksessa motivaation eri osatekijöiden vaikutusta tietoturvaohjeistusten noudattamiseen.

Tutkimuksen tavoitteena on selvittää miten työntekijöiden motivaatio tietoturvaohjeiden noudattamiseen syntyy ja muuttuu. Samalla selvitetään mitä tietoturvakriteerejä Suomessa julkaistut tietoturvaohjeet sisältävät, millä tasolla työntekijät pyrkivät noudattamaan tietoturvaohjeita ja erityisesti mitkä tekijät motivoivat työntekijöitä heidän pyrkiessä noudattamaan tietoturvaohjeistuksia. Tietoturvakriteerillä tarkoitetaan tässä tutkimuksessa yksittäisiä toimintoja, joilla pyritään varmistamaan tietoturvan toteutuminen yrityksessä.

Tutkimuksen teoreettisessa osassa käsitellään motivaatioteorioita ja tietoturvaa. Lisäksi kuvataan motivaation merkitystä työn ja työssä oppimisen tukena. Tutkimuksen empiirinen osa on tehty neljässä vaiheessa. Aluksi on tehty yhteenveto suomalaisille pk-yrityksille suunnatuista tietoturvaohjeistuksista. Kyseisen yhteenvedon ja tietoturvan kirjallisuuskartoituksen pohjalta on laadittu tietoturvakriteerit, joita on viimeisissä vaiheissa käytetty kvantitatiivisen ja kvalitatiivisen tutkimuksen tukena kyselyssä ja haastatteluissa.

Tutkimuksen lopputuloksena saadaan selville motivaation syntymiseen ja muuttumiseen vaikuttavia tekijöitä. Tulosten mukaan työntekijöitä motivoi merkittävästi oma usko tietoturvan toteuttamisen tärkeydestä. Tietoturvan noudattamisen taustalla voi olla myös toisen henkilön tai olosuhteiden aiheuttama vaatimus.

Asiasanat

tietoturva, motivaatio, ohjeistus

Publisher
University of Vaasa

Date of publication
September 2015

Author(s)
Niina Kinnunen

Type of publication
Monograph

Name and number of series
Acta Wasaensia, 331

Contact information
University of Vaasa
Faculty of Technology
Computer Science
P.O.Box 700
FI-65101 Vaasa, Finland

ISBN
978-952-476-636-4 (print)
978-952-476-637-1 (online)

ISSN
0355-7339 (Acta Wasaensia 331, print)
2323-9123 (Acta Wasaensia 331, online)
1455-7339 (Acta Wasaensia. Computer Science 13, print)
2342-0693 (Acta Wasaensia. Computer Science 13, online)

Number of pages
234

Language
Finnish

Title of publication
Motivation for following information security instructions and change therein

Abstract
Authorities set ambitious objectives for information security. In a company, employees have a significant effect on the level of information security. Motivation is important for the employees' actions. This research is an attempt to find out what is the influence of motivation to information security actions.

The objectives of this research are to find out how the motivation of the employees form and change while the employees are trying to follow information security instructions. At additional objective is to find out what information security criteria appear in literature and in instructions that are written especially for Finnish small and mid-size companies. This research also aims to find out to what level instructions are followed, and what motivates employees to follow information security instructions. In this research, information security criteria is taken to mean actions which aim at supporting information security in a company.

The theory is formed of motivation and information security. The relevance of both motivation and learning at work is handled. The research results are formed in four steps. The first is a summary of instructions. The results of this step are used in the last steps of quantitative and qualitative research with a questionnaire and interviews.

The result of this research is a set of issues that forms and changes motivation. The key finding is that employees are most significantly motivated if they believe in the importance of an information security action. Compliance with information security is also affected by factors of circumstance and colleagues at work.

Keywords
information security, motivation, instructions

ESIPUHE

Tutkimukseni aiheena on hallinnollinen tietoturva ja yritysten työntekijöiden motivaatio noudattaa yrityksen tietoturvaohjeita. Aihe on käytännönläheinen ja ihmiskeskeinen. Tehdessäni työtä viiden vuoden ajan on aihe ollut koko ajan esillä julkisuudessa.

Kiitän professori Merja Wannetta työni ohjauksesta. Yhteistyömme on jatkunut pitkään alkaen pro gradu -tutkielmani ohjauksesta. Vaikka väitöskirjaa tehdessäni on etäisyys työpisteidemme välillä ollut useita satoja kilometrejä, olen kokenut, että olen saanut ohjausta aina, kun olen sitä tarvinnut.

Kiitän professori Mikko Siposta ja professori (emeritus) Pertti Järvistä työni esitarkastuksesta. Teidän tarkat huomionne käsikirjoituksestani ja kommenttinne empiirisen osan parantamiseksi ovat auttaneet työni viimeistelyssä.

Kiitän tutkimuksessa yhteistyötä tehnyttä Oy Kaha Ab:tä ja erityisesti IT-osaston vastaavaa Sanna Kainulaista, joka toimi yrityksen yhteyshenkilönä. Oman työsi ohella sinulta löytyi aina aikaa tutkimuksen järjestelyille.

Kiitän Haaga-Helia tohtorikoulutusprojektin vetäjää, dosentti Tarja Römer-Paakkasta tuesta ja avusta työni eri vaiheissa. Sinun kanssasi keskustellessani heräsi ajatus motivaation käyttämisestä työni teoreettisessa osassa. Kiitän myös ystävääni Virpi Juppoa tuesta ja avusta työni eri vaiheissa, erityisesti työni viimeistelyssä.

Työnantajalleni Haaga-Helia ammattikorkeakoululle ja erityisesti esimiehelleni koulutusohjelmajohtaja Paavo Lehessalolle haluan esittää kiitokset tutkimustyöni mahdollistamisesta. Sinun osoittama tuki palkkatyöni järjestämiseksi tutkimustyön mahdollistavalla tavalla on ollut erittäin arvokasta. Ilman tätä tukea väitöskirjani tekeminen tässä elämäntilanteessa olisi jäänyt hyvin todennäköisesti kokonaan tekemättä. Järjestely on mahdollistanut myös sen, että täysipäiväisen työni ohella tehty tutkimustyö ei ole vienyt sekuntiakaan pois pienten lasteni elämästä, mistä olen kiitollinen.

Tohtorin tutkinto ei ole ollut minulle mikään pitkäaikainen unelma. Aloitin jatko-opinnot, koska pidin maisteriopinnoista ja pro gradun kirjoittamisesta. Unelma väitöskirjasta ja tohtorin tutkinnosta syntyi heti maisteriopintojen valmistuttua, mutta se heräsi uudelleen henkiin joulukuussa 2009, jolloin tajusin lukujärjestyksessäni olevan koko kevään yhden tyhjän arkipäivän. Siitä alkaen olen kirjoittanut väitöskirjaa yhtenä päivänä opetusviikossa, kaikkiaan 169 päivänä.

Väitöskirjan tekeminen on ollut mielenkiintoista. Se on ollut minulle mielekäs harrastus. Ajoittain se on kuitenkin ollut myös erittäin haastavaa ja välillä minäkin olen kokenut etenemisen ja luomisen tuskaa. Väitöskirjassa käsittelen keskeisesti motivaatiota. Minäkin koin käytännössä vahvasti motivaation merkityksen, kun aloitin käsikirjoituksen työstämisen uudelleen tammikuussa 2014 saatuani vahvistuksen, että ensimmäinen esitarkastus ei mennyt läpi. Toisessa esitarkastuslausunnossa todettiin, että työni painottaa käytäntöä huomattavan paljon. Sellainen minä olen, käytännön ihminen. Tutkimuksen ajatustyötä olen tehnyt mm. kymmenillätuhansilla ajokilometreillä, takkapuita tehdessä ja puutarhatöissä. Kaikenlainen hyötyliikunta on ollut minulle hyvää hapenottoa väitöskirjatyöhön etenkin silloin, kun eteneminen on ollut väliaikaisesti umpikujassa.

Äiti ja isä, Hilkka ja Erkki, te olette opettaneet minulle arvot, joille elämäni perustuu. Oppienne mukaisesti elämäni tukipilareita ovat mm. koulutus ja periksiantamattomuus. Neuvonne käydä kouluja ja oma esimerkillinen tapanne urakoida työt aina sisulla loppuun asti, on ollut minulle se perimmäisin voima saattaa tämä väitöskirja valmiiksi. Siksi haluan omistaa tämän työni erityisesti teille ja näin kiittää opettamistanne elämänarvoista ja jatkuvasta tuestanne ja rakkaudestanne.

Sisko ja veljet perheineen, koko perhe sen laajimmassa merkityksessä, ystävät, sukulaiset ja työkaverit, teidän mielenkiintonne ja kannustuksenne työni tekemiseen saa lämpimät kiitokset. Ystäväni Päivi, Virpi ja Riitta, omalla esimerkillänne te olette kannustaneet minua tässä työssä.

Oma rakas perheeni: Mikko, mitkään sanat eivät riitä kuvaamaan sitä kiitosta, jonka haluan osoittaa sinulle sinulta saamastani tuesta. Pilke silmäkulmassa esittämäsi kysymys, joko olen tohtori, on saanut minut hymyilemään kerta toisensa jälkeen. Kiitos kultarakas, ihan kohta olen tohtori. Noora ja Niko, te olette kaikkein tärkeimmät ja rakkaimmat. Nyt te olette vielä pieniä, mutta toivon, että tämä tekemäni työ voisi myöhemmin toimia teidän perimmäisimpänä voimana omassa elämässänne vastaantulevien haasteiden voittamisessa ja tavoitteiden saavuttamisessa. Minä ja isi olemme aina teidän tukenanne.

Mäntsälässä, kesäkuussa 2015

Niina Kinnunen

Sisällys

ESIPUHE VII

1 JOHDANTO 1
1.1 Aiheen esittely 3
1.2 Aikaisemman tutkimuksen puutteiden tai ristiriitojen esittely 4
1.3 Tutkimusongelman kuvaus 8
1.4 Tulokset 12
1.5 Tutkimuksen eteneminen 12

2 MOTIVAATIO JA OPPIMINEN 14
2.1 Motivaatioteorioita 14
2.2 Työssä oppiminen 21
2.3 Motivaatio työskentelyn ja työssä oppimisen tukena 25
2.4 Motivaatioviitekehys 29

3 TIETOTURVA 32
3.1 Keskeiset käsitteet 32
3.2 Tietoturvadokumentointi 47
3.3 Tietoturvasuunnittelu ja -riskit 56
3.4 Tietoturvakäyttäytyminen 72

4 TIETOTURVAOHJEISTAJIA JA -OHJEISTUKSIA 84
4.1 Suomen ja EU:n lainsäädäntö, kansainvälinen normisto sekä Euroopan verkko- ja tietoturvavirasto (ENISA) 84
4.2 ISO ja Suomen Standardisoimisliitto SFS: Tietoturvastandardit 87
4.3 Yritysturvallisuus EK Oy: Käytännön tietoturvallisuusopas pk-yrityksille 91
4.4 TIEKE Tietoyhteiskunnan kehittämiskeskus ry: Tietoturvaopas 92
4.5 Arjen tietoyhteiskunnan tietoturvallisuus -ryhmä: Kansallinen tietoturvastrategia 100
4.6 Elinkeinoelämän keskusliitto EK, sisäasiainministeriö ja puolustusministeriö: Kansallinen turvallisuusauditointikriteeristö (KATAKRI) 102
4.7 Viestintävirasto, CERT-FI ja NCSA-FI: Yrityksen tietoturvaopas 103
4.8 Teknologian tutkimuskeskus VTT 113
4.9 Valtionhallinnon tietoturvallisuuden johtoryhmä: VAHTI-ohjeistus 114

5 MOTIVAATIO TIETOTURVAKRITEERIEN NOUDATTAMISESSA 117
5.1 Hallinnollisen tietoturvan tietoturvakriteerien muodostaminen 117
5.1.1 Yleiset tietoturvakriteerit 118
5.1.2 Hallinnolliset tietoturvakriteerit 121
5.2 Kyselytutkimuksen toteutus 122
5.3 Tulokset tietoturvakriteerien noudattamispyrkimyksestä 124
5.3.1 Yleiset tietoturvakriteerit 124
5.3.2 Hallinnolliset tietoturvakriteerit 131

5.3.3 Yhteenveto: heikosti noudattamaan pyrityt tietoturvakriteerit 134
5.4 Ensimmäisen haastattelututkimuksen toteutus 136
5.5 Tulokset tietoturvakriteerien noudattamaan pyrkimisen motivaatiotekijöistä 139
5.6 Toisen haastattelututkimuksen toteutus 149
5.7 Tulokset motivaation syntymiseen ja muuttumiseen vaikuttavista tekijöistä tietoturvakriteerien noudattamisessa 151

6 KESKUSTELUA 156
6.1 Tulosten tieteellinen merkitys 156
6.2 Käytännön suositukset 167
6.3 Rajoitukset 168
6.4 Jatkotutkimusaiheet 173

LÄHTEET 175

LIITTEET 192

Kuviot

Kuvio 1. Motivaatioprosessi (Ruohotie 1998: 50). 17
Kuvio 2. Turvallisuusjohtamisessa huomioitavat yritysturvallisuuden osa-alueet (Yritysturvallisuus EK Oy 2009a; Heljaste ym. 2008: 28)... 41
Kuvio 3. Tietoturvaprosessin vaiheet (Laaksonen ym. 2006: 120)..... 44
Kuvio 4. Tietoturvakriteerien noudattamaan pyrkimisen motivaatiotekijät. 144
Kuvio 5. Yleisten tietoturvakriteerien noudattamaan pyrkimisen motivaatiotekijät. 145
Kuvio 6. Hallinnollisten tietoturvakriteerien noudattamaan pyrkimisen motivaatiotekijät. 147

Taulukot

Taulukko 1. Tutkimuksen kokonaisuus. 10
Taulukko 2. Hyvän tietohallintotavan vaatimukset (Laaksonen ym. 2006: 123–124). 43
Taulukko 3. Tiedon luokittelun merkintätapa (Viestintävirasto 2010f)..... 60
Taulukko 4. Viestintäviraston tietoturvaohjelma (Viestintävirasto 2010d)... 62
Taulukko 5. Tietoturvakäyttäytymisen artikkeleita. 73
Taulukko 6. Tietoturvakriteerit työntekijälle asetettavista yleisistä tietoturvavaatimuksista. 125
Taulukko 7. Yrityksen yleistä toimintaa koskevat yleiset tietoturvakriteerit.125
Taulukko 8. Yrityksen yleistä toimintaa koskevat yleiset tietoturvakriteerit eriteltynä. 126
Taulukko 9. Yrityksen toimintaa koskevat yleiset tietoturvakriteerit. 126
Taulukko 10. Tietoja koskevat tietoturvakriteerit. 127
Taulukko 11. Tietoja koskevat tietoturvakriteerit eriteltynä. 128
Taulukko 12. Työntekijän oikeuksia ja velvollisuuksia koskevat yleiset tietoturvakriteerit. 128
Taulukko 13. Työntekijän oikeuksia ja velvollisuuksia koskevat yleiset tietoturvakriteerit eriteltynä. 129
Taulukko 14. Työntekijän oikeuksia ja velvollisuuksia koskevat tietoturvakriteerit. 130
Taulukko 15. Työntekijän oikeuksia ja velvollisuuksia koskevat tietoturvakriteerit eriteltynä. 130
Taulukko 16. Yleiset hallinnolliset tietoturvakriteerit. 131
Taulukko 17. Yleiset hallinnolliset tietoturvakriteerit eriteltynä. 132
Taulukko 18. Yrityshallinnon tietoturvakriteerit eriteltynä. 132
Taulukko 19. Hallinnolliset tietoturvakriteerit. 133
Taulukko 20. Hallinnolliset tietoturvakriteerit eriteltynä. 133
Taulukko 21. Hallinnolliset toteuttamisen tietoturvakriteerit eriteltynä. 134
Taulukko 22. Kyselyn tulosten yhteenveto: heikosti noudattamaan pyrityt yleiset tietoturvakriteerit. 135

Taulukko 23. Kyselyn tulosten yhteenveto: heikosti noudattamaan pyrityt hallinnolliset tietoturvakriteerit. 136
Taulukko 24. Yleisten tietoturvakriteerien noudattamaan pyrkimisen motivaatiotekijät. 146
Taulukko 25. Hallinnollisten tietoturvakriteerien noudattamaan pyrkimisen motivaatiotekijät. 148

1 JOHDANTO

Joulukuussa 2008 hyväksyttiin Valtioneuvoston periaatepäätös kansallisesta tietoturvastrategiasta, jossa Suomi nähdään vuonna 2015 tietoturvan edelläkävijämaana maailmassa (Liikenne- ja viestintäministeriö 2010c; Liikenne- ja viestintäministeriö 2008). Valtion hallinnolla ei ole kuitenkaan täysin selkeää kuvaa tietoturvaohjauksen tulevaisuudesta. Viestintäministeri Lindén esitti 8.2.2011 julkaistussa tiedotteessa, että julkishallinnon tietoturva tulisi keskittää Viestintävirastolle (Liikenne- ja viestintäministeriö 2011). Tietoturvasuunnittelun vastuun keskittämistä esitetään myös 21.10.2010 julkaistussa Helsingin Sanomien pääkirjoituksessa ”Valtiollisessa tietoturvassa on suuria puutteita”, jossa todetaan, että hajautettu tietoturvan ohjaus on riski etenkin häiriö- ja poikkeustilanteissa. Pääkirjoituksessa mietitään jopa onko olemassa tarve perustaa turvallisuusministeriö ohjaamaan tietoturvaa kokonaisvaltaisesti. (Helsingin Sanomat 2010.) Lisäksi yritykset kaipaavat viranomaisilta ohjeistuksia sekä selviä suosituksia siitä, mitä toimenpiteitä yrityksessä tulisi ja saisi tehdä, jotta tietoturvan ylläpitäminen ja parantaminen toteutuisi. Lisäksi yritykset haluavat varmistaa toimenpiteiden lainmukaisuuden ja tehokkuuden palvella osapuolten tavoitteita. (Laaksonen, Nevasalo & Tomula 2006: 21.)

Tilastokeskuksen (2006: 57, 80–81) mukaan Suomessa oli vuonna 2005 eniten (98 %) Internetiä käyttäviä yli 10 työntekijän yrityksiä EU-maissa. EU-maiden keskiarvo oli tuolloin 91 %. Samassa tutkimuksessa kävi ilmi, että jo tuolloin 99 % suomalaisista yli 10 työntekijän yrityksistä käytti ainakin joitakin tietoturvan välineitä, kuten virustorjuntaohjelmaa, palomuuria, varmuuskopiointia ja turvattua palvelinyhteyttä.

Keskuskauppakamarin ja Helsingin seudun kauppakamarin (2008: 15, 53) 1286 yritykselle tekemässä tutkimuksessa selvisi, että 79 %:a tutkimukseen osallistuneista yrityksistä käsitteli turvallisuusasioita työntekijöiden kanssa ja työntekijät pystyivät vaikuttamaan turvallisuutta koskevaan päätöksentekoon 86 %:ssa yrityksistä. 40 % yrityksistä antoi työntekijöille turvallisuuskoulutusta ja 56 %:ssa turvallisuusasiat olivat osa perehdyttämiskoulutusta. 75 %:ssa yrityksistä kannustettiin työntekijöitä kertomaan turvallisuusasioiden puutteista. Tutkimuksessa selvisi myös, että yritysjohto oli henkilökohtaisesti mukana turvallisuuden kehittämisessä 85 % vastanneista 1286 yrityksessä. Tutkimukseen vastanneista 1286 yrityksestä 784 yritystä (61 %) ilmoitti panostavansa tietoturvaan tulevaisuudessa sen hetkistä enemmän (Keskuskauppakamari & Helsingin seudun kauppakamari 2008: 61–62). Tutkimuksen tulosten perusteella voidaan nähdä, että yrityksissä on pääpiirteittäin positiivinen käsitys yrityksen tietoturvan tilasta. Tietoturvassa nähdään kuitenkin myös parannettavaa. Tietoturva-asioiden sisällyttämisessä työhön-

tuloperehdytykseen ja tietoturvakoulutuksessa yleisesti nähdään noin puolella yrityksistä parannettavaa. Nämä molemmat kuuluvat yrityksen hallinnollisesta tietoturvasta huolehtimiseen.

Ernst & Youngin (2008) tekemän tutkimuksen mukaan yritykset pyrkivät yhä useammin parantamaan tietoturvaa suojellakseen yrityksen mainetta. Tietoturvan parantamisessa yritysten tulisi panostaa yhä enemmän yrityksen sisäisiin uhkiin, yhteistyökumppaneiden aiheuttamiin tietoturvauhkiin ja yksityisyyden suojan turvaamiseen. Tekniset ratkaisut eivät pelkästään riitä, vaan myös työntekijöiden tietoturvakouluttamisella on yhä merkittävämpi rooli. Heikkous tietoturvassa johtuu usein ihmisistä. Omien työntekijöiden lisäksi tulisi varmistaa yhteistyökumppaneiden sitoutuminen tietoturvan ylläpitämiseen.

Ernst & Youngin (2009) tekemän tutkimuksen mukaan sisäiset ja ulkoiset tietoturvariskit lisääntyivät vuodesta 2008 vuoteen 2009. Se korostaa liiketoiminnan kannalta kriittisen tiedon suojaamisen merkitystä yritysten tietoturvassa. Tutkimustuloksista selviää, että yritysten suurimpia tietoturvariskejä ovat äskettäin irtisanottujen työntekijöiden mahdollinen kosto yritykselle, kuten tietovarkaus tai tietojenkäsittelyjärjestelmien sabotointi. Myös riittämättömät tietoturvabudjetit ja resurssit aiheuttavat riskejä tietoturvalle.

Computer Security Instituten (2009) vuosittain tekemässä Computer Crime and Security Survey -tutkimuksessa 110 vastaajaa (25 %) 443 vastaajana olleesta tietoturva- ja tietojenkäsittelyammattilaisesta totesivat, että yli 60 % yrityksen taloudellisista tappioista johtui yrityksen työntekijöiden aiheuttamista tahattomista toimista. Tahattomista työntekijöiden toimista aiheutunutta taloudellista tappiota ilmoitti tapahtuneen kaikkiaan 65,8 % vastaajista (291 vastaajaa). Tahallisista työntekijöiden aiheuttamista taloudellisista tappioista ilmoitti 43,2 % vastaajista (191 vastaajaa). Malware-haittaohjelman hyökkäyksen kohteeksi joutuminen oli ollut vastaajien keskuudessa suurin ongelma, kun 285 vastaajaa (64,3 %) ilmoitti tämän tapahtuneen omassa yrityksessä. 187 vastaajaa (42,2 %) oli joutunut kannettavan tietokoneen tai mobiililaitteen varkauden uhriksi. Kolmanneksi suurin ongelma oli yrityksen sisällä tapahtunut Internet-yhteyden tai sähköpostin sääntöjenvastainen käyttö työntekijöiden toimesta, minkä ilmoitti tapahtuneen 131 vastaajaa (29,7 %). Melkein yhtä monta vastaajaa (129 vastaajaa eli 29,2 %) ilmoitti palvelujen estossa tapahtuneista tietoturvarikkomuksista. Tutkimuksen tulosten perusteella voidaan nähdä, että työntekijän tahattomasta toiminnasta aiheutuvat tietoturvahaitat ovat yleisempiä kuin tahallisesta toiminnasta aiheutuvat haitat. Tahattoman toiminnan merkityksen ymmärtämiseen voidaan merkittävästi vaikuttaa hallinnollisen tietoturvan keinoin.

Ernst & Youngin (2010) tekemän vuotuisen kansainvälisen Global Information Security Survey -tutkimuksen mukaan yritykset eivät koe uusien teknologioiden, kuten sosiaalisen median, aiheuttamien tietoturvariskien selvittämistä tärkeänä eivätkä ne huolehdi näistä riskeistä, vaikka yritykset ovat tiedostaneet uusista teknologioista aiheutuvien tietoturvariskien lisääntymisen. Työntekijöiden liikkuvuus ja sen mukanaan tuoma etätyöskentely lisäävät haasteita yrityksen tietoturvalle. Tutkimuksen mukaan työntekijöiden tietoturvatietoisuutta pidetään riittämättömänä ja tietoturvaan asennoitumista huolestuttavana. Tietoturvatietoisuuden lisääminen koulutuksella on yrityksille yhä tärkeämpää. Liikkuvassa työssä merkittävin rooli on kannettavan tietokoneen sijaan käyttäjällä. Tutkimuksen mukaan vuonna 2011 yritykset aikovat panostaa tietovuotojen estämiseen sekä tiedon häviämisen ja tuhoutumisen torjumiseen.

1.1 Aiheen esittely

Viranomaistahojen tietoturvalle asettamat tavoitteet ovat kunnianhimoiset. Tavoitteiden jalkauttaminen ruohonjuuritasolle ei kuitenkaan automaattisesti vastaa asetettua tavoitetta. Yrityksissä tietoturvan toteutumisen tasoon vaikuttavat eniten työntekijät, jotka voidaan nähdä tietoturvan suurimpana uhkana (Heljaste, Korkiamäki, Laukkala, Mustonen, Peltonen ja Vesterinen 2008: 69). Culnan ja Williams (2009) sekä Myyry ja muut (2009) toteavat, että työntekijät eivät noudata tietoturvaohjeita, vaikka he tietävät niiden olemassaolosta. Työntekijän toimintaan liittyy keskeisesti motivaatio. Tästä syystä tässä tutkimuksessa selvitetään motivaatiotekijöiden vaikutusta tietoturvan toteuttamisessa.

Tämän väitöskirjan aiheena on hallinnollinen tietoturva ja se sijoittuu tietojärjestelmätieteen alalle. Väitöskirjan peruskäsitteitä ovat *tietoturva*, *tietoturvakriteeri* ja *motivaatio*. Tekniikan sanastokeskus (2002) määrittelee *tietoturvan* ”*järjestelyiksi, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus*”. Määritelmässä käytettävyydellä tarkoitetaan, että tieto on saatavilla halutuille henkilöille haluttuna aikana nopeasti ja oikeassa muodossa. Eheydellä tarkoitetaan, että tieto on paikkansapitävää ja virheetöntä. Luottamuksellisuudella tarkoitetaan, että tietoon pääsevät käsiksi vain ne, joilla siihen on oikeus. (Tekniikan sanastokeskus 2002.) Tietoturvan käsitettä on avattu tarkemmin luvussa 3. *Tietoturvakriteerillä* tarkoitetaan tässä tutkimuksessa sellaisia nimettyjä yksittäisiä toimenpiteitä, joilla pyritään varmistamaan tietoturvan toteutuminen yrityksessä. Tähän tarkoitukseen ei ole olemassa yleisesti käytössä olevaa yhtä termiä. Elinkeinoelämän keskusliitto EK julkaisi vuonna 2009 Kansallisen turvallisuusauditointikriteeristön tietoturvalle (liite 1), johon viitaten tässä tutkimuksessa käytetään yksittäisestä toimenpiteestä yksikkömuotona termiä tietoturvakriteeri. Tie-

toturvakriteerien perusteella olisi mahdollista testata yrityksen tietoturvan taso. *Motivaatio* virittää ja ohjaa ihmisen käyttäytymistä (Ruohotie 1998: 35). Motivaation käsitettä avataan tarkemmin luvussa 2.

1.2 Aikaisemman tutkimuksen puutteiden tai ristiriitojen esittely

Tietoturvan tutkimus on melko varhaisessa vaiheessa. Tietoturvan tutkimuksen tarvetta perustellaan mm. riskien tiedostamisen ja ennaltaehkäisemisen tarpeella. (Helenius 2005.) Tietoturvatutkimuksen yksi tavoitteista on tietoturvan parantaminen yrityksissä. Tietoturvatutkimuksen haasteena on sopivien yleisten teoreettisten viitekehysten puuttuminen (Karjalainen 2011: 27; Puhakainen & Siponen: 2010). Moody (2011: 19) toteaa, että suurin osa turvallisuustutkimuksesta liittyy informaatioteknologian resurssien väärinkäyttöön sen sijaan, että olisi selvitetty miksi ihmiset jättävät tarkoituksella huomioimatta tietoturvan toiminnassaan. Moody on myös todennut, että tietoturvatutkimuksessa motivaation selittämiseen pyrkivää tutkimusta ei ole tehty. Hän tutki tietoturvakäyttäytymisen syitä erilaisista teoreettisista lähtökohdista. Tutkimuksella selvitettiin tietoisen tietoturvaohjeiden laiminlyönnin syitä. Nykäsen (2011: 14) mukaan tietoturvakäyttäytymiseen liittyvässä tutkimuksessa on käytetty lähinnä käyttäytymistieteisiin pohjautuvia teorioita. Vaikka yritysten tietoturvatason tilanne on yleisesti tiedossa, esimerkiksi tietoturvakoulutuksen merkitystä työntekijän tietoturvakäyttäytymisessä on tutkittu erittäin vähän. Hän tutki tietoturvakoulutuksen vaikutusta yksilön tietoturvakäyttäytymiseen. Tulosten mukaan koulutuksessa tulee pyrkiä vaikuttamaan yksilön tapoihin ja käyttäytymiseen sekä yksilön oman toiminnan seurausten vastuuttamiseen.

Cox, Connolly ja Currall (2001) tutkivat keskustelun, muistilistojen ja Internet-pohjaisten ohjeiden vaikutuksia ihmisen tietoturvakäyttäytymiseen. Tutkimuksessa todettiin, että ihmisen käyttäytyminen on keskeinen ja kriittinen tekijä tietoturvalle. Tutkimuksen tuloksena todettiin, että kaikki kolme tekijää (keskustelu, muistilistat ja Internet-pohjaiset ohjeet) ovat merkityksellisiä tietoturvatietoisuuden parantamiseksi.

Partanen (2005) tutki tietoturvaa johdon ja organisoinnin näkökulmasta. Hän selvitti tutkimuksessaan mitä asioita yrityksen tietoturvassa olisi huomioitava, jotta se olisi kunnossa. Tutkimuksessa tehtiin tietoturvan tilan kartoitus kyselynä 32 pohjoiskarjalaiselle yritykselle. Tutkimuksen tuloksena selvisi, että parhaiten yritykset huolehtivat ohjelmisto- ja laitteistoturvallisuudesta. Paremmin pitäisi huomioida henkilöstö- ja hallinnollinen turvallisuus. Puhakaisen (2006) tutkimukses-

sa selvitettiin, miksi yritysten työntekijöille luotuja tietoturvasäännöksiä ei noudateta, vaan yrityksessä havaitaan toistuvasti eritasoisia laiminlyöntejä. Tutkimuksen tuloksissa selvisi, että laiminlyöntejä tapahtuu, koska yrityksen johto sitoutuu huonosti tietoturvasäännöstöön, säännöstön käyttöä motivoidaan yrityksessä heikosti ja tietoturvasäännöstön koulutus suunnitellaan ja toteutetaan huonosti. Säännöstössä ilmeni myös puutteita, jotka vaikuttivat säännöstön noudattamiseen vähentävästi. Tuloksissa todettiin lisäksi, että yritysten tietoturvatoimenpiteet painottuvat yhä liikaa tekniikkaan ja, että hallinnollisilla tietoturvatoimenpiteillä olisi mahdollista merkittävästi kehittää yritysten tietoturvaa. Tutkimuksessa tieto ja sen tunnistaminen nähtiin keskeiseksi osaksi tietoturvaa.

Myyry ja muut (2009) selvittivät, että moraalisten perustelujen vaikutusta tietoturvaohjeiden noudattamiselle ei ole tutkittu käytännössä. Herath ja Rao (2009a) ovat todenneet, että viimeaikaisten tutkimusten mukaan loppukäyttäjillä on erilaisia ajatuksia turvallisuudesta. Tutkimuksessaan he kehittivät teorian, joka perustuu rangaistuksen kannustavaan vaikutukseen, painostukseen ja työntekijän tehokkaan toiminnan huomioimiseen. Tutkimuksessa todettiin, että tietoturvakäyttäytymiseen voidaan vaikuttaa sekä sisäisen että ulkoisen motivoinnin keinoin vaatimalla noudattamaan sääntöjä ja seuraamalla toimintaa. Tulosten mukaan tietoturvaohjeiden noudattamispyrkimykseen vaikutettaessa työntekijän tehokkaan toiminnan huomioimisella on tärkeä rooli sisäisessä motivoinnissa. Rangaistuksen saamisella kiinni jäämisestä oli niin ikään vahva motivoiva vaikutus. Tulosten mukaan negatiivisen vaikutuksen tietoturvakäyttäytymiseen aiheutti rangaistuksen ankaruus.

Ku, Chang ja Yen (2009) tutkivat yleisesti tunnetun tietoturvan hallintajärjestelmän (ISMS) käyttöä erityisesti Taiwanissa. Tutkimuksessa selvitettiin tietoturvan hallintajärjestelmän onnistumiseen vaikuttavia tekijöitä. Tutkimuksen tuloksena todettiin, että hallintajärjestelmän käyttöönotossa tärkeitä motivaatiotekijöitä ovat aiemmat onnistuneet kokemukset, dokumenttien saatavuus, kustannusten rajaaminen, organisaation oppiminen ja organisaatiokulttuuri. Keskeisimpinä hallintajärjestelmän onnistumiseen vaikuttavina tekijöinä he nimeävät aiemman kokemuksen tietoturvastandardeista, dokumentaation tason ja standardinmukaisuuden sekä ohjeiden ymmärtämisen tason. Lisäksi he näkevät keskeisinä vaikuttavina tekijöinä riskienhallinnan menetelmät, ylimmän johdon tuen, organisaatiokulttuurin, infrastruktuurin tarkkailun, tietoturvatietoisuuden sekä koulutuksen olemassa oleviin toimintatapoihin ja tapojen yhteensopivuuden.

Useat aikaisemmat tutkimukset ovat osoittaneet, että suomalaisten yritysten tietoturvan taso ei ole kovinkaan hyvä. Erityisesti henkilöstö- ja hallinnollinen turvallisuus tulisi huomioida yrityksissä paremmin. (mm. Partanen 2005). Yritysten

yksi keskeinen ongelma on, että työntekijät laiminlyövät yrityksen tietoturvakäytäntöjä. Työntekijöiden tietoturvakäyttäytymisen syyt on tärkeää ymmärtää. (Karjalainen 2011.) Yritysten tietoturvaohjeita noudatetaan heikosti. Työntekijät eivät tiedä toimivansa väärin eivätkä ymmärrä tahallisen tai tahattoman toimintansa aiheuttamia seuraamuksia. Työntekijöiden heikko tietoturvatietoisuus on merkittävin syy tietoturvaväärinkäytöksille. (Siponen, Pahnila & Mahmood 2007; D'Arcy, Hovav & Galletta 2009.) Tianin, Shenin ja Wangin (2010) tutkimuksessa tarkasteltiin Internetin käytön määrää ja yleisyyttä työpaikalla omiin henkilökohtaisiin käyttötarpeisiin Kiinassa. Tulosten mukaan yrityksen tietokoneita käytetään työhön liittymättömään omaan henkilökohtaiseen tarpeeseen, mikä aiheuttaa haittaa yrityksen toiminnalle (mm. Anandarajan 2002; Tian, Shen & Wang 2010). Samanlaisia tuloksia on saatu myös muissa tutkimuksissa. Työhön liittymätön Internetin käyttö häiritsee merkittävästi työntekijän keskittymistä ja työntekoa (mm. Lim, Teo & Loo 2002; D'Arcy & Hovav 2007). Lim, Teo ja Loo (2002) tutkivat Internet-kyselyllä 188 työntekijää tavoitteena selvittää miten usein ja miksi he käyttävät Internetiä työhön kuulumattomiin tarkoituksiin. Tulosten mukaan vähintään puolet työntekijöistä käytti useita kertoja viikossa useista eri syistä Internetiä työhön kuulumattomiin tarkoituksiin. Myös sähköpostia käytettiin laajasti työhön kuulumattomaan viestintään. D'Arcy ja Hovav (2007) puolestaan tutkivat neljän tietoturvatoimenpiteen vaikutusta tietojenkäsittelyjärjestelmien väärinkäytön ehkäisemiseksi. Tutkitut tietoturvatoimenpiteet olivat tietoturvaohjeet, tietoturvaohjelma, tietokoneiden valvonta ja tietoturvasovellusten käyttö. Internet-kyselyyn vastasi 579 käyttäjää. Tulosten mukaan tietoturvaohjeet olivat tutkituista tietoturvatoimenpiteistä tutuin ja vastaavasti tietoturvaohjelma vierain. Tulosten mukaan yritykset käyttävät resursseja tietoturvaohjeiden luomiseen, mutta yritykset eivät koulutuksissa tuo esille miksi ohjeiden noudattaminen on tärkeää. Koulutus olisi kuitenkin tehokas keino väärinkäytön vähentämiseen.

Kull (2012) tutki 29 Euroopan maan tietotekniikka-alalle asettamia sääntövaatimuksia. Hän selvitti tutkimuksessaan yrityksen tietotekniikan turvallisuuden määrää tarpeen ja riittävyyden lähtökohdista. Tutkituissa maissa tietoturvaan liittyen oli määritelty ainoastaan sääntövaatimukset tietoturvapolitiikalle. 14 maassa sääntövaatimukset oli määritelty perusteellisesti ja kahdessa maassa jotenkuten. Seitsemässä maassa ei mainittu tietoturvapolitiikkaa säännöissä lainkaan. Seuraavaksi parhaiten oli määritelty sääntövaatimukset pääsynhallinnalle. Tutkimuksen mukaan suomalaisten viranomaisten yrityksille tarjoamia tietoturvaohjeistuksia ei ole tutkittu tieteellisesti lainkaan. Tutkimuksen tuloksena syntyi määrittely ja menetelmä tietotekniikan valvonnalle.

Puhakainen (2006) on todennut, että työntekijät mieltävät tietoturvan yhä teknisenä asiana, mikä näkyy tietoturvatoiminnan keskittymisellä teknisiin ratkaisuihin.

Yrityksissä ei ymmärretä työntekijän tietoturvatietoisuuden merkitystä. Kuitenkin, tietoturvatietoinen ja tietoturvan toteuttamiseen motivoitunut työntekijä huomaa yrityksen toimintaa uhkaavat epäkohdat tietoturvassa sekä haluaa kehittää ja parantaa omaa työskentelyään ja tietoturvakäyttäytymistään. Colwill (2009) ja Sarkar (2010) ovat tutkineet yrityksen sisältä tulevia uhkia tietoturvalle. Molemmissa tutkimuksissa todettiin, että tietoturvaa ja erityisesti yrityksen sisältä tulevia uhkia ei pystytä ratkaisemaan pelkästään teknisillä ratkaisuilla. Colwillin (2009) tutkimuksen oleellisimpana tuloksena on, että tietoturvan riskianalyyseissä ja ohjeiden noudattamisen hallinnoimisessa tulee erityisesti kiinnittää huomiota työntekijöihin ja muihin yrityksen sisällä oleviin tahoihin. Tekniset ratkaisut tulee suunnitella, toteuttaa ja ylläpitää huomioiden ihmisen käyttäytyminen. Sisäpiiriläisten aiheuttamille tietoturvauhkille tulee pyrkiä luomaan ennaltaehkäiseviä toimenpiteitä ja mittareita. Tulosten mukaan tietoturvauhkia tulee ennaltaehkäistä tietoturvakoulutuksella, tietoturvatietoisuuden lisäämisellä, työntekijöiden ja sidosryhmien tietoturvan seurannalla sekä kiinnittämällä huomio ihmisiin. Sarkar (2010) puolestaan näkee sisältä tulevat tietoturvauhat epäselvempinä ja hämmentävämpinä kuin muut tietoturvauhat. Yrityksissä tulisikin ensimmäisenä määritellä sisältä tulevat uhat. Sen jälkeen pystytään määrittelemään myös muiden uhkien todennäköisyys. Tutkimuksen tuloksena ehdotetaan, että sisäisten uhkien ennustaminen tulisi tehdä arvioimalla kolmea tahoa: teknistä toteutusta, tietoturvajärjestelyjä ja ihmisen käyttäytymistä. Yritysten tulisi parantaa turvallisuutta ja paineensietokykyä sisäiset uhat huomioiden niin, että sisäisten uhkien toteutumisesta on mahdollista selviytyä.

Useissa tutkimuksissa (mm. Aytes & Connolly 2003; Puhakainen 2006; Siponen, Pahnila & Mahmood 2007) on osoitettu, että parantamalla työntekijöiden tietoturvatietoisuutta voidaan vaikuttaa työntekijän motivaatioon ja sitä kautta tietoturvakäyttäytymiseen. Spearsin ja Barkin (2010) tutkimuksessa todetaan, että käyttäjien ottamisella mukaan tietoturvan riskienhallintaan lisätään tietoturvatietoisuutta. Samalla pystytään tehokkaammin yhdistämään tietoturvariskien hallinta liiketoimintaympäristöön. Näillä keinoilla kehitetään tietoturvan hallintaa sekä saavutetaan parempia tuloksia. Tutkimusaineisto kerättiin kyselyllä 228 henkilöltä. Tutkimuksen mukaan, vaikka käyttäjät nähdään usein tietoturvan heikoimpana lenkkinä, voivat käyttäjät olla tietoturvalle tärkeitä, koska heiltä saadaan liiketoiminnasta tietoja, joiden perusteella pystytään kehittämään tehokkaampia tietoturvatoimintoja. Tutkimuksesta selviää myös, että käyttäjien ottamisella mukaan tietoturvariskienhallintaan, käyttäjät sitoutuvat suojelemaan liiketoiminnalle merkittäviä tietoja.

Siponen ja Vance (2010) ovat todenneet, että tietoturvaohjeiden noudattamatta jättäminen on iso haaste yritysten tietoturvajohdolle. Perinteisesti tietoturvaohjei-

den viitekehyksenä on käytetty peloteteorioita. Peloteteorian keskeinen ajatus on, että seuraamusten pelko estää toimimasta tietyllä tavalla, esimerkiksi rangaistuksen pelko estää rikoksia. Siponen ja Vance käyttivät tutkimuksessaan kuitenkin neutralisoimisteoriaa. Neutralisoimisteorian keskeinen ajatus on, että henkilön lainvastaisen käyttäytymisen taustalla on jokin neutralisoiva tekijä, jolla toiminnan syitä voidaan selittää. Siposen ja Vancen tutkimuksen tulosten mukaan neutralisoiminen tulisi huomioida merkittävänä tekijänä, kun yrityksessä kehitetään ja otetaan käyttöön tietoturvaohjeita ja -käytänteitä. Jotta työntekijät saadaan noudattamaan tietoturvaohjeita, on tietoturvaohjeiden vastattava työntekijän työtehtäviä ja työntekijän on ymmärrettävä tietoturvaohjeiden sisältö ja merkitys suhteessa omiin työtehtäviinsä (Puhakainen 2006; Pahnila, Siponen & Mahmood 2007; Siponen, Pahnila & Mahmood 2007; Puhakainen & Siponen 2010; Siponen & Vance 2010; Vance 2010). Huomattavaa on myös, että Höne ja Eloff (2002a) ovat tutkimuksessaan todenneet, että ohjeistukset sisältävät usein termejä, jotka ovat vaikeasti ymmärrettäviä. Ohjeet usein myös kirjoitetaan liian teknisestä näkökulmasta. Heidän mielestään on yleisesti tiedossa, että tietoturvapolitiikka on yksi tärkeimmistä välineistä, kun yrityksessä noudatetaan ja varmistetaan tietoturvaa tehokkaasti.

1.3 Tutkimusongelman kuvaus

Aikaisemmissa tutkimuksissa on osoitettu, että suomalaisten yritysten tietoturvan taso ei ole kovin hyvä ja siinä on parannettavaa. Tutkimuksissa on todettu, että yritysten tulisi tietoturvassa kiinnittää huomio erityisesti hallinnolliseen tietoturvaan. Yrityksissä tulisi huomioida työntekijä suurimpana tietoturvauhkana, ja siksi lisätä työntekijöiden tietoturvatietoisuutta. Tietoturvatietoisuudelle asetettavia vaatimuksia ei ole tutkittu suomalaisten viranomaistahojen tietoturvaohjeiden kontekstissa. Tällaisen analyysin tekeminen on tärkeää ja hyödyllistä yrityksille, koska yrityksillä ei ole välttämättä aikaa käydä läpi laajoja dokumentteja. Tutkijoille ja tietoturvan kehittäjille tällaisella analyysillä halutaan osoittaa viranomaisten ohjeistusten nykytila.

Useissa tietoturvatutkimuksissa on osoitettu motivaation yhteys tietoturvakäyttäytymiseen. Tutkimuksissa on myös osoitettu, että työntekijöiden tietoturvakäyttäytymiseen pystytään vaikuttamaan motivoimalla työntekijöitä. Motivaation taustalla oleviin tekijöihin kohdistuvaa tietoturvatutkimusta on tehty epäsuorasti ja hyvin vähän. Tietoturvatutkimusta, joka kohdistuu tietoturvan noudattamisen motivaation syntymiseen ja erityisesti muuttumiseen vaikuttaviin tekijöihin, ei ole tehty lainkaan. Tällainen tutkimus on tärkeää, jotta ymmärrettäisiin työntekijän

käyttäytymistä ja tietoturvan parantamiseen käytettäisiin työntekijöitä tehokkaimmin motivoivia tekijöitä.

Tämän tutkimuksen *tutkimusongelma* on löytää ymmärrystä tietoturvan noudattamisesta ja motivaation roolista tietoturvan noudattamisessa, jotta pk-yrityksissä voitaisiin löytää tehokkaita työkaluja tietoturvan ylläpitoon. Tutkimuksen *tavoitteena* on selvittää millä tasolla työntekijät pyrkivät noudattamaan tietoturvakriteerejä ja mitkä tekijät motivoivat työntekijöitä heidän pyrkiessä noudattamaan tietoturvakriteerejä. Erityisesti tutkimuksen tavoitteena on selvittää mitkä tekijät vaikuttavat motivaation syntymiseen ja muuttumiseen tietoturvakriteerien noudattamisessa. Tavoitteena on myös selvittää mitä tietoturvakriteerejä Suomessa julkaistut ohjeet sisältävät.

Tutkimuksessa käsitellään motivaatiota. Motivaatiota tarkastellaan erityisesti työskentelyn ja työssä oppimisen tukena. Motivaation käsittelyssä keskitytään motivaatioon vaikuttavien tekijöiden kuvaamiseen. Tutkimuksen *menetelmänä* käytetään empiria-vetoista kvantitatiivista ja kvalitatiivista tutkimusta. Tutkimuksessa on kuvaileva lähestymistapa. *Tutkimusaineisto* muodostuu dokumenttiaineistosta sekä kyselyllä ja haastatteluilla kerättävistä aineistoista. Ensimmäinen tutkimusaineisto on dokumenttiaineisto, joka muodostetaan pk-yrityksille suunnatuista tietoturvaohjeistuksista. Näiden analysointiin käytetään dokumenttianalyysiä. Tulosten pohjalta laaditaan kvantitatiivinen kysely, jolla muodostetaan toinen tutkimusaineisto. Sen tulosten pohjalta laaditaan pääosin kvantitatiivinen haastattelu, jolla kerätään kolmas tutkimusaineisto. Tämän aineiston keruussa käytetään myös kvalitatiivista menetelmää. Tulosten pohjalta laaditaan vielä toinen haastattelu, jolla kerätään viimeinen tutkimusaineisto. Tämä haastattelu on kvalitatiivinen. Kvalitatiivisessa tutkimuksessa aineistolla pyritään tekemään mahdolliseksi käsitteellinen ymmärrys tutkittavasta ilmiöstä, josta pyritään lisäksi rakentamaan teoreettinen näkemys (Eskola & Suoranta 2005, 62–63). Tuomi ja Sarajärvi (2009, 92) lisäävät, että tutkimuksen viimeisessä vaiheessa tuloksia tulkitaan ja niistä tehdään johtopäätökset. Tämän tutkimuksen metodologinen näkökulma on kuvaileva. Tutkimuksen tutkimuskysymykset, menetelmät ja aineisto sekä vastausten sijoittuminen tutkimuksessa on esitetty taulukossa 1.

Taulukko 1. Tutkimuksen kokonaisuus.

Tutkimuskysymykset	Menetelmä ja aineisto	Luku
Tietoturvaohjeistusten sisältö ja kriteerien muodostamisen taustatyö 1. Mitä tietoturvakriteerejä Suomessa julkaistut ohjeet sisältävät?	**Dokumenttianalyysi** Tietoturvakirjallisuus ja tietoturvaohjeistukset	III, IV, V
Työntekijöiden kokemus pyrkimyksestä toteuttaa tietoturvaohjeita 2. Millä tasolla työntekijät pyrkivät noudattamaan tietoturvakriteerejä?	**Kyselytutkimus** Kvantitatiivinen Pk-yrityksen työntekijät (esimiehet ja työntekijät)	V
Työntekijöiden kokemus tietoturvaohjeiden motivaatiotekijöistä 3. Mitkä tekijät motivoivat työntekijöitä heidän pyrkiessä noudattamaan tietoturvakriteerejä?	**Haastattelututkimus I** Kvantitatiivinen ja kvalitatiivinen Pk-yrityksen työntekijät (esimiehet ja työntekijät)	V
Työntekijöiden motivaation syntyminen ja muutos tietoturvaohjeiden noudattamisessa 4. Mitkä tekijät vaikuttavat motivaation syntymiseen tietoturvakriteerien noudattamisessa? 5. Mitkä tekijät vaikuttavat motivaation muuttumiseen tietoturvakriteerien noudattamisessa?	**Haastattelututkimus II** Kvalitatiivinen Pk-yrityksen työntekijät (työntekijät)	V

Tutkimus muodostuu neljästä vaiheesta. *Ensimmäisessä* vaiheessa muodostetaan tietoturvakriteerit tietoturvakirjallisuuden ja erityisesti suomalaisille pk-yrityksille suunnattujen tietoturvaohjeistusten sisällöstä. Tavoitteeseen pääsemiseen käytetään dokumenttianalyysiä. Tutkimuksessa selvitetään mitä tietoturvakriteerejä Suomessa julkaistut ohjeet sisältävät. Samalla saadaan selville mitkä viranomaistahot ohjeistavat erityisesti pk-yritysten tietoturvaa Suomessa ja mitä näiden ylläpitämiä tietoturvaohjeistuksia on olemassa. Samalla selvitetään myös muita keskeisiä Suomessa erityisesti pk-yritysten tietoturvaa ohjeistavia tahoja. Ensimmäisen vaiheen tuloksena saadaan tietoturvakriteerit, jotka on muodostettu tietoturvakirjallisuuden ja suomalaisille pk-yrityksille suunnattujen tietoturvaohjeistusten sisällöstä.

Tämän jälkeen *toisessa* vaiheessa tarkastellaan ensimmäisen vaiheen pohjalta muodostettujen tietoturvakriteerien noudattamaan pyrkimisen tasoa. Ajzen (1985) on osoittanut *suunnitellun toiminnan teoriassa*, että aikomuksen määrä on suhteessa tehtävästä suoriutumisen todennäköisyyteen. Siksi tässä tutkimuksessa keskitytään erityisesti tutkimaan tietoturvaan pyrkimisen tasoa, eli motivaatiota ja halua pyrkiä toimimaan tietoturvaohjeiden mukaisesti. Tutkimusmenetelmänä käytetään yrityksen työntekijöille kohdistettavaa kvantitatiivista kyselytutkimusta. Tarkastelussa yrityksen työntekijät jaetaan aseman mukaan esimiehiin ja työntekijöihin. Kyselyn tuloksena saadaan selville tietoturvakriteerien noudattamaan pyrkimisen taso tutkitussa yrityksessä. Erityisesti kyselystä nostetaan esille tietoturvakriteerit, joita työntekijät pyrkivät noudattamaan heikoiten.

Kolmannessa vaiheessa tarkastellaan toisen vaiheen tuloksena saatuja heikoiten noudattamaan pyrittyjä tietoturvakriteerejä. Niihin liittyen selvitetään tekijöitä, jotka motivoivat työntekijää noudattamaan tietoturvakriteerejä. Tätä varten toteutetaan sekä kvantitatiivinen että kvalitatiivinen haastattelututkimus. Tutkimuksen tuloksena saadaan työntekijöiden näkemyksiä heikosti noudattamaan pyrityistä tietoturvakriteereistä sekä motivaatiotekijöitä, jotka motivoivat työntekijöitä pyrkimään tietoturvakriteerin noudattamiseen.

Lopulta *neljännessä* vaiheessa tarkastellaan tekijöitä, jotka vaikuttavat työntekijän motivaation syntymiseen ja muuttumiseen tietoturvakriteerien noudattamisessa. Tätä varten toteutetaan toinen haastattelututkimus, joka on kvalitatiivinen. Tutkimuksen tuloksena saadaan työntekijöiden näkemyksiä motivaation syntymiseen ja muuttumiseen vaikuttavista tekijöistä hallinnollisten tietoturvakriteerien noudattamisessa.

Tutkimus *rajataan* tarkastelemaan hallinnollista tietoturvaa. Tietoturvan muita osa-alueita käsitellään siltä osin, mikä on tutkimuksen tekemiselle tarpeellista. Tutkimus tehdään työntekijöiden näkökulmasta ja siinä käsitellään esimiesten ja työntekijöiden tuloksia erikseen. Tutkimuksen kontekstina on suomalainen pk-yritys. Tutkimus rajataan tarkastelemaan erityisesti suomalaisia pieniä ja keskisuuria yrityksiä eli niin sanottuja pk-yrityksiä ja niiden työntekijöitä. Yritys on pieni, kun työntekijöitä on vähemmän kuin 50 henkilöä ja liikevaihto tai taseen loppusumma on enintään 10 miljoonaa euroa. Keskisuuressa yrityksessä työntekijöitä on alle 250 henkilöä ja liikevaihto on maksimissaan 50 miljoonaa euroa tai taseen loppusumma on maksimissaan 43 miljoonaa euroa. (Euroopan unioni 2007; Tilastokeskus 2011.) Tietoturvan hallinnollisen näkökulman takia pienistä yrityksistä tarkastellaan vain suurimpia yrityksiä, koska erittäin pienissä yrityksissä hallinnollisen tietoturvan toteutuminen on useimmiten hyvin epämääräistä tai olematonta. Tutkimuksen ulkopuolelle on rajattu valtionhallinto, kunnat, järjestöt, verkostot ja muut organisoitumismuodot, joista voitaisiin yhteisesti käyttää nimitystä organisaatiot. Tämän takia tutkimuksessa käytetään termiä *yritys* termin *organisaatio* sijaan.

Tietoturvakirjallisuuden ja -ohjeistusten sisällön esittely ja tutkiminen toteutettiin vuosina 2010–2011. Tietoturvakirjallisuutta täydennettiin keväällä 2014. Kysely- ja ensimmäinen haastattelututkimus toteutettiin vuoden 2013 alussa. Toinen haastattelututkimus toteutettiin huhtikuussa 2014.

1.4 Tulokset

Tästä tutkimuksesta syntyy neljä tulosta: ensimmäisenä tuloksena saadaan *tietoturvakriteerit*, jotka on muodostettu tietoturvakirjallisuuden ja suomalaisille pk-yrityksille suunnattujen tietoturvaohjeistusten sisällöstä. Tutkimuksen toisena tuloksena saadaan selville *tietoturvakriteerien noudattamaan pyrkimisen taso* tutkitussa yrityksessä. Tuloksissa keskitytään erityisesti tietoturvakriteereihin, joita työntekijät pyrkivät noudattamaan heikoiten. Tutkimuksen kolmantena tuloksena saadaan selville *motivaatiotekijöitä*, jotka motivoivat suomalaisen pk-yrityksen työntekijöitä heidän pyrkiessä noudattamaan hallinnollisen tietoturvan tietoturvakriteerejä, joita esitetään tietoturvakirjallisuudessa ja suomalaisille pk-yrityksille suunnatuissa tietoturvaohjeistuksissa. Lopulta tutkimuksen neljäntenä tuloksena saadaan selville *motivaation syntymiseen ja muuttumiseen vaikuttavia tekijöitä* työntekijöiden pyrkiessä noudattamaan hallinnollisia tietoturvakriteerejä. Tutkimuksen tulokset muodostetaan yrityksen työntekijöille suunnatun kyselytutkimuksen ja kahden haastattelun perusteella.

1.5 Tutkimuksen eteneminen

Tutkimuksen toisessa luvussa tarkastellaan motivaatiota ja sen teorioita. Luvussa kuvataan motivaation merkitystä työn ja työssä tapahtuvan oppimisen tukena. Luvun päätteeksi muodostetaan motivaatioviitekehys empiirisen tutkimuksen tarpeisiin. Luvussa kolme esitetään kirjallisuuskartoitus tietoturvaan. Huomioitavaa on, että luvuissa kolme ja neljä kuvataan tarkasti alkuperäisten lähteiden termistö, jotta lukijalle tulisi mahdollisimman totuudenmukainen kuva ohjeistuksissa käytössä olevasta termistöstä.

Empiirisen tutkimuksen aineistot, toteutus ja tulokset on kuvattu luvuissa neljä ja viisi. Luvussa neljä esitetään suomalaisia tietoturvaohjeistajia ja tarkastellaan tietoturvaohjeistusten sisältöjä. Ohjeistuksissa keskitytään erityisesti pk-yrityksille suunnattuihin tietoturvaohjeistuksiin.

Luvun viisi alussa muodostetaan tietoturvakriteerit luvuissa kolme ja neljä esitetyn sisällön pohjalta. Muodostettuja tietoturvakriteereitä käytetään kyselytutkimuksessa, jonka toteutuksen ja tulosten kuvaamisella lukua jatketaan. Kyselytutkimuksen perusteella valitaan vähiten motivoivat tietoturvakriteerit tarkemman arvioinnin kohteeksi. Tietoturvakriteerien motivoivuutta sekä motivaation syntymiseen ja muuttumiseen vaikuttavia tekijöitä selvitetään kahdella haastattelututkimuksella, joiden toteutus ja tulokset on kuvattu luvun loppupuolella.

Luvussa kuusi käydään keskustelua, jossa aluksi pohditaan tulosten tieteellistä merkitystä sekä tehdään käytännön suosituksia. Luvun lopussa pohditaan tutkimuksen rajoituksia ja esitetään jatkotutkimusaiheita.

2 MOTIVAATIO JA OPPIMINEN

Tässä luvussa tarkastellaan motivaatiota ja siihen liittyviä teorioita sekä työpaikalla tapahtuvaa oppimista. Luvussa tarkastellaan motivaation merkitystä erityisesti työn ja työssä tapahtuvan oppimisen tukena. Luvussa esitellään motivaatioteorioita, joille on keskeistä työntekijän toiminta ja sen tarkastelu. Luku päätetään muodostamalla motivaatioteorioista viitekehys, jota käytetään myöhemmin kohdassa 5.4 esitettävän haastattelututkimuksen toteutuksessa.

2.1 Motivaatioteorioita

Motivaatio-sanan kantasana on latinankielinen moveo, joka tarkoittaa liikuttamista. Motivaatio saa ihmisen aktivoitumaan, liikkumaan ja pyrkimään kohti päämääriä. Motivaation lähteitä ovat esimerkiksi into, ilo ja vireys. Motivaation taso riippuu useista motiiveista. (Rasila & Pitkonen 2010: 5, 11, 20.) Motivaatio on johde sanasta motiivi, joka on yksilön käyttäytymisen virittäjä ja ylläpitäjä. Motiivit, kuten tarpeet, sisäiset yllykkeet, palkkiot ja rangaistukset, ovat päämääräsuuntautuneita. Yksilön motiivi voi olla tiedostettua tai tiedostamatonta. (Ruohotie 1998: 35–36.) Motiivi on syy toimia tietyllä tavalla (Nurmi & Salmela-Aro 2005: 10). Ruohotie (1998: 35–37) pitää motivaation alkuperänä latinankielistä sanaa movere, joka tarkoittaa liikkumista. Motivaatio on järjestelmä, joka virittää ja ohjaa ihmisen käyttäytymistä. Motivaatio ja tahto on erotettava käsitteinä. Motivaatio on tila, joka on saatu aikaan motiiveilla ja edeltää päätöksentekoa. Tahto on päätöksenteon jälkeinen tila.

Motivaatiolle on keskeistä suunta ja vireys. Motivaation taso vaihtelee tilanteen ja tehtävän mukaan. Toiminnan seurauksena syntyvät pienetkin tulokset luovat mielihyvää, itseluottamusta ja rohkeutta, sekä kasvattavat motivaatiota. Motivoituminen erilaisiin tilanteisiin ja tehtäviin on taito, jota voi opetella ja harjoitella kuten muitakin taitoja. Motivaatiotason kehittymiseen vaikuttavat esimerkiksi usko omiin kykyihin ja mahdollisuuksiin sekä oman itsensä arvostus. (Rasila & Pitkonen 2010: 41; Ruohotie 1998: 34, 37.) Jo evoluutioteorian pohjalta on esitetty, että motivaatio on ihmisille yhteinen lajiominaisuus, joka on kehittynyt lisätäkseen yksilöiden sopivuutta ympäristöönsä (Nurmi & Salmela-Aro 2005: 18). Niitamo (2005: 40) lisää, että psykologian tieteellisillä tutkimuksilla on osoitettu, että ihmisen toimintaan vaikuttavat kaksi toisistaan lähes riippumatonta motiivia: tunneperäinen ja tietoperäinen motivaatio.

Rasilan ja Pitkosen (2010: 12) mukaan motivaatiotutkimusten yhteisenä tuloksena on todettu, että motivaatiotekijöitä on runsaasti ja niiden merkitys on erilainen eri

ihmisille. Mm. Vartiainen ja Nurmela (2005: 189) ja Ruohotie (1998: 50) ovat todenneet, että mikään yksittäinen motivaatioteoria ei yleisesti hyväksytysti kuvaa yksiselitteisesti ihmisen toimintaa. Heidän mukaansa ei ole myöskään olemassa yhtä suurta yleisesti hyväksyttyä integroivaa motivaatioteoriaa. Ruohotie (1998: 50) lisää vielä, että yhdistävän teorian esteenä ovat puutteet käsitteiden määrittelyssä, useat samaa ilmiötä kuvaavat teoriat sekä prosessien ja toimintojen rajaaminen eri tavalla.

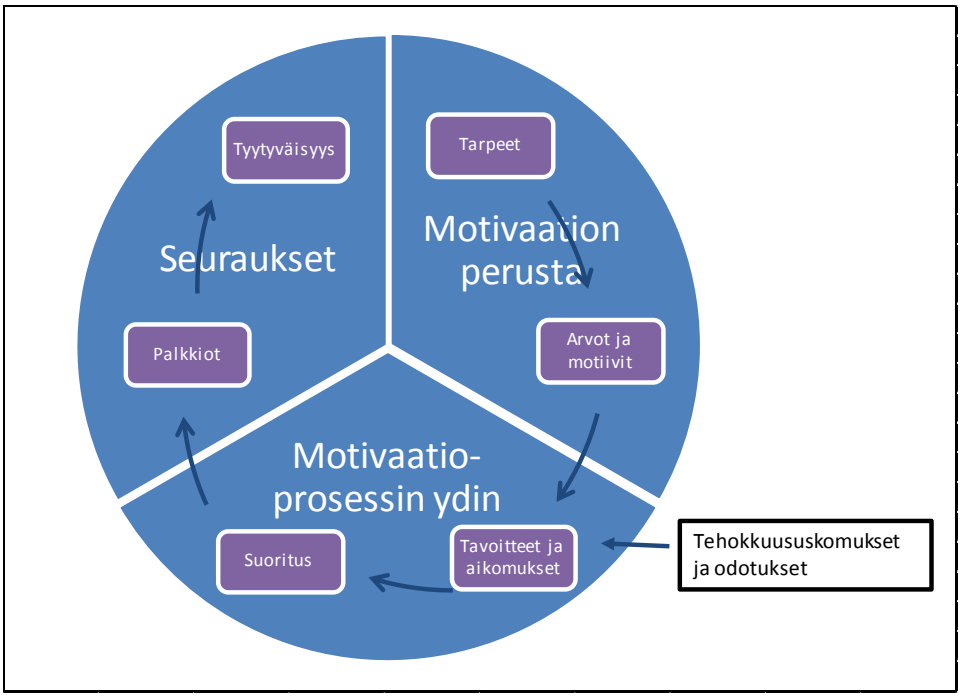
Motivaatioteoriat voidaan jakaa ryhmiin eri tavoilla, kuten sisältö- ja prosessimotivaatioteorioihin tai ulko- ja sisäsyntyisiin motivaatioteorioihin. Sisältömotivaatioteorioilla kuvataan yksilössä sisäisesti olevia ominaisuuksia, jotka antavat yksilön toiminnalle energiaa ja suunnan sekä pitävät toimintaa yllä. Prosessimotivaatioteoriat kuvaavat tapahtuman, eli kerrotaan miten energisointi, suuntaaminen ja ylläpito etenevät. Ulkosyntyisessä motivaatiossa motivaatio tulee ulkoa. Ulkoinen motivaatio luodaan ärsykkeillä, joihin reagoimisen jälkeen tekijä palkitaan. Tämän takia ulkoinen motivaatio on melko lyhytkestoista. Ulkosyntyisiä motivaatioteorioita ovat esimerkiksi vahvistamis- ja tavoiteteoria. Ne selittävät motivaatioon ihmisen ulkopuolelta vaikuttavia tekijöitä. Sisäsyntyisissä motivaatioteorioissa motivaatio tulee sisältä. Sisäinen motivaatio on tehokkaampaa, koska se on yksilön aitoa kiinnostusta opittavana olevasta kohteesta. Sisäistä motivaatiota luova toiminta on tyypillisesti leikinomaista, etsivää, tutkivaa ja haastavaa. Tällaisesta toiminnasta tyydytys tulee varsinaisesta tekemisestä eikä ihminen odota seurausta, esimerkiksi ulkoista palkkiota. Sisäiseen motivaatioonkin voidaan kuitenkin vaikuttaa myös ulkopuolelta, mutta vain välillisesti. Sisäiset vaikutustekijät ovat usein kognitiivisia prosesseja. Perustarpeet tyydyttävä ympäristö lisää sisäistä motivaatiota. Sisäsyntyisiä motivaatioteorioista esimerkkinä voidaan mainita odotusarvoteoria. (Vartiainen & Nurmela 2005: 189–190; Kolb 1984: 77–78; Niitamo 2005: 41.) Sisäinen ja ulkoinen motivaatio ovat tämän tutkimuksen kontribuutiossa keskeisiä ja mielenkiintoisia.

Nurmi ja Salmela-Aro (2005: 12, 16–17) toteavat, että viime aikojen eniten käytetyt motivaatioteoriat korostavat sisäsyntyisen motivaation merkitystä. Nämä teoriat ovat muodostuneet kritiikistä, joka on kohdistettu behavioristiselle teorialle. Ensimmäisenä sisäsyntyisen motivaation käsitteen loi Deci, joka yhdisti motivaatioon autonomian ja kontrolloidun toiminnan. Hän esitti, että ulkosyntyinen toiminta voi muuttua sisäsyntyiseksi autonomiseksi toiminnaksi. Ensin ulkoisesti säädelty toiminta muuttuu sisäisesti säädellyksi toiminnaksi. Tämän jälkeen sisäisesti säädelty toiminta muuttuu tunnistetusti säädellyksi toiminnaksi. Käytännössä ihminen tekee aluksi jonkin asian palkkion toivossa, sitten esimerkiksi itsearvostuksen kohottamiseksi ja lopulta siksi, että hän itse arvostaa toimintaa ja sen seurauksia.

Ulkoisen ja sisäisen motivaation sijaan Niermeyer ja Seyffert (2004: 14–16, 19, 62) jakavat motivaation yleiseen ja erityiseen motivaatioon. Menestyksekäs toiminta vaatii persoonallisuutta, pätevyyttä ja liikkumavaraa. Yleinen motivaatio pohjautuu persoonallisuuteen. Se on ihmisen luontainen halu kehittää, saavuttaa ja vaikuttaa. Myös erityinen motivaatio pohjautuu osittain persoonallisuuteen. Se kohdistuu konkreettiseen tavoitteeseen ja tilanteeseen, ja on syy ihmisen sitoutumiseen. Erityisen motivaation säilyttäminen vaatii ponnistelua ja rentoutumista. Erityisen motivaation taso on korkeimmillaan, kun työntekijä uskoo, että tavoitteen tuloksella on hänelle merkitystä ja sillä on positiivisia vaikutuksia sekä, että tulokseen on vielä mahdollista vaikuttaa ja hän voi itse vaikuttaa siihen.

Motivaatiotutkimuksen menetelmät ja mittarit ovat olleet pitkään osa ihmisen tulevaisuuteen suuntautumisen tutkimusta. Menetelmänä on useissa mittareissa pyydetty henkilöä kertomaan oman tulevaisuutensa toiveista ja peloista, minkä jälkeen toiveita ja pelkoja on pyydetty arvioimaan. Henkilön on täytynyt esimerkiksi arvioida kunkin toiveen tai pelon todennäköinen toteutumisaika ja oma mahdollisuus vaikuttaa sen toteutumiseen. Modernissa motivaatioteoriassa tutkitaankin motivaatiota nimenomaan ihmisen tavoitteiden näkökulmasta. Tavoitteena on ensin määritellä ihmisen tavoitteet, pyrkimykset ja hankkeet, ja sen jälkeen selvittää ihmisen arvio omista mahdollisuuksistaan toteuttaa ne ja vaikuttaa niihin. Lisäksi tavoitteena on, että ihminen arvioi määriteltyjen tavoitteiden, pyrkimysten ja hankkeiden tärkeyden sekä kertoo millaisia tunteita ihmisellä herää niihin liittyen. (Nurmi & Salmela-Aro 2005: 19–20, 23.) Tavoitteiden ja pyrkimyksen tason selvittäminen on tämän tutkimuksen kontribuutiossa keskeistä.

Motivaatioprosessissa merkityksellisiä ovat oppijan odotukset, uskomukset ja arvot. Odotukset muodostuvat oppijan itseluottamuksesta, uskosta omiin kykyihin ja menestymismahdollisuuksiin, itsesäätelymahdollisuuksista ja tunnepitoisista reaktioista arviointitilanteessa. Arvot koskevat mielekkyyttä (saavutus-, mielenkiinto- ja hyötyarvot) ja oppijan tavoiteorientaatiota, joka voi olla sisäistä tai ulkoista. (Ruohotie 1998: 70–71.) Ruohotie (1998: 50–51) on kuvannut motivaatioon liittyvän prosessin, joka on esitetty kuviossa 1.



Kuvio 1. Motivaatioprosessi (Ruohotie 1998: 50).

Kuviosta 1 on nähtävissä, että motivaatioon vaikuttavan prosessin perustana ovat tarpeet ja niistä muotoutuvat arvot ja motiivit. Motivaatioprosessin ydin sisältää tavoitteet ja aikomukset sekä toiminnan, joilla niihin pyritään. Tavoitteisiin ja aikomuksiin ja henkilön suoritukseen vaikuttavat tehokkuususkomukset ja odotukset. Motivaatioprosessi päättyy seurauksiin, jotka muodostuvat palkkioista ja niitä seuraavasta tyytyväisyydestä. Seuraavaksi esitellään motivaatioteorioita, jotka sijoittuvat prosessissa eri vaiheisiin.

Tarpeisiin perustuvia motivaatioteorioita

Tarpeisiin perustuvana tunnetuimpana motivaatioteoriana voidaan pitää Maslowin (1943) *tarveteoriaa*. Sen mukaan ihmisen tarpeet ohjaavat ihmisen toimintaa. Tarpeet voidaan jakaa viiteen hierarkkiseen tasoon, jotka ovat alimmasta ylimpään fysiologiset, turvallisuuden, yhteenkuulumisen ja rakkauden, sosiaalisen arvostuksen sekä itsensä toteuttamisen tarpeet. Alemmalle tasolle sijoittuvat tarpeet tulee olla riittävässä määrin tyydytettyjä, jotta ylemmän tason tarpeet voivat tulla tyydytetyiksi. (Maslow 1943; Rasila & Pitkonen 2010: 36.) Jo aiemmin oli Murrayn (1938) *motiiviteoriassa* perustana käytetty tarvetta. Murray luokittelee ja tarkastelee tarpeita yksilön ja ympäristön huomioivalla tavalla. Teoriassa kuvataan suoriutumisen, vallan ja läheisyyden perusmotiivit. Teoriassaan hän totesi tarpeen kuvastavan yksilön näkökulmaa, johon ympäristö luo painetta. (Murray 1938; Nurmi & Salmela-Aro 2005: 15–16.)

Tarpeet painottuvat eri ihmisillä eri tavoin. McClellandin (1976; 1978) tutkimuksen tuloksena motivaatiotekijöinä nähdään saavutusten, vallan ja yhteenkuulumisen tarpeet. Hänen *suoritusarvoteoriansa* mukaan saavutuksia painottava henkilö haluaa haastavia työtehtäviä ja realistisia tavoitteita. Hänelle on tärkeää työn tulokset ja palautteen saaminen. Valtaa painottava henkilö haluaa vaikuttaa ja johtaa. Muodollinen valta ja asema sekä omien mielipiteiden huomioiduksi tuleminen ja henkilönä arvostaminen ovat hänelle tärkeitä. Yhteenkuulumista painottava henkilö haluaa yhteistyötä ja yhdessä oloa sekä vuorovaikutusta, jossa on hyvä henki. Hänelle on tärkeää toisten huomioiminen ja itse huomioon otetuksi tuleminen. Tähän tutkimustulokseen pohjautuen McClelland on luonut motivaation mittausmenetelmiä, joita ovat suoriutumis-, valta- ja läheisyysmotivaatioita mittaavat menetelmät. (Rasila & Pitkonen 2010: 12–13; Nurmi & Salmela-Aro 2005: 16; Ruohotie 1998: 53.)

Myös Decin ja Ryanin *fenomenologinen itsemääräämisteoria* pohjautuu tarpeisiin. Sen mukaan sisäsyntyisen motivaation näkökulmasta ihmisellä on yleisesti kolme psyykkistä tarvetta, jotka ovat autonomia, kompetenssi ja läheisyys. (Deci & Ryan 2000; Nurmi & Salmela-Aro 2005: 17.) Fysiologiaan pohjautuvassa motivaatioteoriassa lisätään, että oppiminen ei vaikuta tarpeisiin. Sen mukaan tarpeet, motiivit ja vietit ovat henkilön sisäisiä ominaisuuksia, jotka syntyvät elimistössä ja aivoissa. (Nurmi & Salmela-Aro 2005: 11.)

Arvoihin ja motiiveihin perustuvia motivaatioteorioita

Arvoihin ja motiiveihin perustuvan Vroomin (1964) *odotusarvoteorian* (käytetään myös odotusteoria) mukaan ihmisen toimintaan liittyvät tarkoituksellisuus, päämäärähakuisuus ja tiedostetut aikeet sekä ponnistelu, suorituksellisuus ja palkitseminen. Siinä on löydettävissä odotusarvo ja välinearvo. Teorian mukaan motivoituakseen tekijän on nähtävä tehtävä sopivan haastavana – ei liian helppona tai vaikeana (odotusarvo). Lisäksi odotusteorian mukaan motivoituakseen tekijän on uskottava, että suoriutumisesta saa toivotunlaisen palkkion tai hyödyn (välinearvo). Motivaatioon pohjautuen työntekijä ponnistelee oman kyvykkyytensä (kuten lahjakkuus, tiedot ja taidot) rajoissa suorittaen toimintaa yhä uudelleen päästäkseen tavoitteeseen. Suorituksen tavoitteena on tulos, joka voi olla ulkoinen tai sisäinen. Saavutettu tulos aiheuttaa työntekijässä tyytyväisyyttä, mutta se voi aiheuttaa myös tyytymättömyyttä, sillä aina ei synny haluttuja tuloksia. Jotta suoritus voitaisiin merkittävällä tavalla palkita, on määriteltävä suoritukseen sidottavat hyvät mittarit. Lisäksi palkkio tulee valita työntekijäkohtaisesti sellaiseksi, että saaja arvostaa sitä. (Vroom 1964; Vartiainen & Nurmela 2005: 193–195; Ruohotie 1998: 54, 57.)

Nuttinin (1984) *relationaalisen motivaatioteorian* mukaan yksilön sisäisen tarpeen ja tarpeen ulkoisen kohteen välillä on suhde, motiivi. Motiivi ei ole yksilön sisäinen ominaisuus tai voima. Teorian mukaan motivaatiota toteutetaan määrittelemällä motiivit konkreettisiksi tavoitteiksi, minkä jälkeen ne toteutetaan luotujen suunnitelmien ja strategioiden mukaisesti. Teorian toinen keskeinen piirre korostaa kognitiivisten mekanismien merkitystä motivaatiossa, ts. ihminen tietää, mikä häntä motivoi ja mikä on hänen tavoitteensa. Teoriassaan Nuttin nimesi motivaatiolle fysiologisia ja kognitiivisia tarpeita. Uteliaisuus ja sosiaalisuus ovat esimerkkejä kognitiivisista tarpeista. Modernille motivaatiotutkimukselle on keskeistä Nuttinin relationaalisen motivaatioteorian mukainen ajatus motivaatiosta relaationa, eli suhteena sisäisen tarpeen ja sen kohteen välillä. Nuttin kehitti tavan mitata motivaatiota. Se perustuu lauseentäydennysmenetelmään. Käytännössä henkilöä pyydetään täydentämään aloitettuja lauseita, esimerkiksi ”Haluan, että…”. (Nuttin 1984; Nurmi & Salmela-Aro 2005: 12–13.)

Tavoitteisiin ja aikomuksiin perustuvia motivaatioteorioita

Tavoitekeskeinen motivaatiotutkimus oli yleistä 1980-luvulla. Tällöin tehtiin useita tutkimuksia, joissa henkilöä pyydettiin nimeämään tavoitteita ja arvioimaan niitä. (Nurmi & Salmela-Aro 2005: 20.) Tavoitteisiin ja aikomuksiin perustuva Ajzenin (1985; 1991) *suunnitellun toiminnan teoria* pohjautuu aikomukselle toimia. Teorian mukaan aikomuksen määrä on suhteessa tehtävästä suoriutumisen todennäköisyyteen. Aikomus yhdistää motivaatiotekijät. Tuntiessaan tarvetta ihmisen sisäinen tila on epätasapainossa ja tarpeen tyydyttämällä toiminnalla saavutetaan tasapaino. Tarpeita ovat toimeentulo-, liittymis- ja kasvutarpeet. Erityisesti oppimisen kannalta tärkeää on itsearvostuksen tarve. Arvoilla tarkoitetaan päämääriä, joihin pyritään tavoitteellisella toiminnalla, jossa laaditaan suunnitelma ja asetetaan tavoite. Arvot näkyvät tavoitteissa. Toisaalta arvot voivat muuttua, jos tavoitteet muuttuvat saadun palautteen perusteella. (Ajzen 1985; Ajzen 1991; Ruohotie 1998: 51, 53–54.)

Tavoitteisiin ja aikomuksiin perustuu myös *tavoitteisen toiminnan teoria* (ts. tavoiteteoria), jossa keskeistä on toiminnan säätelyä ohjaava päämäärä. Siinä tavoitteet ovat tehtävä- ja tilannesidonnaisia. Teoria pohjautuu ajatukselle, että tietoiset tavoitteet ja aikomukset ohjaavat ihmisen toimintaa. Parhaaseen tulokseen päästään, kun työntekijälle asetetaan tarkat ja haasteelliset tavoitteet, joiden asettamiseen hän on saanut itse osallistua, ja lisäksi hänelle annetaan tavoitteiden saavuttamiseen tähtäävästä toiminnasta palautetta ja kannustusta sekä hänet saadaan sitoutumaan toimintaan. Tavoitehakuisessa toiminnassa on tärkeää, että tavoite asetetaan ja tavoitteeseen pääseminen ei tunnu liian vaikealta. Taitavassa tavoitehakuisessa toiminnassa tavoite määritellään yksityiskohtaisesti, selkeästi ja konk-

reettisesti. Sille on ominaista, että tavoite pystytään näkemään toteutuneena. Tavoitehakuisessa toiminnassa tavoitteen toteuttaminen on määrätietoista toimintaa. Jos toiminnassa kohdataan esteitä tai vastoinkäymisiä, toimintaa parannetaan entisestään eikä niiden anneta lannistaa tavoitteeseen pääsemisessä. (Vartiainen & Nurmela 2005: 192; Rasila & Pitkonen 2010: 23; Ruohotie 1998: 50.)

Emmonsin vuodelta 1986 olevassa *henkilökohtaisten pyrkimysten teoriassa* (pyrkimysinventaarissa) keskeinen käsite on pyrkimys, jolla tarkoitetaan ihmisen luonteenomaista tai tyypillistä tavoitetta toimia elämässä. Teoriassa henkilö nimeää ensin 15 henkilökohtaista pyrkimystä täydentämällä lauseen *”Minä tyypillisesti pyrin…”* 15 kertaa. Sen jälkeen henkilö sijoittaa pyrkimyslauseet taulukkoon ja arvioi niitä 17 dimensiolla, joita ovat esimerkiksi tunteet ja saavuttaminen. (Nurmi & Salmela-Aro 2005: 21.)

Suoritukseen perustuvia motivaatioteorioita

Leontjevin (1977) *toiminnan teorian* mukaan ulkomaailman ja psyykkisten ilmiöiden välillä on kohteellista toimintaa. Sen mukaan sekä yksilön toiminta että motiivijärjestelmä on hierarkkinen. Yksilön toiminnan hierarkkiset tasot ovat toiminta, toiminto ja teko, joita vastaavat motivaation hierarkkiset tasot motiivi, tavoite ja alatavoite. Leontjevin mukaan henkilöiden motiivien tärkeysjärjestykset poikkeavat toisistaan. (Leontjev 1977; Nurmi & Salmela-Aro 2005: 14–15.)

Psykoanalyyttisen motivaatioteorian mukaan yksilön toimintaa ei voida motivoida tietoisella ajattelulla. Myös behavioristinen teoria sivuaa motivaatiota ajatuksella, että todennäköisesti yksilö jatkaa toimintaa, josta hän saa palkinnon. (Nurmi & Salmela-Aro 2005: 11.)

Tehokkuususkomuksiin ja odotuksiin perustuvia motivaatioteorioita

Tehokkuususkomuksiin ja odotuksiin perustuvan Banduran *sosiaalis-kognitiivisen teorian* (ts. sosiaalis-kognitiivisen itsesääntelyteorian) mukaan ihminen saa tietoa oman toiminnan ymmärtämiseksi, kun hän tarkkailee itseään, omia toimintatapojaan, tunneperäisiä reaktioitaan ja ympäristöolosuhteitansa. Tämän seurauksena hän ymmärtää omien ajatusten vaikutukset omaan motivaatioon, tunteisiin ja suorituksiin. Suorituksiin perustuvassa *attribuutioteoriassa* lisätään, että myös onnistumisten ja epäonnistumisten syiden tulkinnat vaikuttavat motivaatioon, tunneperäisiin reaktioihin ja suorituksiin. (Ruohotie 1998: 58–59, 62–63.)

Palkkioihin perustuvia motivaatioteorioita

Palkkioihin perustuvassa *vahvistamisteoriassa* on behavioristinen ote. Siinä painotetaan suorituksen seuraamuksia, suorituksen tehokkuuden arviointia ja tekniikoita mitata motivaatiota. Vahvistamisteoria soveltuu palkitsemiseen, joka perustuu tehtävään sekä toistuvan perustoiminnan parantamiseen, mutta ei sovellu toimintatapojen kehittämiseen. (Vartiainen & Nurmela 2005: 191–192; Ruohotie 1998: 64.) Myös Decin (1971) *kognitiivinen evaluaatioteoria* perustuu palkkioihin. Se selittää ulkoisten palkkioiden ja sisäisen motivaation yhteyttä. Sen mukaan sisäistä motivaatiota voidaan muuttaa ulkoisilla palkkioilla. Siinä on löydettävissä kaksi näkökulmaa, jotka ovat kontrollointi ja informointi. Ensimmäisen näkökulman mukaan käyttäytymistä voidaan kontrolloida palkkioilla ja yllykkeillä. Sisäinen motivaatio muutetaan ulkoiseksi motivaatioksi tehokkaammalla kontrolloinnilla. Informoiva näkökulma tuottaa tietoa pätevyydestä ja se liittyy vahvasti saatavaan palautteeseen. Positiivinen palaute vahvistaa pätevyyden tunnetta, josta seuraa motivaation kasvu. (Deci 1971; Ruohotie 1998: 66–67.)

Tyytyväisyyteen perustuvia motivaatioteorioita

Herzbergin, Mausnerin ja Snydermanin (1959) *kaksifaktoriteoriassa* käsitellään työmotivaatioon vaikuttavia tekijöitä. Siinä motivaatioon vaikuttavina tekijöinä nähdään motivaatio- tai hygieniatekijät. Motivaatiotekijät liittyvät varsinaiseen työhön. Teorian mukaan motivaatiotekijät luovat tyytyväisyyttä ja parantavat suoritusta. Motivaatiotekijöitä ovat esimerkiksi saavutukset, tunnustus ja vastuu. Hygieniatekijät liittyvät työympäristöön. Heikosti hoidetut hygieniatekijät aiheuttavat tyytymättömyyttä, jonka seurauksena motivaatio laskee. Hygieniatekijät voivat liittyä esimerkiksi ohjauksen ja valvonnan luonteeseen, työskentelyolosuhteisiin ja turvallisuuteen. (Herzberg ym. 1959; Lämsä & Hautala 2008, 84; Ruohotie 1998: 68–69.)

2.2 Työssä oppiminen

Varsinaisen työn tekemisen ohella ihmisen on opeteltava työtehtävissään tarvitsemiansa tietoja ja taitoja. Työssä oppiminen saattaa ajoittain vaatia varsinaisista työtehtävistä irtautumista. Työssä oppiminen on työpaikalla tapahtuva jatkuva prosessi. Myös yrityksen tietoturvaohjeiden omaksuminen perehdytysvaiheessa tai työsuhteen aikana vaatii työssä oppimista. Siksi työssä oppimisen periaatteita on hyvä tarkastella hieman laajemmin.

Zuboff (1990) on todennut, että työssä oppimisesta on tullut uusi työn muoto. Se on yrityksen jokapäiväistä kehittämistä. Työssä oppiminen on työyhteisön käytän-

töjen sisäistämistä ja niihin osallistumista (Lave & Wenger 1991; Brown & Duguid 1991). Järvinen (1999) sen sijaan pitää työssä oppimista vapaamuotoisena, asiayhteyteen ja paikkaan sidottuna, rakentavana ja kokemukseen pohjautuvana.

Oppiminen on yksi ihmisen tiedollisista toiminnoista, jota kognitiivinen psykologia tutkii (Dix, Finley, Abowd & Beale 2004). Puolimatka (2002, 85) lisää, että kognitiivisessa psykologiassa oppija eli ihminen käsitetään yksilönä, joka ymmärtää, ajattelee ja jäsentää ympäristöä sekä pystyy noudattamaan sääntöjä. Oppiminen vaikuttaa oppijan maailmankuvaan. Oppimisesta saatava hyöty voi olla pitkävaikutteinen ja sillä voi olla monta kerrosta. Oppiminen vaikuttaa esimerkiksi oppijan motivaatioon. Oppimisessa keskeistä on itsemääräämisen ja itsesäätelyn näkökulmat ja prosessit. Niillä pystytään suuntaamaan ja kontrolloimaan oppijan oppimista, motivaatiota ja suoritusta. Itsesäätelyn osa-alueita on 11. Ne ovat tavoitteet, tavoiteorientaatio, tehokkuususkomukset, mielenkiinto, keskittyminen, toimintastrategia, itsetarkkailu, itsearviointi, attribuutiotulkinnat, tulosodotukset ja adaptiivisuus. (Ruohotie 1998: 12–13, 26, 78–79.)

Ruohotie (1998: 77, 131–133) näkee oppimisprosessissa kolme vaihetta: toimintaan sitoutuminen, toiminnan kontrollointi ja toiminnan itsereflektointi. Oppimisprosessi alkaa toimintaan sitoutumisesta, jossa luodaan pohja oppimiselle. Käytännössä toimintaan sitoutumisessa määritellään tavoite, suunnitellaan oppimisstrategia sekä luodaan käsitys itsestä oppijana. Kun oppimisprosessi on alkanut, tulee oppimista kontrolloida. Toiminnan kontrollointi ohjaa oppimisprosessia. Se myös säätelee oppimistoimintaa ja oppijan tarkkaavaisuutta. Työssä oppimisessa korostuvat itsetarkkailu ja oppimista ohjaavien sisäisten mallien olemassaolo. Lopuksi oppimistoimintaa tulee itsereflektoida. Käytännössä tämä tarkoittaa oppimiskokemusten tarkastelua sekä niiden merkitysten arviointia. Oppimista edistäviä tekijöitä on 10. Ne ovat ulkoisten tapahtumien seuraaminen, kyky arvioida palautetta rehellisesti, tulosten mittaaminen, uuden kokeiluun kannustaminen, avoin ilmapiiri, jatkuva kouluttaminen, monimuotoisuuden ruokkiminen, tiedonkulun esteiden poistaminen, osallistuva johtaminen ja riippuvuuden myöntäminen.

Aikuiskoulutus on koulutusta, joka on suunniteltu ja järjestetty aikuisille. Se jaetaan kolmeen tyyppiin: omaehtoinen koulutus, henkilöstökoulutus ja työvoimapoliittinen koulutus. Näistä henkilöstökoulutuksesta vastaavat työnantajat. Aikuiskoulutuksessa suuri osa oppimisesta tapahtuu työpaikoilla eli on työssä oppimista. Suomalaiset osallistuvat aikuiskoulutukseen kansainvälisesti verrattuna paljon. (Opetus- ja kulttuuriministeriö 2012.) Vahervan (2002: 95) mukaan työpaikka voidaan nähdä enenevässä määrin oppimisympäristönä. Laajentamalla työtehtäviä ja lisäämällä työntekijän vastuuta työntekijä kokee työnsä palkitsevammaksi.

Työntekijälle tarjotaan uusia kokemuksia ja mahdollisuutta luovaan kokeiluun. Lisäksi työntekijä oppii uutta tietoa. Kuitenkin suuri osa työpaikalla tapahtuvasta oppimisesta saattaa korostaa pysyvyyttä ja tavoitella rutiinien ja asiaintilojen säilyttämistä (Ruohotie 1998: 14). Engeström (2001) huomauttaa, että työssä oppimisessa työntekijässä tapahtuvan oppimisen lisäksi tapahtuu myös työpaikan eli työyhteisön oppimista.

Yrityksessä tapahtuvan oppimisen käyttäytymis- ja toimintamalleissa on löydettävissä välttämisstrategioita. Lisäksi oppiminen tapahtuu oppimaan oppimisen teorian mukaisesti. Välttämisstrategian mukaan työntekijän uhkien käsittely tapahtuu välttelemällä niitä. Käytännössä tämä näkyy vaikeiden asioiden ja muutosten lykkäämisenä. Oppimaan oppimisen teoriassa strategia on juuri päinvastainen. Siinä pyritään oppimaan tulevaisuuden uhkien käsittelyä. (Ruohotie 1998: 16.)

Marton ja Booth (1997: 38) jakavat oppimisen kuuteen osa-alueeseen, jotka ovat tiedon lisääntyminen, mieleenpainaminen ja toistaminen, tiedon soveltaminen, asian ymmärtäminen ja asian näkeminen uudella tavalla sekä näiden koosteena muuttuminen ihmisenä. Kolb (1984: 76–78) on määritellyt oppimisprosessimallin aikuiselle oppijalle. Siinä oppimisprosessi kuvataan kehänä, joka muodostuu konkreettisesta kokemuksesta, reflektoivasta havainnoinnista, abstraktista käsitteellistämisestä ja aktiivisesta kokeilemisesta. Jotta oppimista tapahtuu, täytyy havainnoida, reflektoida ja käsitteellistää. Tällaisen oppimisen voidaan nähdä soveltuvan mm. tietoturvaohjeiden omaksumiseen.

Eräässä oppimisen teoriassa korostetaan aiempaa enemmän yhteistyötä ja sosiaalista vuorovaikutusta. Sosiaalinen näkökulma sisältyy myös useimpiin oppimisteorioihin. (Tynjälä 2000: 148.) Jonassenin (1995) merkityksellisen oppimisen mallissa oppimiseen vaikuttavina tekijöinä nimetään aktiivisuus, tavoitteellisuus ja tilannesidonnaisuus. Hänen mukaansa oppimiseen vaikuttavia tekijöitä ovat konstruktiivisuus, reflektiivisyys, yhteisöllisyys ja vuorovaikutteisuus. Myös Belth (1965: 60–62) esittää oppimisen tilannesidonnaisena tapahtumana. Illeris (2002: 9) nimeää oppimisen ulottuvuuksiksi yhteisöllisyyden, kognitiivisuuden ja emotionaalisuuden. Oppimisen malliin voidaan lisätä myös siirtovaikutus (Ruokamo & Pohjolainen: 1999).

Lave ja Wenger (1991: 29–43) ovat luoneet tilannesidonnaisesta oppimisesta teorian, jossa oppiminen nähdään yhteisöllisenä tapahtumana. Erityisesti teoriassa on huomioitavaa, että yhteisön kokeneempien jäsenten tehtävänä on ohjata oppijan tietojen ja taitojen kehittämistä. Käytännössä tämä tarkoittaa tiedon ja osaamisen jakamista oppijoiden kesken. (Sawyer 2006; Järvelä, Häkkinen & Lehtinen 2006.) Tiedon ja osaamisen jakaminen on keskeistä tietoturvaohjeiden omaksumisessa.

Oppijat pystyvät olemaan vuorovaikutuksessa keskenään tieto- ja viestintätekniikan avulla. Myös oppijoiden kognitiivista oppimista voidaan tukea tieto- ja viestintätekniikalla. De Corte, Verschaffel, Entwistle ja Van Merriëboer (2003) ovat osoittaneet omassa tutkimuksessaan, että tieto- ja viestintätekniikalla voidaan saavuttaa oppimista tukevia hyötyjä, jotka ovat yhteisöllinen tiedonrakentelu ja verkostomainen toiminta sekä niihin kuuluvat motivationaaliset ja kognitiiviset prosessit.

Tynjälä (2000: 100) näkee tilannekohtaisina vaikuttavina tekijöinä oppijan ajatuksen omasta suoriutumiskyvystä, käsityksen oman toiminnan ja oppimistilanteen hallinnasta, ajatuksen kyvystä vaikuttaa toiminnan lopputulokseen sekä tavan selittää toiminnan onnistuminen tai epäonnistuminen. Tilannesidonnaiset piirteet muuttuvat tilanteen mukaan.

Laukkanen (2000) esittelee artikkelissaan Greenon filosofian, jonka mukaan oppimisessa käytetään järjestelmiä, joilla oppijat ovat vuorovaikutuksessa keskenään. Järjestelmät ovat entistä parempia ja kehittyneempiä. Yrityksissä tämä ilmenee siten, että työntekijät ymmärtävät mitkä taidot ovat merkittäviä. Työntekijät myös ymmärtävät miten tärkeää on käyttää sosiaalisia järjestelmiä.

Tämän tutkimuksen kontribuutiossa on erityisen mielenkiintoinen Ruohotien (1998: 31–32) näkemys oppimisen tulokseen vaikuttavista tekijöistä, jotka ovat oppijan asenteet, ajatusrakenteet sekä mielikuvat, jotka ovat syntyneet oppijan aiemmista kokemuksista. Ajatusrakenteet ovat kognitiivisia, affektiivisia ja konatiivisia. Kognitiiviset rakenteet ovat tiedon saamisen ja tiedostamisen prosesseja, kuten havaitseminen, ajattelu ja päättely. Affektiiviset rakenteet ovat tunnereaktioihin liittyen tunne, mieliala ja temperamentti. Konatiiviset rakenteet ovat yksikön kehittymiseen liittyen esimerkiksi motivaatio, impulssi, tahto ja määrätietoinen pyrkimys.

Tiedot opitaan nopeasti, mutta ne myös unohdetaan nopeasti. Taidot opitaan hitaammin, mutta opittuaan ne säilyvät pitkään. Oppimisessa tiedon käsittely on induktiivista tai deduktiivista. Uudelle oppijalle suositellaan induktiivista tiedon käsittelyä. Induktiivisessa tiedonkäsittelyssä edetään yksityiskohtaisesta tiedonkäsittelystä kohti yleisiä lainalaisuuksia ja kokonaisuuksia olevien tietojen käsittelyyn. Tällöin materiaali tulisi esittää ensin yksityiskohtaisesti ja vasta lopuksi materiaalista tulisi muodostaa yleistyksiä ja kokonaisuuksia. Deduktiivinen tiedon käsittely etenee päinvastoin: ensin käsitellään yleisiä periaatteita ja kokonaisuuksia, mistä edetään yksityiskohtaiseen tiedon käsittelyyn. Oppija, jolla on ennestään tietoa asiasta, voi edetä tiedon käsittelyssä deduktiivisesti. Tällöin materiaali voidaan heti aluksi esittää kokonaisuutena ja edetä siitä yksityiskohtiin. (Bannert 2002; Pollock, Chandler & Sweller 2002; Kalyga, Chandler & Sweller 1998.)

Ruohotien (1998: 15–16) mukaan työpaikalla tapahtuvaa oppimista voidaan mitata arvioimalla asetettujen tavoitteiden saavuttamisen tasoa. Oppimista on tapahtunut, kun yrityksessä saavutettu tulos vastaa asetettua toimintasuunnitelmaa. Työntekijöiden toiminta on siis ollut oikeanlaista ja toiminnan seurauksena on onnistunut lopputulos. Myös epäonnistumisen aiheuttaneen virheen löytäminen ja korjaaminen ovat merkki oppimisesta.

2.3 Motivaatio työskentelyn ja työssä oppimisen tukena

Työssä oppiminen on työpaikalla tapahtuva jatkuva prosessi. On ymmärrettävää, että työn tekemisen ohella tapahtuva työssä oppiminen vaatii motivaatiota. Motivaatio liittyy vahvasti työssä oppimiseen ja se on keskeistä työelämässä toimimiselle ja toiminnan ohjaamiselle. Yrityksen tietoturvaohjeiden noudattaminen työtehtävissä on tärkeää. Yrityksen tietoturvaohjeita päivitetään yrityksessä jatkuvasti. Siksi työntekijältä vaaditaan jatkuvaa motivaatiota seurata ja huomioida tietoturvaohjeet jokapäiväisissä työtehtävissä.

Toimintahalu ja tavoitesuuntautuneisuus luovat työmotivaatiota. Työmotivaatiolla tarkoitetaan kokonaisuutta, jossa yksilö tekee työtään energisesti sekä luo, suuntaa ja ylläpitää omaa toimintaansa työssä. (Vartiainen & Nurmela 2005: 188–189.) Liukkosen (2002: 5, 15) mukaan motivaatio vaikuttaa työntekijän jaksamiseen, hyvinvointiin ja suoriutumiseen. Pelkkä osaaminen ja taidot eivät riitä työtehtävistä suoriutumiseen, mikäli työntekijällä ei ole motivaatiota. Motivaatiolla on suuri merkitys työtehtävistä suoriutumiseen. Työtehtävistä suoriutuminen vaatii työntekijältä noin 20–30 prosenttia hänen kyvyistään. Työntekijän motivoinnilla pystytään saamaan työntekijä käyttämään jopa 80–90 prosenttia hänen kyvyistään. (Lämsä & Hautala 2008: 90.)

Työssä ja oppimisessa tapahtuvalle motivaatiolle on Maslowin (1943) tarveteorian mukaisesti edellytyksenä, että teorian mukaisten tarvehierarkioiden tarpeet alemmalta hierarkiatasolta alkaen tulee olla tyydytettyjä. Käytännössä tämä tarkoittaa, että yksilön perustarpeiden tulee olla kunnossa, jotta oppimista voi tapahtua tai työntekijä voi keskittyä työhönsä. (Rasila & Pitkonen 2010: 36–37.)

Motivaatio vaikuttaa oppimiseen aktivoimalla oppimiseen pyrkivää toimintaa (Kolb 1984: 77). Ruohotie (1991: 87–89) pitää motivaatiota keskeisenä tekijänä oppimisen tapahtumiseksi. Motivaatio suuntaa oppijan aktiivisuutta oppimiseen sekä tukee oppimisen päämäärän ja tavoitteen saavuttamista. Motivaatiolla on kestävää oppimista tukeva vaikutus. Se myös tukee kestävään oppimiseen panos-

tamista. Oppimistilanteessa motivaatioon vaikuttavat tilanne, välineet ja sisältö. Sisällöllinen motivaatio kohdistuu opittavan asian sisältöön ja käyttömahdollisuuksiin. (Engeström 1994.)

Työmotivaatio syntyy ulkoisista ja sisäisistä motiiveista. Näistä ulkoiset motiivit pystytään kertomaan määrinä ja esittämään sanallisesti. Sisäiset motiivit perustuvat tunteisiin ja ovat ehkä osittain tiedostamattomia. (Vartiainen & Nurmela 2005: 188–189.) Myös Nurmi ja Salmela-Aro (2005:10) huomauttavat, että motivaatio voi olla myös tiedostamatonta. Suomen Ekonomiliiton (2005: 91) julkaisussa työmotivaatio nähdään työhön liittyvänä tahtotilana. Työmotivaatio auttaa työntekijää ylläpitämään ja kehittämään yrityksen toimintaa ja siksi työntekijöiden työmotivaation voidaan katsoa olevan edellytys yrityksen olemassaololle.

Yrityksen johtamisessa yksi suurimpia haasteita on työntekijöiden motivointi. Tyytyväisyydellä ja motivaatiolla on yhteys. Tyytyväisen ja motivoituneen työntekijän työskentely on tehokasta, laadukasta, innostunutta ja iloista. Motivoituneena työntekijä suoriutuu työstään paremmin ja nauttii tekemisestä sekä pysyy työssään. Työntekijä on vastuullinen ja aktiivinen osaaja, jonka tulee itse huolehtia omasta motivaatiostaan. Kuitenkin etenkin yhteistyötä tehtäessä kumppanin motivaatiota pitää pyrkiä tukemaan. Työntekijän työmotivaation tarkastelussa voidaan keskittyä erimittaisiin ajanjaksoihin: koko työuraan, rajattuun ajanjaksoon tai yksittäiseen hetkeen. (Rasila & Pitkonen 2010: 5–6, 8, 11, 44.) Kuitenkin, Vartiainen ja Nurmela (2005: 190) huomauttavat, että motivaatio yksinään ei vaikuta työntekijän toiminnan määrään ja laatuun. Työntekijän halu ja kyky käyttää omaa osaamistaan työnantajan strategian ja vision tukemiseen vaikuttavat työntekijän tietojen ja taitojen käyttämiseen. Toiminnan määrään ja laatuun vaikuttavat myös työympäristön tilannekohtaiset esteet ja tuki. Thomson ja von Solms (2005) esittävätkin, että yrityksen johdon tulee pyrkiä vaikuttamaan yrityskulttuuriin, jotta tietoturva tulee osaksi työntekijöiden jokapäiväistä tekemistä.

Jokaisella ihmisellä on motivaatiota. Kun mietitään työntekijöiden motivoimisen mahdollisuuksia ja rajoja, voidaan todeta, että työntekijän persoonallisuuteen ei voida vaikuttaa. Motivointia voidaan kuitenkin tehdä työntekijän pätevyyttä ja liikkumavaraa lisäämällä, esimerkiksi työasenteita ja kyvykkyyttä kehittämällä. Yrityksen eduksi muodostuvaan motivaatiotasoon voidaan vaikuttaa kaikilla työntekijöillä. Kaikki työntekijät voidaan saada motivoituneiksi. Tämä saavutetaan rehellisellä ja luotettavalla kanssakäymisellä työntekijöiden kanssa sekä kehittämällä työntekijöitä ja tarjoamalla hyvät reunaehdot. Erityisen tärkeää on yrityksen johtohenkilöstön motivoiva käyttäytyminen. Motivaatio on tulos prosessista, jossa on neljä vaikuttavaa tekijää: motivaatiovaikuttimen voimakkuus, usko omiin vaikutusmahdollisuuksiin, psykologinen aikaperspektiivi ja tunneäly. Näi-

den vaikutustekijöiden lisäksi motivaatioon vaikuttavat työntekijän tahdonvoima ja pätevyys sekä tarjotut reunaehdot. Psykologiseen aikaperspektiiviin vaikuttavat esimerkiksi ikä, kokemus ja kasvatus sekä suuntautuneisuus menneisyyteen, nykyisyyteen tai tulevaisuuteen. Tunneäly muodostuu tietoisuudesta itsestään, itsensä johtamisesta ja motivoimisesta, sitoutumisesta sekä empatiasta. Tunteiden vaikutus motivaatioon on keskeistä. Kuitenkin onnistunut toiminta vaatii sekä järjen että tunteiden osalta positiivista ajattelua. (Niermeyer & Seyffert 2004: 8–10, 12–14, 20–22, 62–63.)

Vaikka jokaisella ihmisellä on motivaatiota, huomauttavat Niermeyer ja Seyffert (2004: 38, 42, 61–62), että motivoituminen vaatii tavoitteita, joihin pyrkimisestä tulisi kunkin työntekijän päättää henkilökohtaisesti. Vain näin toimimalla työntekijä voi vastata tavoitteisiin pääsemisestä sekä kannustaa ja palkita itseään pyrkimyksessään. Asetettavien tavoitteiden tulisi täyttää viisi vaatimusta, jotka ovat realistisuus, haastavuus, houkuttelevuus, mitattavuus ja henkilökohtainen merkitys. Mitattavuus voi kohdistua esimerkiksi aikaan tai tavoiteltavaan tilaan. Vaikka työntekijän tulisi itse tehdä päätös tavoitteeseen pääsemisestä, on johtohenkilöstön motivoitava työntekijöitä. Usein sitä pidetään jopa johtohenkilöstön päätehtävänä.

Robbinsin (2001: 207–208) mukaan työntekijän ottamisella mukaan päätöksentekoon on vahva motivoiva vaikutus. Yrityksen työntekijöitä tulee motivoida yksilöllisesti asettamalla työntekijälle henkilökohtaisesti selkeät ja täsmälliset tavoitteet. Tavoitteen onnistumisesta tulee antaa selkeä ja täsmällinen palaute sekä palkita yksilö tarvittaessa. Ajantasaisen palautteen saamisella on työntekijään selkeästi motivoiva vaikutus. Rasila ja Pitkonen (2010: 32–34) lisäävät, että palautteella, motivaatiolla, työtyytyväisyydellä ja työn ilolla on todettu olevan yhteys. Motivaation suurin tukahduttaja on palautteen puuttuminen. Jopa negatiivinen palaute on motivoivampaa kuin palautteen saamattomuus kokonaan. Palautetta työstä tulisi saada jatkuvasti. Palautetta olisi hyvä saada esimieheltä ja etenkin kollegoilta. Työntekijän tulisi antaa palautetta myös itselleen.

Tämän tutkimuksen yhteydessä on merkittävää huomata Vartiaisen ja Nurmelan (2005: 197) toteamus, että yrityksissä pystytään erilaisilla johtamisjärjestelmillä luomaan tavoitteisiin suuntautunutta motivoitunutta toimintaa. Niermeyerin ja Seyffertin (2004: 65, 69) mukaan johtohenkilöstö pystyy motivoimaan työntekijöitä kehittämällä työntekijöiden pätevyyttä, löytämällä yhteistyönä tavoitteet, joiden saavuttaminen on houkuttelevaa sekä yritykselle että työntekijälle, parhailla mahdollisilla työehdoilla sekä osoittamalla työntekijälle, että ponnistelulla saavutetaan tuloksia. Motivoiva johtaminen toteutetaan viidellä osatekijällä, jotka ovat tavoitteiden muotoilu haasteellisiksi, työntekijän itseluottamuksen vahvista-

minen, liikkumavaran tarjoaminen, työntekijöiden kehityksen tukeminen ja vaatiminen sekä rakentavan palautteen antaminen. Jos yritysjohto asettaa työntekijälle motivoivia tavoitteita, työntekijälle asetettavat erityistavoitteet perustuvat yritykselle asetettuihin yleistavoitteisiin. Itseluottamuksen määrällä on suora vaikutus motivaatioon.

Työntekijää motivoi tavoitteisiin pyrkivä yhteistyö, joka on tarkoituksenmukaista. Sisäisesti motivoitunut työntekijä tekee työtään työn kiinnostavuuden ja sisällön sekä varsinaisen toiminnan ja työn kohteen takia. Sisäiseen motivaatioon yhdistyy neljä motivaatiotekijää, jotka ovat tunne mahdollisuudesta valita, tunne omasta osaamisesta, tunne työn merkityksellisyydestä ja tunne edistymisestä. Sisäisesti motivoitunut työntekijä kokee työssään työtyytyväisyyttä, joka näkyy mielihyvänä sekä onnistumisen ja edistymisen ilona. Sisäinen motivaatio voidaan nähdä oravanpyöränä, joka ruokkii itse itseään. Ulkoisesti motivoitunut työntekijä tekee työtään tavoitellen välinearvoa, jossa merkitsee ainoastaan työn lopputulos. Suurimmalla osalla työntekijöistä on sekä sisäistä että ulkoista motivaatiota. (Vartiainen & Nurmela 2005: 190; Rasila & Pitkonen 2010: 27, 30.) Vartiainen ja Nurmela (2005: 196–197) lisäävät vielä, että työntekijän sisäistä motivaatiota pystytään lisäämään vuorovaikutusrakenteilla. Sisäinen motivaatio vaikuttaa innostukseen, energisoitumiseen ja syvällisen kiinnostuksen luomiseen. Merkittävin vaikutin on palaute, jota saadaan organisaatiolta, johdolta, esimieheltä, kollegoilta ja asiakkailta. Ulkoiset palkkiot vaikuttavat toiminnan suuntaamiseen ja ylläpitoon.

Motivaation mittaamista on yleisesti tehty projektiivisilla menetelmillä, kuten Murrayn (1938) kehittämä *TAT-menetelmä* (Thematic Apperception Test), joka on kuvatesti ihmisen motivaation tutkimiseen. Siinä tutkittavaa pyydetään kertomaan esitetyssä kuvassa näkemänsä ihmisen tarina. Henkilökohtaisten projektien menetelmässä käytetään yleisimmin kymmentä arviointidimensiota, jotka ovat tärkeys, sitoutuminen, edistyminen, kyky toteuttaa, oma mahdollisuus vaikuttaa toteuttamiseen, muiden henkilöiden/asioiden mahdollisuus vaikuttaa toteuttamiseen, sosiaalinen tuki, sosiaalinen estäminen, stressaavuus ja ajan riittävyys. Dimensioita voi kuitenkin olla enemmänkin, kuten esimerkiksi Littlen perusmenetelmässä, jossa niitä aiemmin todettiin olevan 17. Arviointidimensiot voi muokata tilanteeseen sopivaksi, esimerkiksi käyttämällä erityisiä tunne- tai toimintadimensioita tai sosiaalisia dimensioita. Dimensioiden luokittelu on yleistä. Pääluokkien jako voisi olla esimerkiksi merkitys, saavuttaminen, hallinta, tuki ja kuormitus. Littlen pääluokkien todettiin aiemmin olevan merkitys, rakenne, yhteisöllisyys, tehokkuus ja stressi. (Murrayn 1938; Nurmi & Salmela-Aro 2005: 16, 21; Salmela-Aro 2005: 28, 30, 32–33.)

Little (1983) loi PPI-menetelmän (Personal Project Analysis inventory), joka on teoria henkilökohtaisista projekteista. Sen pohjana käytetään valmiusristikkomenetelmää, jossa tutkittava nimeää ensin vähintään kymmenen henkilökohtaista projektia ja sitten arvioi niitä 17 dimension näkökulmasta asteikolla 0–10. Littlen menetelmässä dimensioiden pääluokat ovat merkitys, rakenne, yhteisöllisyys, tehokkuus ja stressi. (Little 1983; Nurmi & Salmela-Aro 2005: 20–21.)

Salmela-Aro (2005: 30, 37) muotoilee 10 eniten käytettyä dimensiota tarkastelemaan kutakin nimettyä tavoitetta seuraavilla 10 dimensiota sisältävällä kysymyksillä. Tutkittavaa pyydetään vastaamaan kysymyksiin asteikolla 1–7, jossa 1 tarkoittaa ei yhtään ja 7 tarkoittaa erittäin paljon. Kysymykset ovat:

1. *”Miten tärkeä tavoitteesi on?*
2. *Miten sitoutunut olet siihen?*
3. *Missä määrin tavoitteeseesi pääseminen on edistynyt?*
4. *Miten kykenevä olet saavuttamaan sen?*
5. *Missä määrin voit itse vaikuttaa siihen?*
6. *Missä määrin muut henkilöt tai asiat vaikuttavat siihen?*
7. *Missä määrin olet saanut siihen tukea muilta?*
8. *Missä määrin muut ovat estäneet tavoitteeseesi pääsyä?*
9. *Miten stressaavaa on pyrkiä tavoitteeseesi?*
10. *Miten sinulla riittää aikaa tavoitteeseesi?”*.

Deci ja Ryan (Nurmi & Salmela-Aro 2005: 17; Salmela-Aro 2005: 34) ovat luoneet menetelmän mitata toiminnan motivoivuutta. Menetelmää käytettäessä henkilöä pyydetään kertomaan syy, miksi hän toteuttaa tiettyyn tavoitteeseen pyrkivän toiminnon. Vastausvaihtoehtoja annetaan neljä. Ne ovat toisen henkilön tai tilanteen vaatimus, toteuttamisen tuottama mielihyvä tai oma kiinnostus, toteuttamatta jättämisestä aiheutuva häpeä, syyllisyys tai ahdistus sekä oma usko toteuttamisen tärkeydestä. Menetelmä soveltuu erityisesti itsetuotettujen tavoitteiden mittaamiseen.

2.4 Motivaatioviitekehys

Kohdassa 2.1 esiteltiin motivaatioteorioita. Niistä mitään ei ole yleisesti hyväksytty kuvaamaan yksiselitteisesti ihmisen toimintaa. Mitään motivaatioteoriaa ei ole myöskään yleisesti hyväksytty yhdeksi suureksi integroivaksi motivaatioteoriaksi. Modernissa motivaatioteoriassa tutkitaan motivaatiota ihmisen tavoitteiden näkökulmasta. Teorian mukaan ensin määritellään ihmisen tavoitteet, pyrkimykset ja hankkeet, ja sen jälkeen selvitetään ihmisen omat mahdollisuudet toteuttaa ne ja vaikuttaa niihin. Lisäksi tavoitteena on, että ihminen arvioi miten tärkeiksi

hän kokee määritellyt tavoitteet, pyrkimykset ja hankkeet sekä kertoo, millaisia tunteita hänellä herää niihin liittyen. Motivaatiotutkimusten yhteisenä tuloksena on löydetty runsaasti motivaatiotekijöitä, joiden merkitys ihmisille on erilainen. Viime aikoina eniten käytetyt motivaatioteoriat korostavat sisäisen motivaation merkitystä. Sisäisen motivaation käsitteen loi ensimmäisenä Deci.

Oppimiselle ovat keskeistä itsemääräämineen ja itsesäätely. Niillä pystytään suuntaamaan ja kontrolloimaan oppijan oppimista, motivaatiota ja suoritusta. Oppimisprosessi alkaa toimintaan sitoutumisesta. Prosessin aikana oppimista tulee kontrolloida ja lopuksi itsereflektoida. Työpaikalla tapahtuva oppiminen on käytännössä työyhteisön käytäntöjen sisäistämistä ja niihin osallistumista. Motivaatio on keskeinen tekijä oppimisen tapahtumiseksi. Työelämässä toimiminen ja toiminnan ohjaaminen vaativat motivaatiota. Motivaatiolle on tärkeää määritellä suunta tai kohde. Työmotivaatiota luodaan toimintahalulla ja tavoitesuuntautuneisuudella, jotka luodaan sekä ulkoisilla että sisäisillä motivaatiotekijöillä. Ulkoiset motivaatiotekijät pystytään kertomaan määrinä ja esittämään sanallisesti. Sisäiset motivaatiotekijät perustuvat tunteisiin ja saattavat olla osittain jopa tiedostamattomia. Motivaation tasoon vaikuttavat tilanne ja tehtävä. Työntekijän toiminta on tehokkaampaa, kun hän on aidosti kiinnostunut opittavana olevasta asiasta. Jo pienetkin työntekijän toiminnasta syntyvät tulokset kasvattavat motivaatiota.

Decin ja Ryanin toimintojen motivoivuutta mittaava menetelmä soveltuu itsetuotettujen tavoitteiden mittaamiseen. Menetelmää käytettäessä henkilön tulee kertoa syy toteuttaa tiettyyn tavoitteeseen pyrkivä toiminto. Henkilön tulee valita syy neljästä annetusta vaihtoehdosta, jotka ovat toisen henkilön tai tilanteen vaatimus, toteuttamisen tuottama mielihyvä tai oma kiinnostus, toteuttamatta jättämisestä aiheutuva häpeä, syyllisyys tai ahdistus sekä oma usko toteuttamisen tärkeydestä. Tämä mittausmenetelmä valitaan sovellettavaksi myöhemmin empiirisessä haastattelututkimuksessa, joka toteutus esitellään kohdassa 5.4. Tämän menetelmän käyttämiselle tässä tutkimuksessa on löydettävissä useita perusteluja. Aiemmin todettiin, että motivaatiotutkimuksen menetelmissä ja mittareissa on perinteisesti pyydetty henkilöä kertomaan oman tulevaisuutensa toiveista ja peloista, minkä jälkeen toiveita ja pelkoja on täytynyt arvioida. Motivaatiotutkimuksissa on kuitenkin löydetty runsaasti erilaisia motivaatiotekijöitä, minkä takia tietoturvakriteerien motivaatiotekijöitä tutkittaessa on niiden määrää hyvä rajata. Decin ja Ryanin menetelmän motivaatiotekijät (toisen henkilön tai tilanteen vaatimus, toteuttamisen tuottama mielihyvä tai oma kiinnostus, toteuttamatta jättämisestä aiheutuva häpeä, syyllisyys tai ahdistus sekä oma usko toteuttamisen tärkeydestä) soveltuvat hyvin käytettäväksi tietoturvakriteerien noudattamisen motivaatiotekijöinä. Menetelmä sopii hyvin arvioimaan yrityksen tietoturvakriteerien eli tietoturvatoimenpiteiden toteuttamisen motivaatiotekijöitä.

Aiemmissa tietoturvatutkimuksissa on viitekehyksenä perinteisesti käytetty peloteteorioita ja myös neutralisoimisteoriaa. Decin ja Ryanin teorian neljästä motivaatiotekijästä yhteen sisältyy pelko, joka on toteuttamatta jättämisestä aiheutuva häpeä, syyllisyys tai ahdistus. Edellä esitetyn perusteella muut motivaatioteoriat eivät suoraan tarjoa mahdollisuutta pelon merkityksen mittaamiselle työntekijän toiminnassa. Aiemmissa tietoturvatutkimuksissa on ollut viitteitä Decin ja Ryanin mukaisiin motivaatiotekijöihin, kun on todettu, että tietoturvaohjeiden noudattamiseksi työntekijän on ymmärrettävä tietoturvaohjeiden sisältö ja merkitys suhteessa omiin työtehtäviinsä (mm. Puhakainen 2006). Decin ja Ryanin teoriaa ei ole kuitenkaan käytetty aiemmissa tietoturvatutkimuksissa. Decin ja Ryanin teorian käyttäminen on tämän tietoturvatutkimuksen viitekehyksenä mielekästä ja mielenkiintoista. Perusteluna Decin ja Ryanin teorian käyttämiselle ja muiden motivaatioteorioiden käyttämisen poissulkemiselle on myös merkittävää huomata, että muilla olemassa olevilla ja esitellyillä motivaatioteorioilla ei voida suoraan mitata pelon merkitystä motivoivana tekijänä, minkä takia ne eivät sellaisenaan sovellu tämän tietoturvatutkimuksen viitekehykseksi.

Decin ja Ryanin teorian valinnan perusteluina on myös huomioitava, että viime aikoina eniten käytetyt motivaatioteoriat korostavat sisäisen motivaation merkitystä. Decin ja Ryanin menetelmän mukaiset neljä motivaatiotekijää ovat helposti lajiteltavissa sisäisiin ja ulkoisiin tekijöihin: ulkoisesti motivoivaa on toisen henkilön tai tilanteen vaatimus -motivaatiotekijä ja loput kolme motivaatiotekijää (toteuttamisen tuottama mielihyvä tai oma kiinnostus, toteuttamatta jättämisestä aiheutuva häpeä, syyllisyys tai ahdistus sekä oma usko toteuttamisen tärkeydestä) ovat sisäisesti motivoivia tekijöitä.

3 TIETOTURVA

Tässä luvussa luodaan kirjallisuuskatsaus tietoturvaan. Kirjallisuuskatsausta varten käytiin läpi keskeisten tietoturvaa määrittelevien organisaatioiden teokset sekä yliopistoissa pääsykoekirjoina käytettävät teokset. Luvussa aluksi esitellään tietoturvan keskeiset käsitteet. Sen jälkeen käydään läpi tietoturvaan liitettäviä dokumentteja, tietoturvasuunnittelun sisältöä ja tietoturvaan kohdistuvia riskejä. Luku päätetään syventymällä tietoturvakäyttäytymiseen. Luvussa käytettävä termistö tullaan kuvaamaan alkuperäisessä lähteessä olevan termistön mukaisena, koska dokumenttien sisällön analysointi on yksi tutkimuksen tavoitteista. Luvun sisällön pohjalta muodostetaan myöhemmin kohdassa 5.1 tietoturvakriteerejä.

3.1 Keskeiset käsitteet

Tietoturva ja tietoturvallisuus (information security, data security) tarkoittavat samaa. Yleisessä suomalaisessa asiasanastossa – YSA:ssa (2011) tietoturvallisuus termin sijaan suositellaan käyttämään termiä tietoturva. Tekniikan sanastokeskus (2002) ja Tietotekniikan liitto (2008: 339–340) käyttävät sekä termiä tietoturva että tietoturvallisuus. Tietotekniikan liiton (2008: 340) tietoturva-termin määritelmän mukaan tietoturvalla tarkoitetaan tavoitetilaa, jossa tiedot, tietojärjestelmät ja palvelut suojataan asianmukaisesti siten, että uhat, jotka kohdistuvat tietojen, tietojärjestelmien ja palvelujen käytettävyyteen, eheyteen ja luottamuksellisuuteen, eivät aiheuta merkittävää vahinkoa yhteiskunnalle ja sen jäsenille. Valtiovarainministeriö (2003: 51) ja Viestintävirasto (2009a) käyttävät julkaisuissaan esitettyä Tietotekniikan liiton tietoturva-määritelmää. Tietotekniikan liiton (2008: 340) määritelmän mukaisesti tietoturvalla tarkoitetaan myös lainsäädäntöä ja muita normeja sekä toimenpiteitä, joilla pyritään varmistamaan tietoturva normaali- ja poikkeusoloissa. Leppänen (2006: 285) huomauttaa, että tietoturva käsitetään helposti liian laajana ja sitä pidetään jopa turvallisuusjohtamisen synonyyminä erityisesti teknologiayrityksissä.

Tietoturva on perinteisesti yhdistetty tiedon arvoon. Klassisessa tiedon arvoon perustuvassa määritelmässä tietoturvan katsotaan koostuvan ainoastaan tiedon käytettävyydestä, eheydestä ja luottamuksellisuudesta. Tällöin tietoturvalla tarkoitetaan toimenpiteitä, joiden tavoitteena on varmistaa tiedon käytettävyys, eheys ja luottamuksellisuus. Tässä yhteydessä *käytettävyydellä* tarkoitetaan, että tieto on saatavilla siihen oikeutetulle taholle sillä hetkellä, kun taho sitä tarvitsee. Tiedot ovat saatavissa käyttöön nopeasti ja oikeassa muodossa. *Eheydellä* tarkoitetaan, että saatu tieto kuvaa tarkasti sen tilan tai tapahtuman, jota sen sanotaan esittävän ja on siten paikkansapitävää. Näin ollen ehyt tieto on oikein, eikä se sisällä tahat-

tomastikaan tehtyjä virheitä. *Luottamuksellisuudella* tarkoitetaan, että tietoon pääsevät käsiksi vain ne, joilla siihen on oikeus. (mm. Tekniikan sanastokeskus 2002; Leppänen 2006: 260–261; Valtiovarainministeriö 2008: 107, 109; Hakala, Vainio & Vuorinen 2006: 4; Heljaste ym. 2008: 30; Liikenne- ja viestintäministeriö 2010a.)

Tietoturvaominaisuuksien käytettävyys, eheys ja luottamuksellisuus määrittelyssä ei kerrota välitöntä tietoa siitä, miten tietoturva tulisi hoitaa tai, mitä toimenpiteitä sen varmistamiseksi tulisi tehdä. Määrittelyssä kerrotaan ainoastaan tietoturvatoiminnan tavoitteet. (Saarenpää, Pöysti, Sarja, Still & Balboa-Alcoreza 1997: 75.) Mm. Leppäsen (2006: 260–261) ja Hakalan ja muiden (2006: 4–5) mukaan käytettävyydellä tarkoitettu tiedon saatavuus tarkoittaa käytännössä mahdollisuutta luoda tietoa, käsitellä, hyödyntää ja muuttaa tietoa sekä siirtää ja tuhota tietoa. Käytettävyys vaikuttaa työn tehokkuuteen ja laatuun. Käytettävyyteen pyritään ylläpitämällä tietoa riittävän tehokkailla laitteilla sekä työstämällä tietoja tiedon muotoon parhaiten soveltuvilla ohjelmistoilla. Käytettävyydellä pyritään myös tiedon automaattiseen jatkojalostukseen sekä antamaan järjestelmän tiedot käyttäjälle sopivassa muodossa, esimerkiksi yhteenvetona. Käytettävyyden toteutumiseen vaikuttavat tietojenkäsittelyn resurssit, toiminnan varmuus ja laatu. Tiedon eheyteen pyritään pääasiassa ohjelmoinnilla, kuten ohjelmoimalla sovelluksiin esimerkiksi syötteen tarkistuksia tai -rajoitteita. Eheyttä ylläpidetään myös laitteisto- ja tietoliikenneratkaisuilla sekä salakirjoitusmenetelmillä. Tiedon luottamuksellisuutta varmistetaan suojaamalla tiedot ja tietojärjestelmät käyttäjätunnuksella ja salasanalla. Myös salakirjoitusmenetelmillä pystytään suojaamaan arvokasta tietoa. Luottamuksellisuus varmistetaan käytännössä käyttäjien hallinnalla, tietojen luokittelulla, yksityisyyden suojan varmistamisella sekä suojaamistoimenpiteillä.

Tiivis tietoturvasanasto (2004: 13–16) on ottanut tietoturvan määritelmän komponentteihin mukaan tietoturvan, käytettävyyden, eheyden ja luottamuksellisuuden lisäksi termit aitous, yksityisyyden suoja, tietosuoja ja tietoturvapolitiikka. Myös tässä määritelmässä tietoturva ja tietoturvallisuus rinnastetaan tarkoittamaan samaa. Kirjan Tiivis tietoturvasanasto määritelmän mukaan tietoturva tarkoittaa järjestelyjä, joiden tavoitteena on varmistaa käytettävyys, tiedon eheys ja luottamuksellisuus. Tietoturva tarkoittaa myös oloja, joissa tietoturvariskit ovat hallinnassa. Teoksen mukaan tietoturvan järjestelyjä ovat esimerkiksi salaus ja varmuuskopiointi sekä palomuurin, virustorjuntaohjelman ja varmenteiden käyttö. Edelleen teoksessa kerrotaan, että tietoturvaan kuuluvat esimerkiksi tietoaineistojen, laitteistojen, ohjelmistojen, tietoliikenteen ja toiminnan turvaaminen. Tiiviin tietoturvasanaston mukaan käytettävyys tarkoittaa, että tieto, järjestelmä tai palvelu on hyödynnettävissä haluttuna aikana. Tiedon eheys tarkoittaa, että tiedon si-

sältö ei ole muuttunut. Aitoudella tarkoitetaan tiedon eheyttä ja, että tiedon alkuperäinen lähde on se, joka sen väitetään olevan. Luottamuksellisuudella tarkoitetaan, että tieto on vain sen käyttöön oikeutettujen käytettävissä. Yksityisyyden suojalla tarkoitetaan oikeutta yksityisyyteen. Tietosuojalla tarkoitetaan, että tiedon luottamuksellisuus toteutuu. Tietoturvapolitiikka määritellään yrityksen hyväksymäksi määritelmäksi yrityksen tietoturvaperiaatteista, sen päämääristä ja toteutuksesta.

Heljaste ja muut (2008: 30) lisäävät, että tietoturva tarkoittaa myös yrityksen liiketoiminnan jatkuvuuden ja asiakastietojen varmistamista sekä jatkuvuutta yrityksen tietoturvatoimenpiteiden parantamisessa ja tietoturvamenetelmien seuraamisessa. Sen sijaan Hakalan ja muiden (2006: 5–6) mukaan, jotta tietoturvan määritelmä olisi riittävä, laajennetaan sitä käytettävyyden, eheyden ja luottamuksellisuuden lisäksi kiistämättömyydellä ja pääsynvalvonnalla. *Kiistämättömyydellä* tarkoitetaan tietojärjestelmää käyttävän henkilön tunnistamista ja henkilötietojen tallentamista. Toiminnalla varmistetaan tiedon alkuperä sekä mahdollinen tietojen luvaton käyttö, mikäli tietojärjestelmän omistajan ja käyttäjän välillä ilmenee juridisia epäselvyyksiä. Kiistämättömyyteen pyritään käyttämällä salausmenetelmien tunnistusmekanismeja tai biometrisiä tunnisteita. Tällaisia ovat esimerkiksi älykortti ja sormenjälkitunnistuslaite. *Pääsynvalvonnalla* tarkoitetaan tietojenkäsittelylaitteiden ja -yhteyksien käytön rajoittamista. Pääsynvalvonnan ylläpitämisessä erityisenä haasteena ovat langattomien verkkoyhteyksien luvattomat käyttäjät. Tietoturvan määritelmään voidaan edellä mainittujen lisäksi sisällyttää myös *tunnistus*. Sillä tarkoitetaan tietojärjestelmää käyttävien henkilöiden ja laitteiden luotettavaa tunnistamista. Tällainen tunnistaminen on kuitenkin perusedellytyksenä kiistämättömyydelle ja aiemmin mainitulle luottamuksellisuudelle, minkä takia autenttisuuden lisääminen määritelmään ei ole tarpeellista.

Tietoturvaa käsittelevällä www-sivustollaan Valtiovarainministeriö (2010c) toteaa, että tietoturva on perusedellytys yhteiskunnan toiminnoille ja palveluille sekä sovelluksille ja tietotekniselle perusrakenteelle. Tietoturva koskee kaikkia työntekijöitä. Se on kiinteä ja keskeinen osa organisaation koko toimintaa sekä toiminnan ja tietojenkäsittelyn laatutyötä ja varmistamista. Tietoturvassa tulee huomioida myös häiriö- ja poikkeustilanteisiin varautuminen. Tietoyhteiskunnan kehitys, verkottuminen, sähköinen asiointi, toimintojen ja palvelujen siirtyminen tietoverkkoihin, kansainvälistyminen, nopea tekninen kehitys sekä tietoturvahyökkäysten ja muiden uhkien lisääntyminen lisäävät tietoturvan merkitystä. Tietoturvan varmistaminen ja kehittäminen edellyttävät henkilökunnan osaamisen, ohjeistusten ja toiminnan jatkuvaa kehittämistä.

Tietoturvan opetuksessa suomalaisissa yliopistoissa pyritään antamaan opiskelijoille tietoa sekä luomaan puitteet tietoturvan tutkimustyön edistämiselle. Esimerkiksi Oulun yliopistossa pidettävällä tietoturvan peruskurssilla annettava opetus tietoturvan perustietämyksestä kaikille tietotekniikan parissa työskenteleville sisältää 12 osa-aluetta: tietoturvan peruskäsitteet, käyttäjän haasteet, toimiminen tietoturvaprojektissa, modernin organisaation tietoturvan hallinta, tietoriskit, henkilö- ja ohjelmistoturvallisuus, ulkoistamisen ja intranetin tietoturva, biometriset menetelmät sekä tietoturva lainsäädännössä ja kilpailuetuna. Tietoturvasta annettava opetus käsittelee muilla kursseilla mm. lainsäädäntöä, riskienhallintaa sekä tietoturvan hallintaa, johtamista ja kehittämistä. (Helenius 2005, 20–35.)

Suomen Standardisoimisliiton (2006) julkaisun mukaan tietoturvan tavoitteena on varmistaa liiketoiminnan jatkuvuus, minimoidaan liiketoiminnalliset riskit sekä maksimoidaan investoinneista saatu tuotto. Laaksonen ja muut (2006: 115–116) toteavat, että ollakseen tehokasta tietoturvaa on johdettava osana yrityksen liiketoiminnan johtamista. Tietoturva on huomioitava yrityksen kaikissa yksiköissä ja sen on oltava osa jokaisen työntekijän päivittäisiä toimia. Siksi tietoturva tulisi lisätä esimerkiksi osaksi työn ohjeistusta, perehdytystä ja työnohjausta. Laaksosen ja muiden (2006: 228, 286) mukaan tietoturvan tavoitteena on kehittää sisäisiä toimintamenetelmiä ja tiedonkäsittelyä sekä turvata yrityksen tietojen käytettävyys (saatavuus), eheys (oikeellisuus) ja luottamuksellisuus. Tietoturvalle asetettavat keskeiset vaatimukset tulevat pääasiassa yrityksen liiketoiminnasta sekä lainsäädännöstä. Hyvä tietoturva saavutetaan ja sitä ylläpidetään teknisten toimenpiteiden lisäksi huomioimalla ihmisten käyttäytyminen ja lainsäädännön asettamat rajoitukset ja vaatimukset. Myös Leppäsen (2006: 260) mukaan ihmisten toiminta ja tietotekniset ratkaisut vaikuttavat suurelta osin tietoturvaan ja ovat keskeisiä tietoturvan ylläpidossa.

TIEKE Tietoyhteiskunnan kehittämiskeskus ry:n (myöh. TIEKE) (2005a) mielestä tietoturva on pääasiassa käytännön toimintaa ja osaamista. Yrityksessä tulee miettiä, mikä on yrityksen arvokasta ja suojattavaa tietoa sekä varmistetaanko sitä riittävästi, kuka vastaa tietoturvasta ja onko henkilökunnalla kyky toimia oikein ongelmatilanteissa. Tekniikan sanastokeskuksen (2002) julkaisussa todetaan, että tietoturvaa pystytään edistämään salauksella ja varmuuskopioinnilla sekä käyttämällä palomuuria, virustorjuntaohjelmia ja varmenteita. Valtiovarainministeriön (2008: 109) mukaan tietoturvaan pyritään riskienhallinnalla.

Tietoturvan ylläpito on mahdollista vain tietoturvaan vaikuttavien tapahtumien jatkuvalla seurannalla ja tallentamisella. Tietoturvaa suunnitellaan ja kehitetään keräämällä tietoa aikaisemmin tapahtuneista tietoturvaan vaikuttaneista tapahtumista. Tekninen seuranta kohdistetaan niihin yrityksen tietojärjestelmiin ja tapah-

tumiin, jotka ovat merkityksellisiä yrityksen turvallisuudelle. Tietoturvan hallinnollinen seuranta kuuluu kaikille työntekijöille. Epäkohdista tulee raportoida esimiehelle tai tietoturvapolitiikassa määritellylle vastuuhenkilölle. Työntekijöiden inhimillinen toiminta, huolimattomuus, kiirehtiminen ja erehdykset vaarantavat eniten yrityksen tietoturvaa. (Hakala ym. 2006: 101–102.)

Tietoturvaa tulee kehittää jatkuvasti, koska myös yrityksen tilanne muuttuu ja tietoturvavaatimukset vaihtuvat (TIEKE Tietoyhteiskunnan kehittämiskeskus ry 2005a). Tietoturvan toteuttaminen, arviointi, kehittäminen ja ylläpito muodostavat yhden yrityksen liiketoimintaprosessin, jonka toiminta on jatkuvaa (Hakala ym. 2006: 20). Myös Heljaste ja muut (2008: 11) toteavat, että tietoturvan kehittäminen kuuluu yrityksen perustoimintaan samoin kuin liiketoiminnan kehittäminen. He jatkavat, että kehittämisen tulee olla suunnitelmallista ja kehitysalueet kartoittavaa. Lisäksi tuloksia tulee arvioida, jotta kehitys olisi suojattavien arvojen ja niiden uhkien kannalta järkevää ja loogisessa järjestyksessä. Helenius (2005: 6, 45) huomauttaa, että mitä paremmin tietoturva on hoidettu, sitä vähemmän tietoturvaa tarvitsee ylläpitää, kehittää ja kouluttaa sekä tutkia. Tietoturvaan panostaminen on panostamista tulevaisuuteen.

Mm. Liikenne- ja viestintäministeriön (2010a), Viestintäviraston (2009a) ja Heleniuksen (2005: 5) julkaisuissa todetaan, että tietoturvan tavoitteisiin päästään toimenpiteillä, jotka ovat hallinnollisia ja teknisiä. Tämä toteamus on merkittäviä tämän tutkimuksen yhteydessä. Tietoturvan tekniseen toteuttamiseen sisältyvät Laaksosen ja muiden (2006: 172–226, 254) mukaan identiteettihallinta, tietoverkon tekninen suojaaminen, tietojen salaus ja muut salausmenetelmät, virustorjunta, roskasähköpostin ja sähköpostissa saapuvien haittaohjelmien torjunta, tietojärjestelmien turvallisuus, mobiililaitteet ja siirrettävät mediat, laite- ja ohjelmistorekisterit sekä etä- ja langattomat yhteydet. Tietoturvan teknisten ratkaisujen ei pitäisi näkyä työntekijälle ollenkaan tai ainakin mahdollisimman vähän.

Tietoturva käsitteenä on laaja, minkä takia kokonaisuus halutaan usein jakaa helpommin käsiteltäviin osiin. Jaottelu on melko keinotekoinen, koska kaikki osa-alueet vaikuttavat toisiinsa. Jaottelu kuitenkin helpottaa tietoturvasuunnittelua. Tavallisimmin tietoturva jaetaan osa-alueisiin: hallinnollinen tietoturva, fyysinen tietoturva, henkilö(stö)-, tietoaineisto-, ohjelmisto-, laitteisto- ja tietoliikenneturvallisuus. (Hakala ym. 2006: 10–12.) Mm. Valtiovarainministeriö (2010a; 2006: 47), Viestintävirasto (2009a) ja Leppänen (2006: 260) käyttävät samaa tietoturvan jaottelua, mutta lisäävät yhdeksi tietoturvan osa-alueeksi *käyttöturvallisuuden*, jolloin osa-alueita on kahdeksan. Myös Hakala ja muut (2006, 12) mainitsevat yhtenä mahdollisena jaottelun osa-alueena käyttöturvallisuuden, mutta toteavat, että käyttöturvallisuus eli tietojärjestelmien käytöstä aiheutuvat riskit ja niihin

varautuminen on suositeltavaa sisällyttää tietoturvajaottelun kaikkiin osa-alueisiin. Leppänen (2006: 285) huomauttaa, että kaikki tietoturvan osa-alueet ovat yhtä tärkeitä. Yhden osa-alueen painotus johtaa epätasapainoiseen tilanteeseen, joka vaarantaa yrityksen tietoturvan.

Hallinnollisella tietoturvalla varmistetaan tietoturvan kehittäminen ja johtaminen. Siinä on merkittävässä asemassa lainsäädännön sekä lisenssisopimusten ja palvelusopimusten vaikutusten arviointi yrityksen tietoturvakäytäntöihin. Hallinnollisesta tietoturvasta vastaa yrityksen tietohallinto. (Hakala ym. 2006: 10–11.) Leppänen (2006: 285) tarkoittaa hallinnollisella tietoturvalla tietoturvan johtamista ja hallinnan prosesseja. Hallinnollinen tietoturva kuuluu turvallisuusjohtamiseen ja kokonaisvaltaiseen riskienhallintaan. Hallinnollisen tietoturvan elementtejä ovat tietoturvapolitiikka ja -ohjeisto, tietoturvan johtaminen ja vastuiden määrittely, tietoturvan resursointi ja käytännön tietoturvatoimenpiteet, yhteys liiketoimintastrategiaan, henkilöstöturvallisuus sekä toipumissuunnitelma ja kriittisten tilanteiden johtaminen. Yrityksen liiketoiminnan ymmärtäminen ja riskienhallinta ovat pohjana merkittävälle osalle tietoturvan hallintaa (Tietoturva ry 2010).

Hallinnollinen tietoturva käsittää johdon tietoisuuden tietoturvauhkista, tietoturvajohtamisen, tietoturvan hallintamenettelyt, työntekijöiden koulutuksen tietoisiksi riskeistä, yrityksen sidosryhmien tietoturvan hallinnan sekä yhteydenpidon asiakkaisiin ja sidosryhmiin tietoturva-asioissa. (Valtiovarainministeriö 2006: 48; Leppänen 2006: 286.) Heljasten ja muiden (2008: 54, 56) mukaan hallinnollinen tietoturva koostuu toimitilaturvallisuudesta sekä henkilökunnan ohjeistuksesta ja koulutuksesta. Työntekijöille tarkoitettuja hallinnollisia tietoturvaohjeistuksia ovat esimerkiksi turvallisuuspolitiikka, yleinen turvallisuusohje, tietoturvallisuusohje, tekninen käyttäjäohje, kulunvalvontapolitiikka, toimitilojen käyttöä koskeva ohje, vierailijaohje, avainohje, ohje väärinkäytösepäilyihin ja vartiointiohje. Päätöksen käytettävistä ohjeista yritys tekee itse. Heljaste ja muut näkevät hallinnollisen tietoturvan yksinkertaisimpina menetelminä puhtaan pöydän periaatteen ja ovien lukituksen.

Heljaste ja muut (2008: 61) esittävät hallinnollisen tietoturvan tarkastuslistassa seuraavat tarkastelukohteet: yrityksen tietoliikenneinfran dokumentointi ja vastuunjako, virustorjuntaohjelmisto ja palomuuri sekä niiden päivittäminen, palvelintilan lukitus sekä valvonta rikos- ja paloilmoittimella, vesivahingon huomioiminen palvelintilassa, varmuuskopioinnin määräaikaisuus ja varmuuskopioiden säilyttäminen, varavoiman varmistus sähkökatkosten varalle sekä ohjeistus salasanojen vaihtoa ja säilytystä varten.

Valtiovarainministeriön (2006: 48) julkaisun mukaan hallinnollista tietoturvaa arvioidaan johdon tietoisuudella tietoturvauhkista, tietoturvajohtamisella, tieto-

turvan hallintamenettelyllä, työntekijöiden tietoisuudella riskeistä sekä yrityksen sidosryhmien tietoturvan hallinnalla ja yhteydenpidolla asiakkaisiin ja sidosryhmiin tietoturva-asioissa. Yleisimmät arvioinnissa havaittavat puutteet löytyvät tietoturvaohjeistuksista, säännöistä ja koulutuksesta, tietoturvasopimuksista ja -selvityksistä, valvonnasta (käytönvalvonta, fyysinen valvonta, huolto), uhka- ja riskianalyyseistä, riskienhallinnansuunnitelmista ja tietoturvapolitiikasta sekä riittämättömistä resursseista ja pääsyoikeuksien virheellisestä hallinnoinnista.

Fyysisellä tietoturvalla suojataan rakennuksen tiloja ja niihin sijoitettuja laitteita fyysisiltä uhkilta sekä ympäristöuhkilta. Fyysisiä uhkia ovat esimerkiksi ilkivalta ja murrot. Ympäristöuhkia ovat esimerkiksi vesi- ja palovahingot. Fyysisestä turvallisuudesta vastaavat yleensä kiinteistöhuolto ja vartiointiliikkeet. (Hakala ym. 2006: 11.) Leppäsen (2006: 292) mukaan fyysisen tietoturvan tavoitteena on suojata tietojenkäsittelyssä käytettävät laitteet onnettomuuksilta ja tahalliselta vahingoittamiselta.

Henkilö(stö)turvallisuus käsittää toimet, joilla varmistetaan tietojärjestelmän käyttäjien toimintakyky. Lisäksi rajataan käyttäjien mahdollisuuksia käyttää yrityksen tietoja ja tietojärjestelmiä. Henkilöturvallisuudesta vastaa yleensä henkilöstöhallinto ja tietohallinnon edustajat yhdessä muiden turvallisuuselinten kanssa. (Hakala ym. 2006: 11.) Leppäsen (2006: 285–286) mukaan työntekijät nähdään riskitekijänä. Henkilöturvallisuuden toteutuminen vaatii avointa ja luottamuksellista ilmapiiriä, turvallisuuskulttuurin rakentamista, selkeitä perusteluita säännöille ja rajoitteille, turhien vastuiden ja tiedon rajaamista. Henkilöturvallisuus muodostuu Valtiovarainministeriön (2006: 48, 50) mukaan tietoturvaohjeistuksista, sääntöjen tiedottamisesta, koulutuksesta ja valvonnasta, avaintyöntekijöiden käytettävyydestä, suunnitelluista ja hallinnoiduista varamiesjärjestelyistä, henkilöstöriskien arvioinnista sekä työsuhteen aloittamisesta ja lopettamisesta aiheutuvista toimista. Näiden tulisi olla myös arvioinnin kohteita. Valtiovarainministeriö lisää, että henkilöturvallisuuden arvioiminen absoluuttisilla mittareilla on mahdotonta. Yleisimmät puutteet henkilöturvallisuudessa ovat Valtiovarainministeriön (2006: 50) mukaan muun muassa turvallisuusselvityksissä, tietoturvaohjeistuksissa, sääntöjen noudattamisessa, koulutuksessa, valvonnassa, työntekijöiden riittämättömyydessä tai sopimattomuudessa sekä varahenkilöjärjestelyissä.

Henkilöturvallisuudella hallitaan työntekijöiden toiminnasta aiheutuvia tietoturvauhkia. Sen tavoitteena on suojata yrityksen tietojenkäsittely niin, että työntekijöiden aiheuttamat väärinkäytökset ja vahingossa tehdyt virheet eivät haittaa yrityksen toimintaa. Henkilöturvallisuuden tietoturvariskejä aiheuttavat esimerkiksi muutokset yhteiskunnassa, kiristynyt kilpailutilanne sekä yrityksessä ja sen ulkopuolella tietojenkäsittelyä tekevien henkilöiden suuri määrä. Tietoturvastandardit

ja vaatimusten määrittelyt käsittelevät henkilöturvallisuudesta usein tietojenkäsittelyn organisointia ja työntekijöiden taustatietojen kartoittamista. Tietojenkäsittelyn turvallisuus edellyttää työntekijältä luotettavuutta ja nuhteettomuutta. Uudessa yhteistyösuhteessa on henkilöturvallisuuden tietoturvasta hyvä huomioida työntekijöiden palkkaaminen tai yhteistyökumppanien valinta ja taustatietojen tarkastus, luottotietojen selvittäminen sekä sopimusten laatiminen. Yhteistyösuhteen jatkuessa on hyvä huomioida työntekijän toimenkuvan muutokset sekä työtehtävien suorittamisen tietoturva, kuten työntekijöiden selkeä ja hyvä ohjeistaminen sekä koulutus ja motivointi. Myös työsuhteen päättyminen tulee huomioida henkilöturvallisuuden tietoturvassa. (Laaksonen ym. 2006: 138–145.)

Tietoaineistoturvallisuus käsittää toimet, jotka liittyvät tietojen säilyttämiseen, varmentamiseen, palauttamiseen ja tuhoamiseen. Tietoaineistoturvallisuudessa tulee huomioida manuaalisen tietojenkäsittelyn asiakirjat ja automaattisen tietojenkäsittelyn tulosteet. Tietoaineistoturvallisuudesta vastaa yleensä tietohallinto ja organisaation arkistoinnista vastaava taho. (Hakala ym. 2006: 11.) Heljasten ja muiden (2008: 54) mielestä yritykset suojaavat tietojaan, mutta ongelmana on, että läheskään aina yritykset eivät tiedä mitä tietoja niiden tulisi suojata. Elintärkeitä tietoja ovat esimerkiksi asiakasrekisteri, asiakkaan tiedot, asiakaskohtaiset hinnat, tuotekehitys, henkilöstötiedot, henkilöarvioinnit, taloudelliset suunnitelmat, markkinatutkimukset, johdon pöytäkirjat, yritysostot ja niiden suunnitelmat, yritysturvallisuusraportit, tärkeät turvallisuusohjeet, sisäisen tarkastuksen raportit, tuloslaskelmat, laskelmat, katetiedot ja sopimukset. Leppäsen (2006: 262–263, 287) mukaan tiedon elinkaaren vaiheet ovat tiedon luominen/kerääminen, käsittely, siirtäminen, varastointi ja hävittäminen. Tietoaineistoturvallisuudessa tulee huolehtia tiedosta vaiheesta riippumatta. Tietoaineistoturvallisuuden keskeinen osa on tietojen luokittelu. Sen tavoitteena on löytää yrityksen toiminnalle merkittävä tieto ja määritellä sille suojaavat prosessit tiedon koko elinkaaren ajalle.

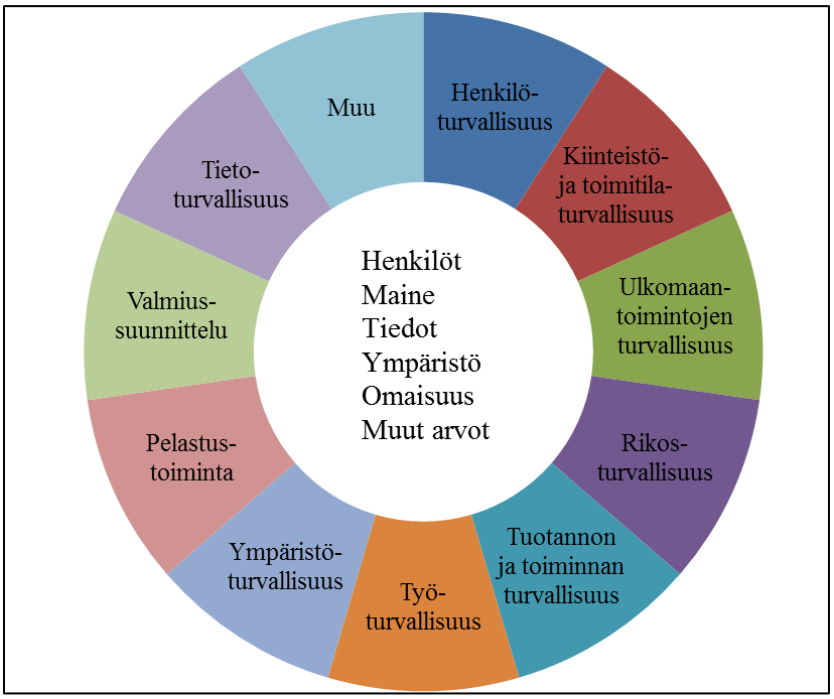
Ohjelmistoturvallisuus liittyy ohjelmistoihin ja käsittää esimerkiksi ohjelmistotestauksen sekä ohjelmistoversioiden ja lisenssien hallinnan. Ohjelmistoturvallisuudesta vastaa organisaation tietohallinto. *Laitteistoturvallisuuden* tavoitteena on mitoittaa tietokoneet ja muut tietojärjestelmään kytketyt laitteet tarkoituksenmukaisesti sekä testata niiden toiminta ja järjestää huolto. Laitteistoturvallisuudessa varaudutaan myös laitteiden kulumiseen ja vanhenemiseen sekä arvioidaan ja minimoidaan laitteiden käytöstä aiheutuvat vaaratekijät. Myös laitteistoturvallisuudesta vastaa pääsääntöisesti tietohallinto. *Tietoliikenneturvallisuudessa* huolehditaan tiedonsiirtoratkaisujen turvallisuudesta. Tietoliikenneturvallisuudesta vastaa organisaation tietohallinto. (Hakala ym. 2006: 11–12.) Leppänen (2006: 300, 303) tarkentaa, että ohjelmisto- ja laitteistoturvallisuuden tavoitteena on varmistaa käytettävien ohjelmistojen laillisuus ja toimintavarmuus sekä suojata

käytössä olevat tietotekniset järjestelmät ja päätelaitteet. Tietoliikenneturvallisuuden tavoitteena on suojata tietoverkot ja niissä liikkuva tieto varmistamalla tiedon käytettävyys, eheys ja luottamuksellisuus.

Käyttöturvallisuuden tavoitteena on Leppäsen (2006: 303–305) mukaan tietojen käytöstä aiheutuvien riskien toteutumisen minimointi. Se tarkoittaa huolehtimista siitä, että kaikki työntekijät hallitsevat toimenpiteet, joilla varmistetaan riittävän tietoturvan ylläpitäminen. Toimenpiteitä ovat työaseman, tietovälineiden, tietoaineistojen, liitetietojen, sähköpostin, Internetin ja lähiverkon käyttö, virustorjunta, käyttöoikeuksien ja salasanojen hallinta, varmuuskopiointi sekä tilojen lukitus ja kulunvalvonta.

Tietoturva on yksi yritysturvallisuuden osa-alueista. Muut osa-alueet ovat henkilö-, työ-, ympäristö- sekä kiinteistö- ja toimitilaturvallisuus, tuotannon ja toiminnan turvallisuus, ulkomaantoimintojen turvallisuus, pelastustoiminta, valmiussuunnittelu sekä rikosturvallisuus. (Heljaste ym. 2008: 27–28; Yritysturvallisuus EK Oy 2009a.) Leppänen (2006: 203) yhdistää ympäristöturvallisuuden sekä kiinteistö- ja toimitilaturvallisuuden ympäristö- ja toimitilaturvallisuudeksi. Myös valtiovarainministeriön (2008: 109) määritelmän mukaan tietoturva on osa yritysturvallisuutta.

Yritysturvallisuustyön keskeinen ajatus on pyrkiä ennaltaehkäisemään ei-toivottuja tapahtumia (Heljaste ym. 2008: 62). Yritysturvallisuutta ohjataan ja hallinnoidaan turvallisuusjohtamisella. Yritysturvallisuus EK Oy (2009a) ei halua erottaa turvallisuusjohtamista omaksi osa-alueekseen, vaan näkee turvallisuusjohtaminen osana yrityksen normaalia johtamista. Turvallisuusnäkökohdat tulisi ottaa mukaan myös yrityksen strategiaan ja päätöksentekoon. Kuvio 2 selkeyttää turvallisuusjohtamista kokonaisuutena ja siihen kuuluvia yritysturvallisuuden osa-alueita tietoturva mukaan lukien. (Yritysturvallisuus EK Oy 2009a.)



Kuvio 2. Turvallisuusjohtamisessa huomioitavat yritysturvallisuuden osa-alueet (Yritysturvallisuus EK Oy 2009a; Heljaste ym. 2008: 28).

Kuviosta 2 nähdään, että turvallisuuden johtamisen alaisuuteen kuuluu yhteensä 10 yritysturvallisuuden osa-aluetta, joista yksi on tietoturva. Muut osa-alueet ovat henkilöturvallisuus, kiinteistö- ja toimitilaturvallisuus, ulkomaantoimintojen turvallisuus, rikosturvallisuus, tuotannon ja toiminnan turvallisuus, työturvallisuus, ympäristöturvallisuus, pelastustoiminta sekä valmiussuunnittelu. Kuvioon on lisätty muu-sektori luokituksen kattavuuden varmistamiseksi. Osa-alueiden merkitykseen yrityksen liiketoiminnan kannalta vaikuttaa yrityksen toimiala. Osa-alueet kattavat yrityksen kaiken turvallisuustoiminnan, joten turvallisuusjohtamisella ohjataan yrityksen turvallisuustoimintaa kokonaisvaltaisesti. Kuvion keskellä on esitetty yritysturvallisuuden osa-alueilla suojattavia yrityksen tärkeitä tekijöitä, joita ovat yrityksen työntekijät, maine, tiedot, ympäristö ja omaisuus. Kuvioon on lisätty muut tekijät varmistamaan luokituksen kattavuus. (Yritysturvallisuus EK Oy 2009a; Heljaste ym. 2008: 27–28.) Heljaste ja muut (2008: 9, 28) huomauttavat vielä, että osa-alueet eivät ole toisistaan erillisiä. Yhden osa-alueen kehittäminen parantaa myös muita osa-alueita. Kuitenkin on huomattava, ettei vain yhden osa-alueen tehokkaallakaan suojaamisella uhkilta voida suojata kaikkia muita osa-alueita. Leppäsen (2006: 57–58) mukaan turvallisuusjohtaminen ei ole helppoa, koska kullakin osa-alueella on omat toimintakulttuurinsa, jotka eroavat toisistaan. Lainsäädäntö säätää yleensä vain yhteen osa-alueeseen kuuluvaa turvallisuusmääräystä kerrallaan. Viranomaisilla on kullakin oma turvallisuuden hallinnonalansa, jota ne valvovat ja yhteistyö yli hallinnonalojen rajojen on vähäistä.

Laaksonen ja muut (2006: 115–170) käsittelevät tietoturvan johtamisesta ja hallinnoinnista yrityksessä johtamisen laajuutta, hyvää tietohallintotapaa (IT Governance), fyysistä ympäristöä, tietoturvaohjelmaa eli tietoturvan toteuttamista käytännössä, henkilöturvallisuutta, tietoturvaohjeistuksia ja -dokumentaatiota sekä toimintaohjeita loppukäyttäjille. Heidän mukaansa tietoturvan johtaminen yrityksessä on kuin minkä tahansa sen toiminnon johtamista: laaditaan tietoturvapolitiikka ja toimintaohjeet, asetetaan tavoitteet, tehdään vastuiden määrittelyt, annetaan resurssit ja lopuksi verrataan toteutunutta tulosta asetettuihin tavoitteisiin sekä määritellään jatkotoimenpiteet toiminnan kehittämiselle. Tietoturvatavoitteiden on tuettava liiketoiminnan tavoitteita ja tuloksen tekemistä.

Laaksosen ja muiden (2006: 123–124) mukaan tietoturva sisältyy hyvään tietohallintotapaan (IT Governance), jonka perustana on ajatus kokonaisvaltaisesta tietojenkäsittelyn hyödyntämisestä yrityksessä. Hyvässä tietohallintotavassa yrityksen eri yksiköiden tarpeet ja toiminnot kartoitetaan, arvioidaan ja priorisoidaan. Lisäksi hyvälle tietohallintotavalle on tunnusomaista, että toiminta on organisoitua, vastuut on jaettu ja tietohallinnon ratkaisuista tiedotetaan tehokkaasti. Taulukossa 2 on esitetty Laaksosen ja muiden (2006: 123–124) mukaiset vaatimukset, jotka yrityksen ylimmän johdon tulisi huomioida yrityksen hyvää tietohallintotapaa käsitellessään.

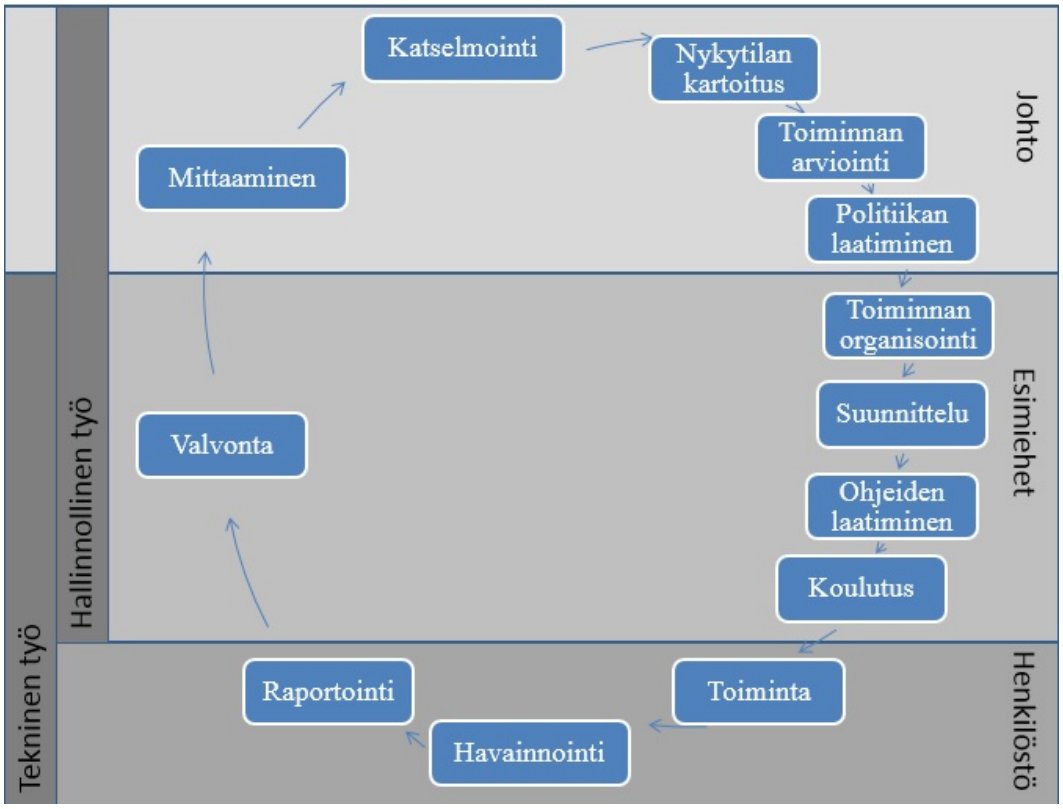
Taulukko 2. Hyvän tietohallintotavan vaatimukset (Laaksonen ym. 2006: 123–124).

Yrityksen johdossa tulee olla riittävästi tietotekniikkaosaamista. Kaikkien yrityksen johtajien tulee tunnistaa ja ymmärtää yrityksen tärkeimmät tietojenkäsittelyriskit. Tietohallinnon ja tietoturvan toiminta sekä valvonta ja hallinnointi tulee erottaa toisistaan. Tietohallinnon ja -turvan vastuut tulee määritellä selvästi. Myös vastuista keskustelu tulee olla selvää. Tietohallintostrategia tulee olla tietohallinnon ja liiketoimintajohdon määrittämä ja hyväksymä. Liiketoiminnan tulee määrittää ja kommunikoida tietojärjestelmille asetettavat vaatimukset. Tämä koskee myös tietoturvavaatimuksia. Projektinhallintamenetelmien ja -käytäntöjen tulee soveltua myös yrityksen tietotekniikkaprojekteihin. Riskienhallintaperiaatteiden ja -menetelmien tulee kattaa myös tietotekniikka ja tietoturva. Yrityksen liiketoiminnassa on hyödynnettävä mahdollisimman tehokkaasti tietojärjestelmiä, minkä varmistamiseksi on yrityksessä järjestettävä riittävästi koulutusta. Tietotekniikasta ja tietoturvasta vastuussa olevien tahojen on ymmärrettävä yrityksen liiketoimintastrategia ja sen vaikutukset.

Fyysisen turvallisuuden tavoitteena on varmistaa yritykselle turvallinen fyysinen toimintaympäristö, jossa ei ole häiriöitä. Tietoturvan ylläpitämisen perustana on toimitilojen suojaaminen, mikä on ensimmäinen vaatimus tiedon luotettavuuden varmistamiselle. Toimitilojen luokittelu tärkeysjärjestykseen helpottaa tunnistamaan tilojen suojaustarpeen tietoturvan kannalta, jolloin vältytään virhearvioinneilta ja tietoturvaresurssit on helpompi mitoittaa oikein. Myös fyysiseen toimintaympäristöön tulee säännöllisesti tehdä riskikartoitus ja sen korjaus- ja parannustarpeet tulee kirjata ja toteuttaa. Fyysisen turvallisuuden varmistamisessa keskeisimpiä asioita tietoturvan kannalta ovat toimitilojen suojaaminen, lämpötilan ja kosteuden hallinta sekä ylijännitesuojaus ja varavirran saatavuuden varmistaminen. Toimitilojen suojaamisessa on huomioitava varkauden mahdollisuus, tulipalon ja vesivahingon estäminen sekä lämpötilan ja kosteuden nousun hallinta, sähköhäiriöiden huomioiminen sekä pölyn muodostumisen estäminen. (Laaksonen ym. 2006: 125–127.)

Kuviossa 3 on esitetty Laaksosen ja muiden (2006: 120–123) mukaisesti yrityksen tietoturvaprosessin (ts. tietoturvan toteuttamisen) vaiheet. Kuviossa tietoturvatyö on jaettu hallinnolliseen ja tekniseen työhön. Tietoturvatoimijoita yrityksen-

sä ovat yrityksen johto, esimiehet ja henkilöstö. Tietoturvaprosessi alkaa johdon aloitteesta. Esimiehet tekevät tarvittavan kehitystyön. Tietoturvan toteuttamiseen osallistuvat kaikki työntekijät. Tietoturvahavainnoista raportoidaan esimiehille. Prosessin päätteeksi yrityksen johto mittaa tietoturvan toteutumista ja vertaa toteutunutta alussa asetettuihin tavoitteisiin.



Kuvio 3. Tietoturvaprosessin vaiheet (Laaksonen ym. 2006: 120).

Kuvion 3 tarkemmassa tarkastelussa nähdään, että tietoturvaprosessi alkaa johdon päätöksestä tietoturvan katselmoinnilla, jolla arvioidaan muutostarpeet. Johto tekee katselmoinnin nykytilan kartoituksella ja toiminnan arvioinnilla. Tulosten perusteella johto laatii tietoturvapolitiikan. Politiikan pohjalta esimiehet organisoivat tietoturvatoiminnan yrityksessä käytännössä. Tämä tarkoittaa vastuuhenkilöiden nimeämistä ja tietoturvatavoitteiden saavuttamisen valvontaan tarvittavien raportointi- ja seurantajärjestelmien suunnittelemista. Tämän jälkeen tietoturva sovitetaan yrityksen päivittäiseen toimintaan, jolloin suunnitellaan toteuttaminen, ohjeistetaan toiminta ja järjestetään tarvittava koulutus. Tietoturvan kouluttaminen, perehdyttäminen ja tiedottaminen ovat tehokkaimpia, kun ne integroidaan osaksi yrityksen muiden toimintojen kouluttamista, perehdyttämistä ja tiedottamista. Näin yksittäinen työntekijä näkee tietoturvan osana kaikkien työntekijöiden toimenkuvaa. Työntekijät huomioivat tietoturvan päivittäisessä toiminnassaan, havainnoivat tietoturvan toteutumista ja raportoivat mahdollisista epäkohdista

esimiesten luoman raportointi- ja seurantajärjestelmän mukaisesti. Esimiesten tehtävänä on valvoa tietoturvan toteutumista. Johto suorittaa tietoturvan mittaamista, jossa se vertaa päivittäistä toimintaa asetettuihin tietoturvatavoitteisiin. Samalla selvitetään toimintatapoja ja muita kohteita, jotka vaativat parannusta sekä osoitetaan tietoturvakehityksen suunta. Mittauksen tuloksista havaittujen puutteiden pohjalta tehdään parannusehdotuksia, jotka otetaan pohjaksi uuteen katselmointiin, kun aloitetaan uusi tietoturvaprosessi. (Laaksonen ym. 2006: 120–123.)

Yrityksen tietoturvaongelmista aiheutuvista seuraamuksista, kuten toimintakatkoksista tai maineen menetyksestä, kärsii aina asianomainen yritys. Vaikka tietoturvan hoitaminen olisi ulkoistettu, toiminnan asianmukaisesta toteuttamisesta tulee siksi huolehtia samoin kuin, jos yritys hoitaisi tietoturvan itse. (Laaksonen ym. 2006: 239.) Ihminen ja ihmisen toiminta on useimmiten tietoturvan suurin uhka (mm. Heljaste ym. 2008: 69; Tietoturva ry 2010). Ihmisen oma maalaisjärki on merkittävin osa tietoturvaa ja pelkästään maalaisjärkeä käyttämällä selvitään useimmista tietoturvan asioista (Heljaste ym. 2008: 69). Keskuskauppakamarin ja Helsingin seudun kauppakamarin (2008: 17) tekemän tutkimuksen mukaan, kun yrityksen koko kasvaa, myös työntekijöiden tekemät rikokset yleistyvät. Työntekijöiden tietoturvakäyttäytymiseen vaikuttavat Laaksosen ja muiden (2006: 249, 255) mukaan tiedon lähteet, vanhempien kollegojen antama esimerkki ja työntekijän oma maalaisjärki sekä päätöksentekotaidot. Työntekijä saa tietoturvatietoa yrityksen arvoista, tietoturvapolitiikasta ja -ohjeista sekä koulutuksista. Erityisesti tietoturvapolitiikka ja -ohjeet ovat merkittävässä roolissa työntekijän toimintatapojen muotoutumisessa. Pelkät ohjeet, miten tulisi toimia, eivät riitä, vaan on tärkeää kertoa myös suositeltavien toimintatapojen perimmäiset syyt. Heljaste ja muut (2008: 72) pitävät tietoturvasäännöstön laatimista keskeisenä osana luotettavan yritysympäristön luomista. Säännöstön tulisi olla lyhyt, selkeä ja käytännönläheinen. Merkittävintä on, että yrityksen johto sitoutuu tietoturvaan ja, että se näkyy yrityksen työntekijöille.

Yrityksen tietoturvan tasoa tulee valvoa, seurata ja mitata. Valvontaa ja seurantaa tehdään kuten mitä tahansa yrityksen muutakin johdon valvontaa ja seurantaa. Tietoturvan valvonta keskittyy tietoturvatoimenpiteillä saavutetun suojaustason seuraamiseen. Valvonnalla varmistetaan tietoturvan riittävyys ja tietoturvatoiminnan oikea suunta. Valvonnan ja mittaamisen tavoitteena on kerätä tietoa tietoturvapuutteista ja -heikkouksista sekä löytää uusia tietoturvan kehityskohteita. Keskitettyä tietoturvaseurantaa tekevät tietohallinto, tietojen omistajat, järjestelmien pääkäyttäjät, liiketoimintayksiköiden esimiehet ja tietoturvaorganisaatio. Lisäksi jokaisen työntekijän tulee valvoa tietoturvan toteutumista oman toimintaympäristö osalta. (Laaksonen ym. 2006: 261.)

Tietoturvatoiminnan tavoitteiden saavuttamistason ja vaikutusten mittaaminen on tärkeää, koska vain mitattavissa olevaa toimintaa pystytään johtamaan (Leppänen 2006: 177). Valtiovarainministeriön (2006: 29, 11, 14) julkaisun mukaan tietoturvan arviointi on tietoturvauhkien ja -haavoittuvuuksien tunnistamiseksi tehtyjä järjestelmällisiä toimenpiteitä. Tietoturvan arvioinnin tavoitteena on varmistaa yrityksen toiminnan luotettavuus, löytää yrityksen tietoturvan vaarantavat uhat sekä varmistaa, että yrityksessä on huolehdittu tiedon luottamuksellisuudesta, eheydestä ja käytettävyydestä. Yrityksen johto vastaa arvioinnista. Jokainen tietoturvan osa-alue voidaan jakaa arviointia varten neljään kohteeseen, jotka ovat tekninen tietoturva (järjestelmät ja laitteet), tietoturvakäytännöt (prosessit ja ihmiset), johtamisjärjestelmät ja -menetelmät (toiminta) sekä tietoturvapoikkeamat (häiriöt, vaaratilanteet ja katkokset). Kukin tietoturvan osa-alue voidaan arvioida erikseen. Tietoturvan osa-alue voidaan arvioida kokonaan tai osittain. Tietoturvan arviointia vaikeuttavat arviointiin perehtyneiden työntekijöiden riittämättömyys, palveluiden ulkoistaminen sekä yrityksen ja palvelutoimittajan tietoverkkojen yhteydet.

Tietoturvan arviointi voidaan Valtiovarainministeriön (2006: 39–46) julkaisun mukaan tehdä yrityksen toimintoihin pohjautuen. Tällöin arvioitavia kohteita ovat johtaminen ja tulosohjaus, toimitilaturvallisuus, prosessit, toiminnan jatkuvuus, riskikartoitus, tietojenkäsittelyn valmiussuunnittelu ja ulkoistaminen. Arvioitavia kohteita ovat myös laitteistot, tietojärjestelmät, tietoliikenne, lokien käyttö, työntekijät ja heidän toimintansa, projektityöskentely, tietoturvakoulutus, tietoturvanohjeistukset sekä asiakirjaturvallisuus ja tietosuoja.

Arviointia, jossa arvioija ja arvioijan arvostukset vaikuttavat tulokseen, kutsutaan subjektiivista mittaamiseksi. Jos tulos on arvioijasta riippumaton, kutsutaan sitä objektiiviseksi mittaamiseksi. Tietoturvan mittaamisella halutaan saavuttaa hyvä tietoturvan taso. Tietoturvatason säännöllisellä mittaamisella on useita tavoitteita. Ensinnäkin pyritään löytämään mahdollisimman monta yrityksen tietoturvassa olevista heikkouksista ja aukoista. Mittaamisella halutaan löytää uudet syntyneet heikkoudet ja aukot mahdollisimman aikaisessa vaiheessa. Toisaalta mittaamisella luodaan vertailuaineistoa, jotta tietoturvaa pystyttäisiin kehittämään yrityksessä. Mittaustulosten perusteella laitetaan tärkeysjärjestykseen tietoturvaa koskevat hankinta- ja muut päätökset sekä kohdennetaan tietoturvaa parantavat toimenpiteet oikein. Tavoitteena on myös selvittää hyödyttävät ja vajaatehoiset tietoturvainvestoinnit. Tulosten avulla tehdään myös päätöksiä työntekijöiden tietoturvakoulutuksen tarpeista. Mittaustuloksilla vaikutetaan yrityksen sidosryhmiin sekä nostetaan yrityksen imagoa ja parannetaan yrityskuvaa. Tavoitteena on myös lisätä yrityksen tuottavuutta sekä ylläpitää ja parantaa yrityksen kilpailukykyä. (Laaksonen ym. 2006: 268–269.)

Laaksonen ja muut (2006: 269–271) jatkavat, että tietoturvan mittaamisessa on oleellista määritellä mitattava kohde. Lisäksi on mietittävä miten mitattava kohde vaikuttaa yrityksen tulokseen ja toiminnan hyvyyteen. Ennen mittaamista tulee pohtia mittauksen tavoitteita. Vasta näiden selvittyä pystytään määrittelemään mittarit ja mittausasteikko sekä mittaamaan tietyn kohteen määrä tai laatu. Mitatun kohteen vaikutus ja tuloksen hyvyys on helpointa arvioida vertaamalla tulosta edellisen mittauksen tulokseen tai yrityksen toiminnan tavoitteisiin. Hyvä tietoturvamittari on luotettava, yksiselitteinen ja helppolukuinen. Se myös soveltuu tarkoitukseensa, keskittyy olennaisen kohteen mittaamiseen ja ilmaisee kehityksen suunnan.

Tietoturvakoulutuksen tavoitteena on Laaksonen ja muiden (2006: 254–255) mukaan suojata yrityksen tieto tarkoituksenmukaisesti ja kustannustehokkaasti. Koulutuksen tulisi pohjautua tietoturvapolitiikkaan ja -ohjeisiin, yrityksen prosessikuvauksiin sekä tietoturvapuutteisiin, jotka ovat ilmenneet johdon tietoturvakatselmoinnissa tai -auditoinnissa. Työntekijöiden motivaatiolla on suora vaikutus koulutuksen tehokkuuteen. Koulutuksessa tulee huomioida, että kunkin työntekijän tulee ymmärtää omaan työhönsä liittyvät riskit sekä tietää miten kyseisten riskien toteutumista minimoidaan. Yritysten tietoturvan kehittämisessä suurimmat virheet tehdään tietoturvatoiminnan organisoimisessa ja työntekijöiden kouluttamisessa.

3.2 Tietoturvadokumentointi

Tämän tutkimuksen keskeinen tekijä ovat viranomaistahojen tietoturvaohjeistukset. Tietoturvan ylläpito ja edistäminen edellyttävät dokumentointia. Dokumentoinnin tulee olla tarpeeksi yksityiskohtaista ja käyttää ennalta sovittua rakennetta. Dokumentointi helpottaa tietohallintoa, mutta se jää usein tekemättä. Dokumentoinnissa kirjataan löydetyt ratkaisut ja perustelut käyttöönotettujen ratkaisujen valinnalle. (Hakala ym. 2006: 32, 103.) Laaksonen ja muut (2006: 149) korostavat, että yrityksen tietoturvaan liittyvien toimintatapojen prosessikuvaukset ovat merkittävässä roolissa, kun tietoturvaa kehitetään yrityksessä. Haasteena yrityksissä on saada työntekijät noudattamaan tietoturvasääntöjä ja -politiikkaa (Helenius 2005, 2). Hakala ja muut (2006: 32) lisäävät, että tietoturvadokumentit laaditaan eri tarkoituksiin. Dokumentti on yleisluontoinen tai yksityiskohtaisempi kuvaus kohteestansa. Yleisluontoiset dokumentit on tarkoitettu yrityksen toiminnan karkeaan ohjaukseen eli strategisten linjausten kuvaamiseen. Tällaisia ovat esimerkiksi tietoturvapolitiikkadokumentit. Yksityiskohtaisemmille dokumenteille on hyvä luoda tyyppiluokittelu, jossa kerrotaan suositus tietojen tallettamiselle, dokumentin sisältävien tietojen arkaluonteisuus, luottamuksellisuus sekä tiedot dokumentin säilyttämisestä ja hävittämisestä.

Yrityksessä voidaan luoda tietoturvaohjelma, jolla pyritään tietoturvan tavoitteisiin. Laaksonen ja muut (2006: 128–138) näkevät ohjelman sisältävän tietoturvatavoitteiden saavuttamiseksi tehtävät toimenpiteet. Tietoturvaohjelmalla varmistetaan tietojen käytettävyys, eheys ja luottamuksellisuus. Siinä on huomioitava viestinnän luottamuksellisuus, yksityisyydensuoja ja sananvapaus. Tietoturvaohjelmassa kerrotaan tietoturvan toimintatapojen keskeisistä suuntaviivoista ja linjauksista, kuten tietoturvatoiminnan järjestelyistä, vastuista, työntekijöiden tehtävistä, ohjeistuksista, koulutuksesta ja valvonnasta. Erityisesti roolien ja vastuiden määrittely on tietoturvan kannalta tärkeää. Rooleja ovat ylin johto, tietoturvaorganisaatio, tiedon omistaja, prosessin omistaja, järjestelmän pääkäyttäjä, tietohallinto, tietoturvan sisäiset ja ulkoiset tarkastajat, työntekijät sekä ulkoiset sidosryhmät. Tietoturvaohjelman toteutumisesta vastaava tietoturvaorganisaatio koordinoi tietoturvapolitiikan ja toimintaohjeiden laatimisen, järjestää tietoturvakoulutusta sekä valvoo tietoturvatoimintaa ja raportoi siitä. Tiedon omistaja on tiedon luoja tai tuottaja. Prosessin omistaja on käytännön vastuussa liiketoiminnan prosessista. Järjestelmän pääkäyttäjä huolehtii sovelluksen toiminnasta ja tuotettavan tiedon luotettavuudesta. Tietohallinnon tehtävänä on rakentaa ja ylläpitää liiketoimintaa tukevia järjestelmiä sekä turvata tietojärjestelmien käytettävyys. Yrityksen johto vastaa ulkoisten sidosryhmien toiminnasta.

Yrityksen tietoturvaohjelma muodostuu *tietoturvapolitiikasta* ja ohjeistosta. Tietoturvaohjelman toimenpiteet, kuten noudatettavat tietoturvaperiaatteet, yleiset toimintalinjat ja tietoturvan organisointi, kirjataan yrityksen tietoturvapolitiikkaan. Tietoturvapolitiikan ja ohjeiden kattavuus, selkeys ja yhdenmukaisuus vaikuttavat työntekijälle muodostuvaan käsitykseen tietoturvan toimintatavoista. Politiikka on yrityksen johdon kannanotto yrityksen tietoturvan puitteille, linjauksille ja vastuille. Tietoturvapolitiikka kattaa yrityksen kaikki toiminnot. Politiikka toimii perustana tietoturvaohjeistukselle ja -koulutukselle. Ohjeisto on käytännössä suuri määrä ohjeita, joista kukin on laadittu yhteen tiettyyn tarkoitukseen. Ohjeet ovat yrityksen laatimia määrityksiä asioiden toteuttamiseksi sekä toimintaohjeita tietoturvan käsittelyyn. Ohjeilla pyritään estämään tietoturvaongelmien syntyminen. Ohjeissa tulee huomioida myös poikkeusolosuhteet. Yrityksissä on alettu sisällyttää tietoturvaan liittyvät ohjeistukset yrityksen muihin toimintaohjeisiin. Tällä halutaan pienentää yrityksissä olevien ohjeistusten määrää. (Laaksonen ym. 2006: 145–146, 249, 21.) Heljaste ja muut (2008: 13) korostavat, että ohjeet vaativat aina kouluttamisen.

Hakalan ja muiden (2006: 7–8) mukaan tietoturvapolitiikka on tärkein yrityksen tietoturvakäytäntöä ja tietoturvaprosessia ohjaava yksittäinen dokumentti. Yrityksen ylin johto hyväksyy käytännön. Tietoturvapolitiikassa määritellään yrityksen käytäntö omissa liiketoimintaprosesseissaan sekä yrityksen liiketoimintaan tarvit-

tavissa tärkeimmissä tietojärjestelmissä. Käytäntö muodostuu useista käytänteistä. Tietoturvapolitiikkaan kirjattavien käytänteiden tavoitteena on saavuttaa haluttu tietoturvan taso. Myös Leppänen (2006: 177–179) antaa ohjeita tietoturvapolitiikan laatimiselle käsitellessään teoksessaan turvallisuuspolitiikkaa. Koska tietoturva on yksi perinteisen turvallisuusjohtamisen osa-alue, voidaan Leppäsen (2006: 177–179) mukaan turvallisuuspolitiikasta kertovien asioiden katsoa sopivan yleisellä tasolla myös tietoturvapolitiikan käsittelyyn. Tietoturvapolitiikan tulee olla lyhyt ja ytimekäs johdon tekemä määrittely tärkeistä toiminnoista, joilla turvataan yrityksen toiminnan jatkuvuus. Tietoturvapolitiikassa määritellään yrityksen tietoturvatoiminnan sisältö. Sillä osoitetaan johdon sitoutuminen tietoturvatoimintaan sekä kerrotaan, mitä asioita tietoturvatoiminnassa painotetaan. Tietoturvapolitiikalla kerrotaan julkisesti, mikä merkitys tietoturvalla on yritykselle ja mitkä ovat yrityksen tietoturvatoiminnan tavoitteet, mikä asema tietoturvatoiminnalla on yrityksen strategiassa sekä kenen vastuulla tietoturva-asiat ovat. Heljaste ja muut (2008: 12–13) lisäävät, että tietoturvapolitiikan olemassa olon merkitys korostuu alle 100 työntekijän yrityksessä. Tietoturvapolitiikassa kuvataan menetelmät, joilla yritys ylläpitää ja kehittää tietoturvaa. Lisäksi tietoturvapolitiikassa määritellään tietoturvavastuut. Tietoturvapolitiikan lisäksi yrityksellä voi olla tarvittaessa erilaisia ohjeita.

Hönen ja Eloffin (2002a) mukaan tietoturvapolitiikalla määritellään selkeät rajat yrityksen tietoturvalle. Sillä osoitetaan yrityksen johdon sitoutuminen ja tuki tietoturvalle. Tietoturvapolitiikan tehtävänä on tukea yrityksen visiota ja missiota. Höne ja Eloff (2002b) ovat myös todenneet, että tietoturvapolitiikka on tietoturvan tärkeimpiä työkaluja. Tietoturvapolitiikan laatiminen ei ole kuitenkaan helppoa, minkä seurauksen tietoturvapolitiikan laatijat nojautuvat olemassa oleviin ohjeisiin. Ohjeina käytetään esimerkiksi erilaisia kansainvälisiä tietoturvastandardeja. Tutkimuksen mukaan standardeja voidaan käyttää pohjana politiikan laatimiselle, mutta pelkästään niihin politiikkaa ei voida perustaa. Kansainväliset tietoturvastandardit eivät ole kattavia ja niiden sisältö on enemmän tietoturvapolitiikan käyttöönottoa ohjaava. Tutkimuksen mukaan on tärkeää, että tietoturvapolitiikka laaditaan yrityksen kulttuuriin sopivaksi.

Tietoturvapolitiikka on osa yrityksen tietoturvasuunnittelua, mutta Hakala ja muut (2006: 7) näkevät tietoturvapolitiikan myös osana organisaation tieto- ja viestintäpolitiikkaa. Mikäli yritykselle on laadittu kokonaisturvapolitiikka, on tietoturvapolitiikka sen osa. Tietoturvapolitiikan laatimisesta vastaa yrityksen ylin johto. Valtiovarainministeriön (2006: 47) julkaisussa todetaan, että tietoturvapolitiikassa yrityksen johto määrittelee yrityksen tietoturvaperiaatteet ja toimintatavat tietoturvalle. Hallinnollisen tietoturvan arviointi perustuu tietoturvapolitiikkaan. Liikenne- ja viestintäministeriön (2010) julkaisussa sen sijaan määritellään tietotur-

vapolitiikan tavoitteeksi edistää elinkeinoelämän, kansalaisten ja julkishallinnon luottamusta palveluiden turvallisuuteen. Luottamusta pyritään luomaan palveluiden helppokäyttöisyydellä, yksityisyyden suojan varmistamisella riittävällä tasolla sekä huolehtimalla palveluiden sisältöjen aitoudesta.

Tietoturvapolitiikka suositellaan Hakala ja muiden (2006: 7–9) mukaan kirjoitettavaksi yleisellä tasolla. Kuitenkin monesti se kirjoitetaan liian yleisluonteiseksi, jolloin sen sisällöstä ei ole konkreettista apua yrityksen tietoturvan ylläpitämiselle. Tavoitteena on, että tietoturvapolitiikan sisältönä kerrotaan miten yrityksen tietoturvaa hallinnoidaan ja kehitetään, mikä turvataso yrityksen eri liiketoimintaprosessien tiedoille vaaditaan sekä menetelmät, joilla turvatasoon pyritään. Tietoturvapolitiikan sisältö tulee olla ymmärrettävissä myös, vaikka ei olisi tietojenkäsittelyn tai hallinnon ammattilainen. Tietoturvapolitiikka on julkinen dokumentti, minkä takia se ei saa sisältää sellaista tietoa, mikä helpottaa hyökkäyksen tai tietomurron suunnittelua yritystä kohtaan. Se on tarkoitettu yrityksen kaikille työntekijöille, mutta antamalla sen myös asiakkaidensa ja yhteistyökumppaniensa käyttöön yritys kertoo tavoitteesta suojata omat ja sidosryhmiensä tiedot. Tietoturvapolitiikka toimii ohjeena yrityksen tietojärjestelmien suunnittelijoille sekä yrityksen liiketoimintaprosesseista vastaaville esimiehille. Tietoturvapolitiikka kirjoitetaan keskipitkälle (n. 5 vuotta) ja pitkälle (n. 10 vuotta) aikavälille, mutta sen sisältöä tarkistetaan vuosittain vastaamaan yrityksen sen hetkistä toimintaa ja tietoturvatarpeita.

Tietoturvapolitiikan sisällöstä on olemassa useita malleja. Laaksonen ja muut (2006: 147–148) korostavat, että tietoturvapolitiikan tulee olla lyhyt ja selkeä ja se tulee kirjoittaa yleisellä tasolla. Tietoturvapolitiikka sisältää yleensä tietoturvan tavoitteet, tietoturvatoiminnan merkityksen yrityksen liiketoiminnassa sekä ohjeistuksen tietoturvaan suhtautumiselle, tietoturvan vastuut ja roolit, tietoturvakoulutuksen merkityksen ja sen vaatimukset, tietojenkäsittelyn suojaamisen suuntaviivat, seuraukset tietoturvapolitiikan laiminlyönneistä sekä tietoturvan yleiset linjaukset yrityksen liiketoiminnan jatkuvuus- ja toipumissuunnitelman toteuttamisessa. Hakala ja muut (2006: 8–9) pitävät yritykselle laadittua tietoturvapolitiikkaa tärkeimpänä yrityksen tietoturvaohjeistamisen dokumenttina. He puolestaan sisällyttävät hyvin laadittuun tietoturvapolitiikkaan seuraavat 11 asiaa:

- yrityksen oma käsitys ja määritelmä yritykselle keskeisen tietoturvan sisällöstä
- tietoturvan keskeiset kohteet ja laajuus yrityksessä sekä tietoturvan tärkeys yrityksen toiminnalle
- maininta, että yritysjohto tahtoo tietoturvatavoitteiden saavuttamisen ja tietoturvaperiaatteiden noudattamisen olevan osa yrityksen liiketoimintastrategiaa ja niillä on yritysjohdon tuki

- rakenteet, joilla tietoturvaan pyritään, erityisesti rakenteet riskien tunnistamiselle ja hallinnalle
- yhteenveto tietoturvakäytännöistä sekä noudatettavista yleisperiaatteista ja standardeista
- yhteenveto vaatimuksista, joita lainsäädäntö, sopimukset ja kauppatavat asettavat tietoturvalle
- yhteenveto, millaisilla toimilla turvallisuusajattelua edistetään ja millaista koulutusta siitä järjestetään
- kuvauksen liiketoiminnan jatkuvuuden hallinnasta ja tietoturvan liittymisestä liiketoimintaan
- määritelmät tietoturvan vastuualueista ja turvallisuuteen vaikuttavien tapahtumien raportoinnista
- käytännöt ja seuraamukset, jotka aiheutuvat turvallisuuspolitiikan rikkomuksista
- luettelo tietoturvaohjeista ja standardeista, joilla tietoturvapolitiikkaa tarkennetaan.

Laaksonen ja muut (2006: 150–160) lisäävät, että tietoturvadokumentoinnissa tulee tietoturvapolitiikan lisäksi luoda dokumentaatio yrityksen keskeisimmistä tietoturvaan liittyvistä prosesseista, joita ovat riskien arviointi, tietoturvan testaaminen sekä käyttöoikeuksien hallinta. Lisäksi tulee dokumentoida lisenssien ja laitteiden hallinta sekä järjestelmämuutosten hallinta, tietoturva-aukkojen ja päivitysten seuranta, tietojen ja järjestelmien luokittelu sekä tietoturvaloukkausten ja -heikkouksien raportointi. Laaksonen ja muut (2006: 151) myös huomauttavat, että käyttöoikeuksien hallintaprosessi on yksi tärkeimmistä yrityksen tietoturvaan vaikuttavista prosesseista. Prosessissa käyttöoikeuksia luodaan, muutetaan ja poistetaan sekä seurataan. Yksinkertaisimmillaan prosessi on, kun käyttöoikeudet annetaan käyttäjille kunkin työtehtävien vaatimien tarpeiden mukaan ja, kun oikeuksien tarve päättyy, poistetaan oikeudet välittömästi. Käytännössä järjestelmien ja käyttäjien suuri määrä tekee prosessista kuitenkin paljon monimutkaisemman. Myös vaikeus selvittää käyttöoikeuksien asianmukaisuus sekä käytössä olevat yhteiskäyttöiset käyttäjätunnukset aiheuttavat puutteita tietoturvaan.

Lisenssien ja laitteiden hallinnasta on hyvä luoda dokumentaatio, jossa kuvataan yrityksen tietojenkäsittelyomaisuus. Omaisuuden hallinta prosessimaisesti alkaa yrityksen liiketoiminnan ja käyttäjän tarpeesta ja se pyrkii hallinnoimaan lisenssejä ja laitteita kustannustehokkaasti. Dokumentaatiota on ylläpidettävä ja sen tulee kattaa myös tietojärjestelmämuutokset. Hallittu järjestelmämuutos sisältää muutoksen vaikutusten arvioinnin, perustellun syyn muutokselle ja sen hyväksymisen sekä onnistuneen testauksen. Hyvät ja turvalliset järjestelmät ovat ehdoton edellytys tietoturvan toteutumiseen tietojärjestelmien käytössä. Oleellista on myös jär-

jestelmien ja sovelluksien tietoturva-aukkojen, haavoittuvuuksien ja riskien seuraaminen. Huomioita havaituista epäkohdista voi löytää esimerkiksi järjestelmä- ja ohjelmistotoimittajilta, CERT-FI:ltä sekä virustorjuntasovellusten toimittajilta. Havaittujen tietoturvaloukkausten ja -heikkouksien raportoinnilla pyritään riittävän nopeaan ja oikeanlaiseen toimintaan. Raportointikäytäntö tulee olla yrityksen kaikkien työntekijöiden sekä myös ulkopuolisten sidosryhmien, kuten yrityksen käyttämien konsulttien ja alihankkijoiden tiedossa. Käytännössä on esitettävä selkeästi raportointikanava ja -menetelmä. Yksinkertaisen lomakkeen käyttäminen raportointivälineenä auttaa dokumentoinnissa, mutta havainnosta ilmoittaminen myös suullisesti tulee olla mahdollista, jotta raportointi varmasti toteutuu. (Laaksonen ym. 2006: 152–156, 160.)

Yrityksen tietoturvan toteutuminen edellyttää, että yrityksen työntekijät koulutetaan tunnistamaan yrityksen tietoturvakäytännöt ja heitä vaaditaan noudattamaan käytäntöjä. Toimintaohjeet on laadittava huomioiden käyttötarkoitus ja käyttäjät. Tietoturvan toteuttaminen ja sitä tukevien toimintaohjeiden noudattaminen tulee sisältyä päivittäiseen työskentelyyn. (Laaksonen ym. 2006: 161–171.) Toimintaohjedokumenttien tulee Laaksosen ja muiden (2006: 161–171) mukaan kattaa ainakin tietojen luokittelu, tietovälineiden käsittely, haittaohjelmien torjunta, Internetin käytön periaatteet, sähköpostin avaaminen ja sen käytön periaatteet, käyttäjätunnuksen ja salasanan ohjeistukset, matkakäytön ja etätyön ohjeistukset sekä varmistuskäytännöt. Lisäksi toimintaohjeissa on tuotava esille niin sanotun puhtaan pöydän periaate.

Tietojen luokitteludokumenteissa on kuvattava tiedon luokka, periaatteet tiedon käsittelylle, määrittely tiedon salaamisen pakollisuudesta, tiedon salaamiseen vaadittavat toimenpiteet sekä toimintatavat, joilla tieto hävitetään. Tiedon luokista on selitettävä kunkin luokan merkitys. Tiedon käsittelystä on käytännössä ohjeistettava ainakin kirjepostissa, sähköpostissa ja puhelimessa toimitettavan tiedon rajoitukset. Salattavasta tiedosta on korostettava varmuuskopioinnin merkitystä. Tiedon hävittämisessä on varmistettava erityisesti luottamuksellisen tiedon oikeanlainen tuhoaminen. Tietovälineiden käsittelyohjeissa tulee kertoa sallitut laitteet ja sallittu käyttö, menettelytapa tietovälineen kadotessa tai rikkoutuessa sekä antaa ohjeet tietoliikenneyhteyksien suojaamisesta ja varmistuskäytännöistä. Lisäksi ohjeessa on kerrottava tekniset keinot, joilla voidaan rajoittaa ja valvoa tallennusvälineiden käyttöä. Ohjeessa on kerrottava myös mitä tietoa saa säilyttää liikuteltavilla tallennusvälineillä. Ohjeita on päivitettävä esimerkiksi, kun käsittelylaitteita uudistetaan. (Laaksonen ym. 2006: 161–162.)

Haittaohjelmien ohjeistuksista kertoessaan Laaksonen ja muut (2006: 163) tarkoittavat haittaohjelmilla sovelluksia, jotka suorittavat tietojärjestelmässä käyttä-

jän käytöstä aiheutumattomia tapahtumia sekä sovelluksia, jotka aiheuttavat tahattomasti tietojärjestelmille haittaa. Laaksosen ja muiden mukaan haittaohjelmien torjunnassa tulee ensinnäkin kieltää selkeästi tiettyjen liitteiden ja viestien avaaminen sekä edelleen lähettäminen. Toiseksi on ohjeistettava miten käyttäjä pystyy välttämään haittaohjelmat ja miten hänen tulee toimia, jos epäilee tietokoneen sisältävän haittaohjelman. Lisäksi toimintaohjeessa on kerrottava mitä haittaohjelmat tekevät näennäisesti ja todellisuudessa.

Internetin käytön ohjeistuksissa Laaksonen ja muut (2006:163–165) toteavat, että Suomessa ei ole tarvetta estää Internetin käyttöä työpaikalla. He kuitenkin lisäävät, että käytön rajoittaminen on järkevää ja käytölle on laadittava selkeät periaatteet. Yrityksessä on oltava selvillä verkon käytöstä aiheutuvat hyödyt ja haitat sekä tunnistettava verkon käyttöön liittyvät tietoturvariskit. Toimintaohjeessa on määriteltävä selkeästi millaiseen tarkoitukseen Internetiä saa käyttää työpaikalla. Erityisen tärkeää on kertoa mahdolliset rajoitukset mihin Internetiä ei saa käyttää sekä millaisten sivustojen selailu on estetty työnantajan toimesta kokonaan. Internetin sopimaton käyttö on kiellettävä selkeästi. Samassa yhteydessä on hyvä muistuttaa, että myös laissa on säädetty kielletystä tietoverkkoihin liittyvästä toiminnasta, esimerkiksi tiedostojen laittomasta jakelusta ja laittoman materiaalin hallussapidosta. Toimintaohjeessa on kerrottava myös miten Internetin käyttöä työpaikalla valvotaan. Internetin käyttö työpaikalla vähäisten yksityisten asioiden hoitamiseen on järkevää sallia ja tämä on hyvä mainita myös toimintaohjeessa.

Sähköpostin käytössä noudatetaan pääpiirteittäin samoja periaatteita kuin Internetin käytössä. Toimintaohjeessa on määriteltävä miten työntekijän toivotaan käyttävän työpaikan sähköpostia. Ohjeessa on hyvä mainita, että vähäinen yksityisasioiden hoitaminen sähköpostilla on sallittua, mutta kuitenkin on hyvä suositella muiden viestintämahdollisuuksien käyttöä yksityisasioiden hoitamiseen. Mikäli työpaikan sähköpostia käytetään yksityiseen viestintään, yksityiset sähköpostit on merkittävä selvästi yksityisiksi. Sähköpostin avaamisessa on huomioitava Laki yksityisyyden suojasta työelämässä -lain luku 6, jossa määritellään työnantajan oikeudet ja mahdollisuudet työntekijän sähköpostiin lähetettyjen sähköpostien avaamisesta. Ohjeessa on hyvä määritellä periaatteet, joilla työnantaja voi sähköpostin otsikosta päätellä, kuuluuko sähköposti työnantajan toimintaan ja voi tarvittaessa lukea työntekijän sähköpostin. Toimintaohjeessa on sähköpostin käyttöön liittyen ohjeistettava menettelytapa työntekijän sairastuessa tai pidemmässä poissaolossa sekä irtisanoutuessa. Ohjeessa on hyvä kertoa periaatteet sähköpostiosoitteiden julkaisemisesta ja neuvoa sähköpostiosoitteen esitystapa. Ohjeistus on annettava myös henkilökohtaisen sähköpostin, väärään osoitteeseen lähetetyn sähköpostin ja perille menemättömän sähköpostin sekä liitetiedostojen ja ros-

kasähköpostin käsittelyyn. Ohjeistus tulee tehdä myös sähköpostin salaukselle. (Laaksonen ym. 2006: 165–166.)

Matkakäyttöä ja etätyötä ohjeistettaessa on tärkeää huomata, että menetetty tieto on yritykselle tavallisesti taloudellisesti suurempi tappio kuin menetetty kannettava tietokone tai muu mobiililaite. Laitteessa oleva tieto ei ole suojattunakaan välttämättä turvassa, jos laite joutuu vääriin käsiin. Tappio on entistä suurempi, mikäli menetetty tieto on tallennettuna ainoastaan menetettyyn laitteeseen. Liikkuvan työn keskeinen tietoturvaa lisäävä toimenpide on liikkuvaa työtä tekevien työntekijöiden ohjeistaminen turvallisista toimintatavoista osana arkipäivän toimintaa. Erityisesti ohjeistaminen tulisi kohdistaa liikkuvan työn riskeihin ja keinoihin suojautua riskeiltä. Matkakäyttöä ja etätyötä ohjeistettaessa sekä laitteiden suojausta varten tulee huomioida missä laitetta aiotaan käyttää ja minkälaista tietoa laitteeseen aiotaan tallettaa. Lisäksi tulee miettiä menetelmät, joilla laitteessa oleva tieto on mahdollista varmistaa. Yksinkertaisinta on pitää kannettavassa laitteessa mahdollisimman vähän tietoa mukana. Lisäksi etäyhteydet tulee tehdä suojatusti. Matkakäytön ohjeessa on edellä mainittujen lisäksi kerrottava miten laitetta tulee kuljettaa, käsitellä ja säilyttää fyysisesti huomioiden laitteen pieni koko, rikkoutumisalttius, tärinä ja lämpötilavaihtelut. Myös lukkojen ja hälyttimien käyttö sekä laitteen lukitsemisen mahdollisuus salasanoin tai erillisavaimin tulee neuvoa ohjeessa. Ohjeessa on huomioitava, että laite unohtuu helposti sekä muistettava kiintolevyjen koko ja varmistaminen. Julkisilla paikoilla työskentelyssä on huomioitava olanylikatselun ja näytön valokuvaamisen mahdollisuus. Vieraiden verkkojen käytössä on huomioitava urkkimisen mahdollisuus. Myös langattoman verkon suojattu käyttö on ohjeistettava. Virussuojaus ja haittaohjelmien torjunta on ohjeistettava. Etätyölaitteet on merkittävä ja niistä tulee löytyä yhteystiedot laitteen muistista tai kiintolevyltä. Ohjeessa on kiellettävä salasanojen säilyttäminen kiintolevyllä. Lisäksi on ohjeistettava, että sovelluksia avattaessa ne eivät saa muistaa käyttäjän salasanoja automaattisesti. (Viestintävirasto 2009b; Laaksonen ym. 2006: 168–169.)

Käyttäjätunnuksen ja salasanojen ohjeistuksesta Laaksonen ja muut (2006: 166–168) toteavat, että yrityksen työntekijöille on tärkeä kertoa yksityiskohtaiset periaatteet salasanan käytölle. Käyttäjätunnukseen ja salasanaan liittyvien ohjeiden perusteleminen on tärkeää. Laiminlyönneistä aiheutuvien riskien kuvaaminen auttaa työntekijää ymmärtämään ohjeiden tärkeyden. Ohjeistuksessa tulee neuvoa miten muodostetaan turvallinen salasana, miten oletussalasana muutetaan, miten salasana vaihdetaan sekä mitä toimenpiteitä käyttäjän tulee tehdä salasanaan liittyen tulevaisuudessa. On myös tärkeä kertoa, että oletussalasana tulee muuttaa heti. Lisäksi tulee ohjeistaa miten tulee toimia, jos salasana katoaa, joutuu väriin käsiin tai syötetään liian monta kertaa väärin. Laaksonen ja muut tuovat esille

myös, että työelämän ja yksityiselämän salasanojen tulee olla eriävät toisistaan. Yrityksessä ei tulisi myöskään olla liian monia käyttäjätunnus-salasana -pareja, jotta työntekijä pystyy muistamaan kaikki ulkoa. On hyvä kirjoittaa ohjeet myös, miten toimitaan, jos joutuu salasanojen kalastelun eli phishing-hyökkäyksen kohteeksi.

Tärkeä tieto tulee varmistaa mahdollisimman nopeasti ja sen varmistamiseen tulee laatia ohjeet. Varmistuskäytännöillä varmistetaan tiedon säilyminen luotettavana ja käytettävänä. Tiedon säilyminen tulee varmistaa myös onnettomuuksissa ja muissa yllättäen tulevissa tilanteissa. Erityisen tärkeää ohjeen laatiminen on esimerkiksi mobiililaitteiden varmistuskäytännön ohjeistamiseen. Varmistuskäytännön ohjeistuksessa on kerrottava tiedon säilytyspaikka ja -tapa sekä arkistointikäytännöt. Myös varmistettuun tietoon tulee olla pääsy niillä, joilla siihen on oikeus. Varmistuskäytännöissä tulee huomioida myös varmistettujen tiedostojen siirto ja palautukset. Erityisen tärkeää on testata ja palauttaa varmistettu tieto silloin tällöin tiedon varmistuksen onnistumisen toteamiseksi. Tiedon varmistamista ei tule jättää pelkästään käyttäjän vastuulle, vaikka hänet ohjeistettaisiin ja koulutettaisiin tiedon varmistamisen käytänteisiin. Kaikkein sujuvinta varmistus on silloin, kun käyttäjä ei edes huomaa tiedon varmistamista. Tämä tarkoittaa käytännössä tiedon keskitettyä tallentamista kaikista ohjelmista verkkolevyille, jotka varmistetaan. Tällainen varmistuskäytäntö ei ole kuitenkaan aina mahdollinen. (Laaksonen ym. 2006: 170–171.) Puhtaan pöydän periaatteella tarkoitetaan, että työpisteisiin ei jätetä työdokumentteja näkyville, vaan pöydät tyhjennetään viimeistään työpäivän päättyessä. Näin dokumentit eivät ole välittömästi nähtävissä ulkopuolisille luvallisestikaan työpaikalla liikkuville henkilöille, kuten siivoojille ja vartijoille. Erityisen huolellinen tulee olla salaisten dokumenttien säilyttämisessä. (Laaksonen ym. 2006: 169–170.)

Liiketoiminnan jatkuvuussuunnitelma on dokumentti, jolla pyritään turvaamaan yrityksen tärkeiden liiketoimintaprosessien toiminta normaalitilanteiden lisäksi häiriötilanteissa ja niiden jälkeen. (Laaksonen ym. 2006: 227–228; Heljaste ym. 2008: 62.) Laaksonen ja muut (2006: 227–228.) lisäävät, että tavoitteisiin päästään järjestelmällisellä käytäntöjen kehittämisellä ja aktiivisella johtamisella. Valtiovarainministeriön (2008) julkaisussa jatkuvuussuunnitelmalla tarkoitetaan kriittisten ja tärkeimpien toimintaprosessien jatkuvuuden turvaamiseksi tehtyä suunnitelmaa, jonka tavoitteena on turvata yrityksen toimintojen, tietojenkäsittelyn ja tiedonsiirron jatkuminen kriisin, katastrofin ja onnettomuuden sekä muutosten ja häiriöiden aikana ja niiden jälkeen. Kattava jatkuvuuden uhkatekijöiden tunnistaminen on vaikeaa. Toipumissuunnitelmalla tarkoitetaan vakavan häiriön aiheuttamaa toiminnan jatkamiseksi tai kokonaan uudelleen aloittamiseksi tehtyä suunnitelmaa (Valtiovarainministeriö 2008; Laaksonen ym. 2006: 227–228). Jatku-

vuus- ja toipumissuunnitelmat tulee kohdistaa yrityksen liiketoimintaprosesseihin, joiden osana tietojärjestelmät ovat. Suunnitelmat käsittelevät kaikkia tietoturvan osa-alueita ja ovat keskeinen osa yrityksen tietoturvaa. Suunnitelmissa tulee huomioida yrityksen sijainti, ympäristö, toiminnan luonne ja laajuus sekä tiedon siirtäminen, muuttuminen ja hävittäminen. (Laaksonen ym. 2006: 228.)

3.3 Tietoturvasuunnittelu ja -riskit

Tietoturvasuunnittelu kattaa kaikki yrityksen toimintaprosessit ja tietojärjestelmät. Hakalan ja muiden (2006: 13–14, 59) mukaan tietoturvasuunnittelua on mahdollista tehdä vasta, kun yrityksen toimintaprosessit ja niitä tukeva organisaatio on määritelty. Mahdollisimman laaja kaikkien työntekijöiden mukaan ottaminen suunnitteluprosessiin takaa parhaan mahdollisen tuloksen. Hyvä tietoturvan suunnittelu vaatii huolellista ja pitkäjänteistä työtä. Hyvän tietoturvasuunnittelun perustana on näkemys yrityksen kokonaisturvallisuudesta, mikä muodostuu fyysisestä turvallisuudesta ja tietoturvasta. Fyysisessä turvallisuudessa suojataan yrityksen työntekijät ja omaisuus erilaisilta riskeiltä. Tietoturvassa suojataan yrityksen tietopääoma sekä estetään tietojenkäsittelylaitteiden ja tietoverkkojen luvaton käyttö.

Hakala ja muut (2006: 17–18) jatkavat, että moderni tietoturvasuunnittelu perustuu kokonaisturvallisuuspolitiikkaan ja liiketoimintaturvallisuuteen. Kokonaisturvallisuuspolitiikka määrittelee tietoturvan tavoitteet. On muistettava, että tietoturva ei ole tärkein tietojenkäsittelyä ja yrityksen toimintaprosesseja ohjaava toiminto, koska liian jäykät turvallisuusmääritykset vaikeuttavat varsinaisen liiketoiminnan ydinprosesseja. Kuitenkin, tietoturva on yrityksen toiminnan ja sen jatkuvuuden mahdollistamiseksi erittäin tärkeä kehittämiskohde. Onnistunut tietoturva vaatii tasapainottelua tietojärjestelmien joustavuuden ja palvelutason sekä tietoturvan välillä. Joustavuuden ja palvelutason lisääminen heikentävät tietoturvatasoa. Parhaan mahdollisen tasapainon löytäminen edellyttää tietohallinnolta syvällistä tuntemusta yrityksen liiketoimintaprosessien luonteesta ja merkityksestä yrityksen toiminnalle.

Hyvä tietoturvasuunnittelu huomioi yrityksen eri tasoilla ja tehtävissä toimivat työntekijät ja heidän tarpeensa. Tämän takia hyvän tietoturvasuunnittelun tekeminen on mahdotonta, mikäli se tehdään pelkästään tietohallinnon tai jonkin muun turvallisuudesta vastaavan tahon voimin. Kokonaan uusi tietoturvasuunnittelu tehdään yleensä tiimi- tai projektityönä, johon olisi hyvä ottaa mukaan ainakin seuraavat yrityksen työntekijät:

- ylimmän johdon edustaja: ohjaa suunnittelua ja huolehtii sen etenemisestä sekä tukee päätettäviä uudistuksia
- turvallisuusjohtamisesta vastaava(t) työntekijä(t)
- yrityksen tärkeimpien liiketoimintaprosessien omistajat eli vastuuhenkilöt
- ruohonjuuritason työntekijät: toimivat työrutiinien asiantuntijoina
- tietohallinnon, tietojenkäsittelyn ja tietotekniikan asiantuntijoita
- työsuojeluorganisaation edustajia
- lisäksi esimerkiksi asiantuntijoita, viranomaisia, lakimiehiä, kiinteistönhoitaja sekä työterveyshuollon edustaja. (Hakala ym. 2006: 18.)

Onnistunut tietoturvasuunnittelu vaatii myös tietojärjestelmien peruskäyttäjien osallistumista suunnittelutyöhön. Tietoturvasuunnittelu voidaan toteuttaa systeemityön vaihejakomallin mukaan, jolloin siihen kuuluvat esitutkimus, määrittely, suunnittelu, toteutus, testaus, käyttöönotto sekä ylläpito ja kehittäminen. Jokaiseen vaiheeseen kuuluu olennaisena osana dokumentointi, millä helpotetaan tietoturvan myöhempää ylläpitoa ja kehittämistä. (Hakala ym. 2006: IV–V, 22–23, 58.)

Esitutkimus-vaiheessa kootaan yrityksen tietoturvaan vaikuttavat standardit ja aiempien tietojärjestelmäprojektien dokumentit sekä kaikki muu materiaali, joka helpottaa tietoturvasuunnittelun tekemistä, kuten säädökset, käsikirjat, tutkimusjulkaisut ja Internet-sivustot. Esitutkimuksessa tarkasteltavia materiaaleja ovat esimerkiksi yrityksen laatukäsikirja, ICT- ja viestintäpolitiikat, kokonaisturva- ja tietoturvapolitiikat, tietoturvasuunnitelma ja -ohjeet, arkistointiohje, työsuojelu-, pelastus- ja valmiussuunnitelmat, laatujärjestelmä- ja tietoturvastandardit, tietojärjestelmä- ja tietoliikennejärjestelmädokumentit, ICT-palveluiden hankintasopimukset sekä henkilötietolaki ja muut yrityksen toiminnassa sovellettavat säädökset. Koottu materiaali analysoidaan, jonka jälkeen päätetään tietoturvasuunnittelussa seuraavaksi tehtävän määrittelytyön organisoinnista ja määrittelydokumenttien rakenteesta. Mikäli yrityksen olemassa olevien dokumenttien rakenne on hyvä, kannattaa niitä hyödyntää tietoturvasuunnittelun määritelmien tekemisessä. Tällöin on tärkeää päättää miten paljon ja miltä osin materiaalia parannetaan. (Hakala ym. 2006: 56–57.)

Määrittely-vaiheen keskeiset osat ovat yleismäärittely, järjestelmäkuvaus ja riskianalyysi. Määrittely on tietoturvasuunnittelun vaativin osa, minkä takia siihen yleensä kuluu myös eniten aikaa. Määrittelyssä kuvataan yrityksen toimintaprosessit sekä niiden käyttämät tieto- ja tietoliikennejärjestelmät. Lisäksi määrittelyssä asetetaan kullekin järjestelmälle turvallisuustavoitteet. Yleismäärittelytyön tavoitteena on ohjata tietoturvasuunnittelutyötä ja antaa yleiskuva määrittelyn sisällöstä. Työ on kattavin, jos tietoturvasuunnitelmaa tehdään yrityksessä en-

simmäistä kertaa, ja sen laajuus vastaavasti pienenee, mikäli tietoturvasuunnittelun tavoitteena on päivittää jo olemassa olevaa tietoturvasuunnitelmaa ja -ohjeistuksia. Työn laajuuteen vaikuttaa myös yrityksen yleis- ja järjestelmäkuvausten dokumentoinnin taso. (Hakala ym. 2006: V–VI, 55, 57.)

Yleismäärittelyssä määritellään yrityksessä käytettävät termit, strategiat ja politiikat, prosessit ja niitä tukeva organisaatio, luokittelujärjestelmät sekä kuvaus- ja dokumenttirakenne. Lisäksi määritellään miten yritys tukee standardinmukaisuutta. Yleismäärittelyssä voidaan laatia myös muita arviointiluokitteluja. Termien tulee kattaa ainakin lainsäädännön termit, yrityksen yleiset turvallisuustermit, liiketoimintaprosessien termit sekä käytettävät tietotekniikka-, tietoliikenne- ja tietojenkäsittelytermit. Strategioista ja politiikoista kannattaa huomioida yrityksen strategiset linjaukset, kuten ICT-politiikka sekä kokonaisturva- ja tietoturvapolitiikat. Prosessien ja niiden organisaatioiden määrittelyn tavoitteena on löytää kaikki yrityksen tietojärjestelmät. Prosesseja ovat esimerkiksi myynti, asiakaspalvelu, markkinointi, tuotanto, ostot, tuotekehitys, logistiikka, työntekijät, talous, johtaminen ja tukipalvelut sekä tietohallinto ja turvallisuus. Prosessien pilkkominen pienemmiksi on tietoturvasuunnittelun kannalta tarpeellista etenkin suurissa yrityksissä. Organisaatiomäärittelyssä huomioitavat dokumentit ovat esimerkiksi toimintaprosessien kuvaukset sekä päätason ja prosessikohtaiset organisaatiokaaviot. Standardinmukaisuusmäärittelyn osalta päätetään käytetäänkö tietoturvasuunnitelman laatimisessa jonkin tietoturvastandardin, esimerkiksi ISO 27002 rakennetta tai noudatetaanko sitä vain joiltakin osin. Määrittelyä tehtäessä on huomioitava yrityksen noudattamat laatujärjestelmästandardit ja laatukäsikirja. Standardinmukaisuusmäärityksissä huomioidaan myös arviointi ja auditointi sekä mahdollinen sertifiointi. (Suomen Standardisoimisliitto 2007; Hakala ym. 2006: V, 58–62.)

Yleismäärittelyssä määriteltävät luokittelujärjestelmät tehdään yrityksen tiedoille ja riskeille. Nämä luokittelujärjestelmät toimivat pohjana riskien analysoimiselle. Tietoturvasuunnittelun yksi tärkeimmistä määrittelyistä on tieto- ja riskiluokkien ja luokittelukriteerien määrittely. Tietojen ja riskien luokittelujärjestelmien tulee olla selkeitä. Järjestelmien tavoitteena on jakaa tiedot ja riskit yhteismitallisiksi kokonaisuuksiksi. Luokittelukriteerien tavoitteena on määritellä perusteet, joilla tiedot ja riskit jaetaan luokkiin. (Hakala ym. 2006: 62, 67.)

Tietojen luokittelujärjestelmän tavoitteena on asettaa tietokokonaisuuksien turvaamistavoitteet sekä määritellä niille tärkeysjärjestys. Näin pyritään määrittelemään ne tiedot, joita suojataan ensisijaisesti. Järjestelmä perustuu tietojen arvoon ja vaikutukseen yrityksen toiminnalle. Tiedon arvoon perustuva luokittelu tehdään tiedon luottamuksellisuuden perusteella. Luottamuksellisuudelle asetettavien

luokkien määrä ja niiden nimet päätetään tietojen luokittelujärjestelmää luotaessa. Luokat voivat olla esimerkiksi julkinen, sisäinen, luottamuksellinen ja salainen. Luokittelu tiedon vaikutuksesta yrityksen toiminnalle tehdään tiedon eheyden ja käytettävyyden perusteella. Käytettävyyttä määrittelevät luokat voivat olla esimerkiksi ei-kriittinen, kriittinen ja erittäin kriittinen, ja eheyttä määrittelevät luokat esimerkiksi virhesietoinen, vähävirheinen ja virheetön. Kullekin luokalle määritellään luokittelukriteerit. Riskien luokittelujärjestelmän tavoitteena on löytää ne riskityypit, joihin pyritään ensisijaisesti varautumaan. Riskit jaetaan luokkiin riskin aiheuttajan perusteella. Riskiluokittelu voidaan tehdä karkeasti luottamuksellisuus-, eheys- ja käytettävyysriskeihin tai se voidaan tehdä tietoturvan osa-alueiden (hallinnollinen, fyysinen, henkilö, tietoaineisto, ohjelmisto, laitteisto ja tietoliikenne) perusteella. Luokittelu voidaan tehdä myös käyttämällä useampaa luokitteluperustetta samanaikaisesti. Yleismäärittelyssä käytettäviä muita arviointiluokitteluja ovat esimerkiksi riskien vaikutusten ja riskien todennäköisyyksien luokittelu. Riskin realisoitumistodennäköisyyden luokittelujärjestelmän luominen kuuluu olennaisena osana tietoturvasuunnittelun yleismäärittelyä. (Hakala ym. 2006: 62–65, 67.)

Jordan ja Silcock (2006: xi–xii) huomauttavat, että merkittävimmät suomalaisyritykset kilpailevat osaamisella. Merkittävimmät tietoturvauhat näissä yrityksissä kohdistuvat erityisesti yrityksen tieto-osaamiseen. Koska tietotekniikka on olennainen väline tiedon hallitsemiseen, korostuu tietojenkäsittelyriskien merkitys. Suojautuminen tietojenkäsittelyriskeiltä onnistuu hyvillä toimintatavoilla ja terveellä maalaisjärjellä. Leppänen (2006: 66–67, 267–268) toteaa, että tieto on yrityksen tavoitteiden toteutumiseen tarvittavaa arvokasta ja merkityksellistä informaatiota. Tiedolla on aina omistaja. Kullekin tiedolle tulee määritellä juridinen omistaja sekä siitä hallinnollisesti vastuussa oleva taho. Tiedolla on myös kohde. Julkisuuslain perusperiaatteena on avoimuus, minkä takia oletus on, että tieto on kaikkien saatavissa ja käytettävissä. Viestintäviraston (2010f) julkaisussa huomautetaan, että tiedon omistaa henkilö, joka on luonut tai tuottanut tiedon. Tiedon omistaja luokittelee tiedon ja dokumentoi sen.

Yrityksen tietojen käsittelyssä tulee huomioida tiedon elinkaari. Elinkaariajattelumallin mukaan aluksi tieto tulee yritykseen, sitten se jaetaan ja sitä käytetään ja lopuksi tieto arkistoidaan tai tuhotaan. Tällainen tiedon elinkaariajattelumalli on tietoturvan kannalta erittäin merkityksellinen. Tiedon omistaja vastaa tiedon elinkaaresta. Se myös päättää milloin tieto muuttuu käyttökelvottomaksi. (Heljaste ym. 2008: 57.)

Tiedon luokittelulla pyritään poistamaan tarve suojata yrityksen kaikki tieto (Heljaste ym. 2008: 57). Tavoitteena on suojata tieto oikealla tasolla. Tietojen luokit-

telulla kerrotaan tiedon merkitys yrityksen liiketoiminnalle. On tärkeää, että etenkin arvokasta tietoa käsittelevät työntekijät ovat tietoisia tiedon arvosta yritykselle. Tiedon luokittelulla kerrotaan myös miten tietoa tulisi käsitellä. Kullekin tietoluokalle on mahdollista dokumentoida omat käsittelysäännöt. Luokittelulla helpotetaan myös yrityksen jatkuvuus- ja toipumissuunnitelmien laatimista. Tietoturvan keskeinen vaatimus käytettävyydestä edellyttää kriittisen tiedon ja tietojärjestelmän toipumista ensimmäisenä. Luottamuksellisuuden toteutuminen edellyttää tärkeimmiksi luokiteltujen tietojen ja tietojärjestelmien suojaamista parhaiten tietomurtoja vastaan. Luokittelulla helpotetaan myös tietojen ja tietojärjestelmien vasteaikojen ja varajärjestelyjen ylläpitoa. (Laaksonen ym. 2006: 156–157, 161.)

Viestintäviraston (2010f) julkaisun mukaan tiedon luokat voivat olla esimerkiksi julkinen, sisäinen, luottamuksellinen ja salainen. Laaksonen ja muut (2006: 157) toteavat vielä, että luokittelu on hyvä pitää maksimissaan 4-luokkaisena, jotta luokittelun tekeminen pysyisi helppona. Tiedon luokittelusta ja tiedon paljastumisesta aiheutuvia seuraamuksia voidaan käytännössä kuvata esimerkiksi taulukossa 3 esitetyllä tavalla.

Taulukko 3. Tiedon luokittelun merkintätapa (Viestintävirasto 2010f).

Tiedon paljastumisesta aiheutuva seuraamus	**Tiedon luokittelu**
Hyötyä yritykselle	Julkinen
Ei hyötyä eikä haittaa yritykselle	Sisäinen
Vahinkoa tai haittaa yritykselle tai työntekijälle	Luottamuksellinen
Vakavaa vahinkoa tai haittaa yritykselle tai työntekijälle	Salainen

Leppänen (2006: 266, 274) lisää luokitteluportaisiin vielä viidennen portaan erittäin salainen tieto. Sillä tarkoitetaan henkilön, yrityksen toiminnan tai valtion turvallisuuden merkittävää vaarantamista.

Kaikkien tiedon käyttäjien tulee käsitellä tietoa yrityksen turvaluokittelussa kuvattujen toimintaperiaatteiden mukaisesti. Valtuutetut tiedon käyttäjät määritellään myös tiedon luokittelun mukaan. Julkisella tiedolla ei ole käyttäjärajoituksia. Sisäistä tietoa saa käyttää kuka tahansa yrityksen työntekijä, mikäli tietoon tai henkilölle ole erikseen määriteltyä rajoitettua jakelu- tai pääsyoikeutta. Luottamukselliseen tietoon on valtuudet vain tiedon omistajan jakelu- tai pääsyoikeuslistalla määritellyillä henkilöillä. Myös salaisen tiedon käyttäjät määritellään tiedon omistajatiedon jakelu- tai pääsyoikeuslistalla. (Viestintävirasto 2010f.) Heljaste ja muut (2008: 69) tuovat esille miten tärkeää on, että luottamuksellisen ja

salaisen tiedon käsittelijä ymmärtää käsiteltävän tiedon luonteen. Keskuskauppakamarin ja Helsingin seudun kauppakamarin (2008: 27) tekemään selvitykseen vastanneista 1286 yrityksestä 36 % ilmoitti, että yrityksellä on tärkeitä tietoja koskeva luokittelu- ja käsittelyohje. Muita tietoja koskeva luokittelu- ja käsittelyohje löytyi 33 % vastanneista yrityksestä.

Kuvaus- ja dokumenttirakenne päätetään yleismäärittelyssä. Tietoturvamäärittelyn dokumentit voivat olla itsenäisiä tai sisällytettynä yrityksen muuhun dokumentaatioon. Tietoturvallisuuden hallintajärjestelmän ja hallinnollisen tietoturvan määrittely- ja politiikkadokumentit sisällytetään yrityksen laatukäsikirjaan. Yrityksen kaikkien tietojärjestelmien kuvaukset tehdään liiketoimintaprosessien pohjalta. Kuvausten laatiminen tehdään ensin yritystasolla, sitten prosessitasolla ja lopulta tietojärjestelmätasolla. Tietojärjestelmätason dokumenteissa tulee erityisesti huomioida tiedot ja riskit. (Hakala ym. 2006: 71, 73, 79.)

Tietoturvan suunnitteluvaiheessa keskitytään riskeihin varautumiseen ja riskien toteutumisen estämiseen sekä vähentämään riskien vaikutusta. Suunnittelussa tulee huomioida kustannusten suhde hyötyyn, sillä kaikkiin riskeihin ei ole kustannustehokkaasti ajatellen järkevää varautua. Suojautumiskeinoissa on punnittava myös eri suojautumiskeinojen taloudellisuutta. Riskeihin liittyen on suunniteltava riskien toteutumisesta toipuminen normaalitilanteissa. Lisäksi on laadittava valmiussuunnitelma poikkeuksellisiin olosuhteisiin. Suunnittelun tulee huomioida toteutumisen seurannan ja dokumentoinnin suunnittelu. (Hakala ym. 2006: 89, 98–99, 101–103.) Erityisesti liikkuvan työn tietoturvan suunnittelussa on oleellista tunnistaa ja suojata liiketoiminnan kannalta tärkeä tieto. Suunnittelussa tulisi huomioida esimerkiksi luottamuksellisen tiedon määrän rajoittaminen kannettavissa laitteissa, varmuuskopioinnista huolehtiminen ja avoimessa verkossa liikkuvan tiedon suojaaminen. (Heljaste ym. 2008: 72–73.)

Tietoturvasuunnitelma laaditaan tietoturvapolitiikassa asetettujen suuntaviivojen ja reunaehtojen pohjalta. Se sisältää käytänteet, joilla pyritään haluttuun tietoturvan tasoon. Tietoturvasuunnitelmassa määritellään kirjallisesti ja yksityiskohtaisesti kussakin tietojärjestelmässä käytettävät työmenetelmät ja tekniset ratkaisut. Tämän takia tietoturvasuunnitelma on luottamuksellinen tai salainen. (Hakala ym. 2006: 9.) Hakala ja muut (2006: 9–10, 20) jatkavat, että tietoturvasuunnitelma laaditaan keskipitkälle aikavälille, joka on käytännössä 2–5 vuotta. Organisaation toimintaprosesseissa tapahtuvien muutosten vaikutukset tulee huomioida ja päivittää tarvittaessa tietoturvasuunnitelmaan. Myös uusien teknologioiden käyttöönotto saattaa aiheuttaa muutostarvetta tietoturvasuunnitelmaan. Tämän takia tietoturvasuunnitelma on hyvä tarkistaa vuosittain. Tietoturvasuunnitelman laatimisesta vastaa organisaation turvallisuudesta huolehtiva elin yhdessä tietohallin-

non sekä tietojenkäsittelyn ja tietotekniikan ammattilaisten kanssa. Ensimmäinen tietoturvasuunnitelma luodaan usein projektina. Tietoturvasuunnitelman pohjalta voidaan laatia tietoturvaohje, joka on käyttäjälle laadittu yksittäistä tietojärjestelmää tai liiketoimintaprosessia käsittelevä erillinen ohje.

Viestintävirasto (2010d) on luonut yrityksille tarkoitetun ohjeistuksen yrityksen tietoturvasuunnitelman avainkohdista. Ohjeistuksen yhteydessä Viestintävirasto käyttää tietoturvasuunnitelmasta nimitystä tietoturvaohjelma. Ohjelman sisältämät 12 kohtaa on esitetty taulukossa 4.

Taulukko 4. Viestintäviraston tietoturvaohjelma (Viestintävirasto 2010d).

1. Kirjoitetaan tietoturvasuunnitelman johdantoon yrityksen toimitusjohtajan tai hallituksen kannanotto tietoturvan tärkeydestä.
2. Kerrotaan tietoturvasuunnitelman tarkoitus ja tärkeys.
3. Nimetään tietoturvan vastuuhenkilöt.
4. Määritellään vastuuhenkilö tietoturvasuunnitelman toteuttamiselle.
5. Kirjataan tarkka luettelo henkilöistä, joita tietoturvasuunnitelma koskee, huomioidaan myös pois lähtevät ja yhteiskumppanit.
6. Tehdään salassapitosopimus ja kilpailukieltosopimus avainhenkilöiden kanssa.
7. Tehdään salassapitosopimus yhteistyökumppanien ja palveluiden toimittajien kanssa.
8. Määritellään suojattava tietoaineisto.
9. Määritellään ja ohjeistetaan tiedon luokitteluperiaatteet.
10. Määritellään periaatteet ja menettelytavat tiedon kirjaamiselle, käsittelylle, säilyttämiselle, välittämiselle, kopioinnille ja hävittämiselle.
11. Määritellään toimenpiteet väärinkäytöstilanteissa ja rikollisen toiminnan varalle.
12. Järjestetään tietoturvakoulutusta ja -valmennusta henkilökunnalle.

Taulukosta on nähtävissä, että Viestintävirasto aloittaa tietoturvaohjelman määrittelyn yrityksen johdosta ja tietoturvasuunnitelman tärkeydestä. Ohjelmassa huomioidaan yrityksen hallussa olevan tiedon tärkeys. Ohjelma korostaa henkilöstön tärkeyttä tietoturvan toteuttamisessa. Myös vastuun jaolle annetaan selkeät ohjeet.

Tietoturvariskillä tarkoitetaan todennäköisyyttä tietoturvauhkan toteutumiselle ja mahdollisesti toteutuvan vahingon merkittävyyttä. Tietoturvauhka voi olla sisäinen tai ulkoinen. Sisäisen tietoturvauhkan muodostaa yrityksen omien työntekijöiden toiminta. Ulkoiset uhat, kuten virukset, tulevat yrityksen ulkopuolelta. Tietoturvauhkille altistumista kutsutaan haavoittuvuudeksi. Tietoturvariskin suuruus on verrannollinen mahdollisen vahingon suuruudelle ja tietoturvauhkan to-

teutumisen todennäköisyydelle. Oikeudetonta puuttumista yrityksen tietoturvaan, kuten tietomurtoa, kutsutaan tietoturvaloukkaukseksi. (Tiivis tietoturvasanasto 2004: 16–17.)

Riski on suomennos latinankielisestä sanasta risco, joka tarkoittaa karia tai jotakin, joka leikkaa. Riski viittaa vaaraan, jossa kärsitään tappio tai syntyy vahinko. Riskiä mitataan todennäköisyyden ja uhkan suuruuden laskennallisena määränä. Riskien arviointi tulee aloittaa kartoittamalla yrityksen toiminnalle tärkeät asiat eli mitä suojattavaa yrityksellä on. Sen jälkeen arvioidaan asioille kohdistuvat uhat. Toiminnalle tärkeät asiat voidaan jakaa neljään tekijään, jotka ovat työntekijät, maine, liiketoiminnan prosessit sekä taloudellinen tappio. Yrityksen on määriteltävä ja arvioitava kohteet, jotka ovat elintärkeitä yrityksen toimintatavoitteiden saavuttamisessa, kuten ihmiset, omaisuus, tieto, toiminta, maine ja ympäristö. Yrityksen toimintatavoitteelle elintärkeää voi olla myös näiden kohteiden muodostama kokonaisuus. Kohteet on suojattava ja niiden vahingoittumattomuus on varmistettava turvallisuus- ja riskienhallintatoimenpiteillä. Riskistä aiheutuvan vahingon tulee olla merkityksellinen, jotta vahingon aiheuttajaa pidetään riskinä. Riski voidaan luokitella onnettomuuden luonteen, riskin ilmenemisen ja seurausten luonteen mukaan. Yrityksessä luokittelu on tehtävä kattavasti ja avoimesti, jotta riskien käsittely kokonaisvaltaisesti on mahdollista. (Leppänen 2006: 29–31, 61; Heljaste ym. 2008: 14, 16.)

Jordan ja Silcock (2006: 1, 3–4) tarkoittavat riskeillä ei-toivottua lopputulosta ja sen mahdollisuutta. Heidän mielestään tietotekniikka on riskialtista tuotekehityksessä, ohjelmistojen käyttöönotossa ja operatiivisissa järjestelmissä. Hakala ja muut (2006: 29) tarkoittavat riskeillä yrityksen tietoturvaa vaarantavia uhkia. Laaksosen ja muiden (2006: 150) mukaan riskit ovat yrityksen toimintaa uhkaavia ei-toivottuja tapahtumia. Niitä pyritään löytämään ja hallitsemaan riskienhallinnalla. Teknologian tutkimuskeskus VTT (myöh. VTT) (2009f) puolestaan näkee riskin vahingon mahdollisuutena. Riskit ovat pääasiassa ihmisten aiheuttamia, minkä ansiosta niihin voidaan vaikuttaa ja varautua ja niiltä voidaan myös suojautua. Vaikka riskit ovat arkipäivän pieniä asioita, voi pienistäkin häiriöistä aiheutua tapahtumaketju, joka voi uhata koko yrityksen toimintaa. Useita riskejä otetaan tietoisesti ja harkiten ja jotkut riskit voivat liiketoiminnassa olla jopa mahdollisuus, mutta ongelmalliseksi riski muodostuu silloin, kun se pääsee yllättämään.

Riskien tunnistaminen ja hallinta helpottuvat, kun riskit luokitellaan riskilajeihin. Luokittelua tehdään riskin luonteen ja sen vaikutuskohteen mukaan. Luokittelussa on hyvä huomioida, että riskilajit menevät osin päällekkäin. Jordan ja Silcock (2006: 60–65) jakavat tietotekniikkariskit seitsemään luokkaan, jotka ovat 1. valmistumattomat tietotekniikkaprojektit, 2. liiketoiminnan lamaannuttava tietotek-

niikkapalveluiden toimimattomuus, 3. katoava tieto-ominaisuus, 4. katkos palveluntarjoajan tai tietotekniikkatoimittajan toiminnassa, 5. viat tietotekniikkasovelluksissa, 6. viat tietotekniikkainfrastruktuurissa eli laitteistossa tai alustaohjelmistoissa sekä 7. strategiset riskit ja tulevaisuuden uhat, joissa tietotekniikan kehitys ajautuu umpikujaan. Yksittäisen riskin toteutuminen saattaa vaikuttaa toisen riskin toteutumistodennäköisyyteen. Riskit voivat olla eri luokista eli yhteen luokkaan kuuluvan riskin toteutuminen saattaa vaikuttaa toiseen luokkaan kuuluvan riskin toteutumiseen.

VTT:n (2009e) ylläpitämällä pk-yrityksille suunnatulla pk-yrityksen riskienhallinta -sivustolla riskien luokat ovat liike-, henkilö-, sopimus- ja vastuu-, tieto-, tuote-, ympäristö-, projekti-, keskeytys-, rikos- ja paloriskit. (VTT 2009h.) Liikeriskit liittyvät yrityksen työntekijöihin, markkinointiin, kysyntään, tuotantoon ja kustannuksiin. Ne kuuluvat olennaisesti yrityksen toimintaan ja ne otetaan tietoisesti liikevoiton saamiseksi. Henkilöriskit ovat yrityksen työntekijöihin kohdistuvia uhkia, jotka voivat tulla yrityksen sisältä mutta myös ulkopuolelta. Henkilöriskeihin sisältyvät myös yrityksen työntekijöiden yritykselle aiheuttamat riskit. Henkilöriskien ennakointi ja hallinta on välttämätöntä yrityksen toiminnalle. Sopimus- ja vastuuriskejä syntyy, kun yritys ei panosta sopimusten tekemiseen riittävästi, ei tee sopimuksia lainkaan tai tekee itselleen epäedullisia sopimuksia. (VTT 2009h; VTT 2009i; VTT 2009j.)

Tietoon liittyviä riskejä kutsutaan tietoriskeiksi. Tietoriskit liittyvät yrityksen kaikkeen toimintaan, minkä takia ne ovat monitasoisia ja laajoja. Tietoriskit voidaan jakaa johtamiseen, toimitiloihin, tietojärjestelmien suojaukseen, liikesuhteisiin sekä työntekijöiden toimintaan liittyviin riskeihin. Tietoriskien hallinta on haastavaa, koska ne muuttuvat jatkuvasti ja niitä syntyy koko ajan lisää. (Leppänen 2006: 103–104; VTT 2009l.) Lisäksi VTT:n (2009k) asiakirjassa korostetaan, että kaikissa yrityksissä on omalle toiminnalle kriittistä tietoa. Tietoa on paljon ja sitä on monessa eri muodossa. Useassa pk-yrityksessä tieto on yrityksen suurin pääoma. Näistä seikoista huolimatta tietoriskien uhkaa on pitkään aliarvioitu. Leppänen (2006: 109) jakaa tietoon kohdistuvat rikokset viestintä-, salassapito-, yrityssalaisuus- ja henkilörekisteririkokseen, tietomurtoon, yritysvakoiluun sekä salakuunteluun ja -katseluun.

Tuoteriskejä ovat esimerkiksi epäonnistuminen tuotteen markkinoille saattamisessa tai tuotteeseen liittyvässä päätöksenteossa. Huomioitavaa on, että yrityksen toimeentulo riippuu usein tuotteesta tai palvelusta. (VTT 2009h; VTT 2009m.) Ympäristöriskeihin kuuluvat mm. ihmisen terveyteen sekä elin- ja työympäristöön liittyvät riskit. Ympäristöriskien tunnistaminen ja ympäristönsuojelu vaikuttavat yrityksestä luotavaan mielikuvaan. Yrityksen sidosryhmät ovat usein kiin-

nostuneita yrityksen ympäristönsuojelun tasosta. Ympäristölainsäädäntö velvoittaa yrityksiä, eikä korvauksilta voi välttyä vetoamalla tietämättömyyteen lainsäädännön vaatimuksista tai vahingon aiheutumiseen tahattomasta toiminnasta. Projektiriskit aiheutuvat esimerkiksi liiallisesta optimismista ja lupauksista. Projektiriskien huomioimisen tarve korostuu, kun yrityksen toiminta on projektiluonteista. Jokainen projekti on riskialtis, minkä aiheuttaa projektin kertaluonteisuus ja siihen liittyvät jatkuvat uudet elementit, kuten työryhmä, asiakas ja tuote. (VTT 2009h; VTT 2009n; VTT 2009o.)

VTT:n (2009h) mukaan keskeytysriskit ovat erityisesti pienten yritysten keskeinen haaste. Keskeytysriskit aiheuttavat häiriöitä toimintaan ja toiminnan turvaamiseen. Esimerkiksi palvelinta koskevissa riskeissä sähkön loppuminen on suurin uhka. Heljaste ja muut (2008: 73–74) huomauttavat, että palvelimet tulee suojata myös varkauksilta ja ympäristöuhkilta, kuten pölyltä ja vesivahingoilta. Rikosriskit voivat kohdistua yritykseen tai sen työntekijään. Rikosriskeihin kuuluvat myös uhat, joissa yritys itse syyllistyy toiminnassaan rikokseen. Rikoksilla on aina negatiivisia seurauksia. Monet rikokset vaikuttavat yrityksen tulokseen ja tuottavuuteen. Rikoksiin liittyy aina vahingonkorvaus. Paloriskit ovat yritystä ja sen työntekijöitä vaarantavia tulipalouhkia. Pienistä paloista voi nopeasti muodostua vakavia suuronnettomuuksia. (VTT 2009p; VTT 2009h.)

Yritysten riskienhallinta on kannattavuutta ja hyödyllisyyttä tavoittelevaa toimintaa, joka on pääasiassa vapaaehtoista. Kuitenkin, koska yritystoiminnassa on aina kyse useiden eri osapuolten oikeuksista ja hyvinvoinnista, on katsottu tärkeäksi päättää riskienhallinnan toteuttamisesta eräiltä osin myös lainsäädännössä. Lainsäädännöllä pyritään yhtenäistämään ja varmistamaan yrityksen riskienhallinnan lähtökohdat eli auttamaan yritystä riskienhallinnassa ja ohjaamaan yritystä toimimaan oikein. Lainsäädännössä on määritelty seuraavia yrityksen riskienhallinnassa huomioitavia osa-alueita: yrityksen perustaminen, kirjanpito, verotus, tuotevastuu ja -turvallisuus, ympäristövastuu ja -turvallisuus, työsuhde, työturvallisuus, työterveyshuolto, työympäristö, suojelu ja yrityksen lopettaminen. (VTT 2009q; VTT 2009r.)

Riskienhallintatyön keskeinen ajatus on pyrkiä ennaltaehkäisemään ei-toivottuja tapahtumia (Heljaste ym. 2008: 62). Leppäsen (2006: 119, 121, 123–125, 128, 175, 186) mukaan riskienhallinnan tavoitteena on hallita tunnistettuja riskejä. Riskienhallinnan tavoitteet täytyy määritellä tukemaan yrityksen tavoitteita ja strategiaa eikä siitä tule tehdä itsetarkoitusta. Leppänen huomauttaa, että kaikkien riskien tunnistaminen ja hallitseminen ei ole mahdollista. Siksi on varauduttava myös sellaiseen riskiin mitä ei ole tunnistettu ja minkä olemassa olosta ei tiedetä. On myös huomioitava, että riskit muuttuvat koko ajan. Yrityksen työntekijöiden

turvallisuusasenteet vaikuttavat päätökseen, mitkä ovat yritykselle kohtuulliset riskit ja millaisia riskejä yritys ottaa. Riskienhallinta on epävarmuuksien ja todennäköisyyksien hallintaa.

VTT (2009u) nimeää neljä riskien hallintakeinoa, jotka ovat riskin välttäminen, pienentäminen, siirtäminen ja jakaminen sekä pitäminen omalla vastuulla. Riskien välttämisestä todetaan, että useita riskejä ei voida välttää kokonaan. Mikäli riski liittyy yrityksen liiketoiminnan toimintoon, riskin välttäminen edellyttäisi kyseisen toiminnon jättämistä kokonaan tekemättömäksi, mikä ei tietenkään ole mahdollista. Sen sijaan riskin pienentäminen on yrityksen riskienhallinnassa olennaista. Tällöin pyritään ensisijaisesti pienentämään riskin toteutumisen todennäköisyyttä, mutta samalla varaudutaan myös riskin toteutumiseen ja pienennetään toteutumisesta aiheutuvia seurauksia. Riskin siirtämisessä ja jakamisessa voidaan riski siirtää sopimuksella toiselle taholle. Tällainen tulee kyseeseen esimerkiksi kuljetuksesta tai alihankinnasta sopimisessa. Myös vakuuttaminen on riskin siirtämistä ja jakamista. Osan riskeistä kannattaa kuitenkin pitää omalla vastuulla tai ne jäävät oman yrityksen vastuulle vaihtoehdoitta. Kunkin tällaisen riskin hallitsemiseksi tulee miettiä erilaisia vaihtoehtoja. Riskienhallinnassa tulee ennaltaehkäisemisen lisäksi suunnitella toiminta ongelmatilanteessa, joka aiheutuu, jos riski toteutuu. Suunnittelu tulee tehdä jokaiselle riskille erikseen. Lisäksi tulee suunnitella miten riskin toteutumisesta syntyneistä seurauksista toivutaan. (VTT 2009u.)

Hakalan ja muiden (2006: 67–70) mukaan riskin realisoitumistodennäköisyyden luokittelujärjestelmässä kunkin riskin vaikutusten ja todennäköisyyksien tarkastelu tehdään yhtä aikaa riskien luokittelun kanssa. Vaikutusten arvioinnissa huomioidaan riskin vaikutuksen seuraamus ja seuraamuksen suuruus sekä tarkasteluajanjakso. Seuraamuksella etsitään riskin vaikutuksen kohde. Seuraamuksia ovat esimerkiksi toiminnalliset, taloudelliset, imagolliset ja juridiset seuraamukset. Riskien vaikutuksen seuraamusten suuruusluokkia voivat olla esimerkiksi eivaikutusta, olennainen, merkittävä ja vakava. Riskin vaikutuksen ajallinen tarkastelu eli tarkasteluajanjakson pituus korostuu, kun kyseessä on eheys- ja käytettävyysriski. Pitkäaikaiset tai pysyvät käytettävyysongelmat voivat tuhota koko yrityksen. Ajallisessa tarkastelussa voidaan esittää kunkin riskin toteutumisessa aiheutuvan ongelman kesto. Tarkastelu voidaan tehdä myös suhteellisesti käyttämällä esimerkiksi luokittelua hetkellinen, lyhytaikainen, pitkäaikainen ja pysyvä. Riskien todennäköisyyksien luokittelu voidaan tehdä, kun riskit on tunnistettu. Tällöin kuvataan millä todennäköisyydellä kukin riski realisoituu. Riskin realisoitumistodennäköisyys voi olla jopa lähes 100 %. Todennäköisyyttä ei yleensä lasketa matemaattisesti. Todennäköisyyden luokittelu kuvataan esimerkiksi sanallisesti. Jos riskin vaikutusten luokittelu on tehty 4-portaisesti, kannattaa myös to-

dennäköisyys luokitella 4-portaisesti, esimerkiksi harvinainen, satunnainen, yleinen ja varma.

Tietoturvakartoituksella kartoitetaan yrityksen tietoturvan tilanne kartoitushetkellä. Yrityksen tietoturvan perusasiat pysyvät kunnossa, kun tietoturvakartoitus tehdään yrityksessä säännöllisesti ja parannetaan kartoituksessa esille nousseet puutteet. Keskuskauppakamarin ja Helsingin seudun kauppakamarin (2008: 53) tutkimuksessa selvisi, että vain joka kolmas (29 %) 1286 vastaajasta oli tehnyt kirjallisen riskikartoituksen viimeisen kolmen vuoden aikana. Turvallisuus oli osana toiminta- ja laatujärjestelmää hieman yli puolessa (53 %) yrityksistä, mutta vuosittaisessa strategian, budjetin ja toiminnan suunnittelussa yritysturvallisuutta käsiteltiin vain 24 % vastaajayrityksistä.

Riskikartoituksessa pyritään löytämään riskit, jotka vaarantavat yrityksen tietoturvaa. Ensin riskit kartoitetaan. Kartoittaminen aloitetaan nostamalla esiin jo realisoituneet riskit. Sen jälkeen mietitään todennäköiset ja odotettavissa olevat riskit nykytilanteessa. Lopuksi mietitään vielä tulevaisuuden mahdollisia riskejä. Kun riskit on kartoitettu, pyritään arvioimaan kunkin riskin toteutumistodennäköisyys sekä realisoitumisen merkitys yrityksen toimintaan ja taloudellisiin seuraamuksiin. Tarkastelussa voidaan käyttää 3- tai 10-portaista luokittelua. Luokittelun tavoitteena on löytää riskit, joiden realisoituminen aiheuttaa yrityksen toiminnalle eniten tuhoa ja joiden torjuminen on siten yrityksen toiminnan jatkumiselle erityisen tärkeää. (Hakala ym. 2006: 29–30; Leppänen 2006: 119, 121, 123–125, 128, 175, 186.)

Riskikartoitus voidaan tehdä yksittäisten liiketoimintaprosessien ja niiden käyttämien tietojärjestelmien tasolla tai koko organisaation tasolla. Molemmissa tapauksissa riskit tarkentuvat lopulta tietojärjestelmäkohtaisiksi, mutta toisaalta yritys tarvitsee myös yhteenvetona kuvauksen koko yrityksen toimintaa uhkaavista merkittävistä riskeistä. Jo riskikartoituksen lopputuloksena voidaan saada käsitys yrityksen tietoturvan kokonaistilasta. Riskin toteutuminen on arvioitava mahdollisimman luotettavasti. Toteutumisen todennäköisyyden jaottelu voidaan tehdä monella tavalla, mutta se on riittävää, jos se tehdään 3-portaisesti, esimerkiksi epätodennäköinen–mahdollinen–todennäköinen. Riskien toteutumisen arvioinnin jälkeen arvioidaan toteutumisesta aiheutuvien seurausten vakavuus yhtä moniportaisella luokittelulla, esimerkiksi vähäinen–haitallinen–vakava. Näiden arviointien yhteenvetona muodostetaan riskin lopullinen tasoluokittelu, jossa asteikko voi olla esimerkiksi merkityksetön–vähäinen–kohtalainen–merkittävä–sietämätön. Tämän jälkeen riskin toteutumisen todennäköisyys pyritään minimoimaan mahdollisimman epätodennäköiseksi. Lopuksi vielä varaudutaan riskin toteutumiseen pienentämällä riskin toteutumisesta aiheutuvat seuraukset mahdollisimman har-

mittomiksi. Tärkeintä on arvioida ja seurata yrityksen toimintaan vakavasti vaikuttavia riskejä, joiden toteutuminen on todennäköistä. (Hakala ym. 2006: 29–30; Leppänen 2006: 119, 121, 123–125, 128, 175, 186.)

TIEKE (2010; 2005b) tarjoaa Internetissä pk-yrittäjille maksuttoman tietoturvakartoituksen, jolla yritys voi testata oman tietoturvatasonsa. Kartoituksen tavoitteena on antaa yrittäjälle ja henkilökunnalle tieto, jolla varmistetaan yrityksen toiminnan häiriötön jatkuminen. Kartoitus tehdään nimettömästi, eikä se vaadi minkäänlaista kirjautumista tai tietojen antoa. Kartoitus muodostuu kysymyssarjasta, joka TIEKEn mukaan kattaa yrityksen tietoturvan perusasiat. Tietoturvakartoitus sisältää kysymyksiä seuraavilta osa-alueilta: turvallisuuden kehittäminen, toimitilat, tiedot ja ohjelmistot, tietojen asiaton käyttö, virustorjunta ja vakuutukset. Kysymyksiin annetaan vastausvaihtoehdot: kyllä, ei sekä ei sovellu. Tietoturvakartoitus sisältää seuraavat kysymykset:

”Turvallisuuden kehittäminen

1. *Annetaanko henkilökunnalle tietoturvakoulutusta säännöllisesti?*
2. *Onko yrityksessä nimetty vastuuhenkilö turvallisuuden kehittämiselle?*
3. *Onko yritykselle laadittu tietoturvasuunnitelma?*

Toimitilat

4. *Onko toimitilat varustettu paloilmoittimella, josta menee hälytys suoraan hälytyskeskukseen?*
5. *Onko toimitiloissa sammutusvälineitä?*
6. *Onko toimitilat varustettu rikosilmoitinlaitteistolla?*
7. *Valvotaanko vierailijoiden tuloa ja liikkumista yrityksen tiloissa?*
8. *Onko tietotekniikkalaitteet luetteloitu ja turvamerkitty?*

Tiedot ja ohjelmistot

9. *Otetaanko tietokoneille talletetuista tiedoista varmuuskopiot?*
10. *Testataanko varmuuskopioiden palautusten onnistuminen säännöllisesti?*
11. *Säilytetäänkö yritystoiminnalle tärkeitä asiakirjoja turvallisessa paikassa?*
12. *Onko tärkeiden tietojen käsittelyä varten laadittu ohjeet, joihin sisältyy tietojen säilyttäminen, jakelu ja tuhoaminen, esim. palvelun tarjoajan kautta tai silppurilla?*

Tietojen asiaton käyttö

13. *Onko henkilökunnalle annettu käyttäjätunnukset ja valvotaanko tietojärjestelmien käyttöä?*
14. *Onko tietokoneiden käyttö suojattu säännöllisesti vaihdettavin salasanoin?*

Virustorjunta

15. *Onko Internet-yhteydet suojattu palomuurilla?*
16. *Onko tietokoneet varustettu automaattisesti päivittyvällä virustorjuntaohjelmalla?*
17. *Onko toimintaohjeita virusten varalta?*
18. *Päivitetäänkö tietokoneen käyttöjärjestelmä säännöllisesti?*

Vakuutukset

19. *Onko tietotekniikka- ja tietoliikennelaitteet vakuutettu vähintään palon, nestevuodon, myrskyn ja murron varalta?".* (TIEKE 2005a; TIEKE 2005b.)

Myös Viestintävirasto (2010c) on luonut Yrityksen tietoturvaoppaan liitteeksi kysymyssarjan, joka on tarkoitettu yrityksille helpottamaan yrityksen tietoturvatilanteen kartoittamista. Kysymyssarja sisältää seuraavat kysymykset:

1. *"Mikä on yritykselle arvokasta tietoa?*
2. *Mikä on yritykselle elintärkeän arvokasta tietoa?*
3. *Kuinka tietoja valvotaan?*
4. *Mitä tietoa tarvitaan päivittäin?*
5. *Mitä tietoa tarvitaan kuukausittain tai harvemmin?*
6. *Onko yritykselle tehty tietoturvallisuuden riskianalyysi?*
7. *Jos yrityksen tietokone varastetaan, voiko joku hyödyntää siinä olevaa tietoa?*
8. *Jos tapahtuu sähkönjakeluhäiriö, voivatko päivän aikana luodut tiedostot hävitä?*
9. *Jos kiinteistössä syttyy tulipalo, voivatko tiedot tuhoutua ja liiketoiminta pysähtyä?*
10. *Jos tietokone ei tunnista käyttäjää, voiko konetta käyttää petokselliseen toimintaan?*
11. *Onko etätyön tietoturvasta huolehdittu?*
12. *Jos työntekijä kertoo junassa tutulleen tuotekehityksen tuloksista, voiko tieto olla merkittävä takana istuvalle kilpailijalle?*
13. *Jos yrityksessä työskentelevä ulkopuolinen työntekijä kuljettaa tietoa ulkopuolelle, voivatko tiedot joutua niitä hyödyntäville tahoille?*
14. *Jos työntekijä irtisanotaan, voiko hän tuhota tärkeitä tietoja tai viedä ne eteenpäin ja hyötyä niistä?*
15. *Onko turvallisuuden kehittämistarpeet tunnistettu?*
16. *Onko turvallisuuden kehittämistarpeet kirjattu kehittämissuunnitelmaksi?*
17. *Onko yrityksellänne selkeä johdon hyväksymä tietoturvallisuuspolitiikka?*
18. *Onko kehittämiskustannukset arvioitu?*
19. *Onko päätetty miltä osin toiminta vakuutetaan?*

20. Onko henkilökunta perehdytetty yrityksen tietoturvan käytäntöihin?
21. Onko tietoturvavastuut määritelty?
22. Onko tehtävät vastuutettu?
23. Miten huolehditaan tärkeiden tehtävien varahenkilöjärjestelyistä?
24. Saako jokainen työntekijä käyttöoikeudet vain niihin tietoihin, joita työtehtävä edellyttää?
25. Miten toimitaan, jos epäillään väärinkäytöksiä?
26. Kuinka usein varmistetaan palautusten, varmenteiden ja varajärjestelmien toimivuus?
27. Missä tilanteissa käytetään sähköpostiviestien salakirjoitusmenetelmiä?
28. Säilytetäänkö turvakopiot eri kiinteistössä?
29. Mikä on yrityksenne tietoturvallisuuden tilanne tänään?"

Myös VTT:n (2009s) pk-yrityksen riskienhallinta -sivustolle on luotu työvälineitä, joilla yritys pystyy kartoittamaan ja arvioimaan oman yrityksensä olemassa olevia riskejä. Riskienhallinta voidaan aloittaa sivustolta löytyvällä haavoittuvuusanalyysillä, jolla riskien kartoittaminen on nopeaa ja karkeaa. Tavoitteena on tunnistaa yrityksen keskeiset riskit ja ne yrityksen riskienhallinnan osa-alueet, joita yrityksen kannattaa ensimmäisenä lähteä kehittämään. Haavoittuvuusanalyysissä yrityksen toiminta jaetaan kuuteen osa-alueeseen: henkilöt, omaisuus ja keskeytykset, toimintaedellytykset, toiminnan organisointi, sidosryhmät ja talous (VTT 2009t). Kun haavoittuvuusanalyysi on tehty eli keskeiset riskit ja ensimmäiset kehittämisen osa-alueet on kartoitettu karkeasti, voidaan riskejä lähteä kartoittamaan tarkemmin riskilajeittain (VTT 2009s).

Laaksonen ja muut (2006: 150) huomauttavat, että riskien arvioinnin tulee käsittää myös yrityksen ulkoistetut liiketoiminnan osat ja järjestelmät. Säännöllisesti tehtävälle riskien arvioinnille tulee suunnitella ja sopia aikataulu, kohteet ja arvioinnin suorittajat, jotka ovat vastuussa arvioinnin tekemisestä. Arvioinnin tuloksista laaditaan raportti arvioinnin kohteena olleille tahoille. Merkittävimmät tulokset raportoidaan myös yrityksen johdolle. Hakala ja muut (2006: 31) jatkavat, että kun riskit ja niiden toteutumistodennäköisyys ja vaikutus yrityksen toiminnalle on selvitetty, siirrytään miettimään keinoja, joilla riskin realisoituminen voidaan estää. Varautumisen suunnittelu kohdistetaan erityisesti niihin riskeihin, joiden realisoituminen aiheuttaisi eniten tuhoa yrityksen toiminnalle. Kullekin riskille pyritään löytämään sekä teknisiä että toiminnallisia ratkaisuvaihtoehtoja. Varautumismenetelmät luokitellaan 3-portaisesti sen mukaan miten kallis menetelmä on, vaatiiko se osaamisen hankkimista tai toimintatapojen muuttamista sekä vaikuttaako menetelmä muihin tietojärjestelmiin.

VTT:n (2009e) riskienhallinta -sivustolla todetaan, että riskeihin voidaan vaikuttaa ja niitä voidaan hallita käytännön toimilla ja työvälineillä sekä käyttämällä tervettä järkeä. Sivustolla voi perehtyä riskienhallintaan ja tehdä yrityksen riskianalyysejä. Sivustolla tarjotaan yrityksille palveluna myös välinesarjoja riskienhallinnan kouluttamiseen. Sivuston loppuun on koottu esimerkkejä yleisistä pk-yrityksen tärkeistä ja vaikeista riskitilanteista sekä kerrottu kullekin riskitilanneesimerkille sivustolta löytyvä välinesarja, josta löytyy apu kyseisen tilanteen riskienhallintaan. Riskienhallinta on toimintaa riskien ja niiden aiheuttamien vahinkojen vähentämiseksi, millä varmistetaan yrityksen toiminnan jatkuvuus sekä pyritään turvaamaan työntekijöiden hyvinvointi. Riskienhallinta on tilanteiden arviointia, suunnittelua ja käytännön tekoja ja sitä tekee jokainen yrityksen työntekijä. Riskienhallinta on tehokkainta, kun se on ennakoivaa, tietoista, suunnitelmallista ja järjestelmällistä. Riskienhallinnan hyötynä on yrityksen ja sen työntekijöiden turvaaminen. Yrityksen menestymismahdollisuudet paranevat, mihin päästään tuotannon tehokkuuden ja laadun parantumisella sekä häiriötilanteiden ja katkosten vähenemisellä. Riskien tunnistamisella myös ymmärrys yrityksen toiminnasta kasvaa. (VTT 2009e; VTT 2009f; VTT 2009g.)

Hakala ja muut (2006: 31) huomauttavat, että täydellisen tietoturvan saavuttaminen on muuttuvien tilanteiden takia mahdotonta, tai ainakin siihen pyrkiminen olisi taloudellisesti niin kallista, että se ei ole mielekästä. Sen takia kaikkiin riskeihin ei pyritäkään varautumaan. Toisaalta niille riskeille, joille on mietitty varautumismenetelmät, laaditaan suunnitelma myös riskin realisoitumisesta toipumiseen. Toipumissuunnitelma sisältää ohjeet miten riskin realisoitumisen jälkeen toimitaan vahinkojen minimoimiseksi. Toipumissuunnitelmassa tulisi olla kirjattuna riskikohtaisesti ainakin ohjeet miten realisoituminen havaitaan, miten välilliset vahingot vältetään ja välittömät minimoidaan sekä miten kauan toipuminen kestää ja mitä se maksaa.

Heljaste ja muut (2008: 69–72, 79) pitävät ihmistä suurimpana tietoturvauhkana. Muita tietoturvauhkia ovat yrityksen käytöstä poistettujen tietokoneiden tiedostoista ja ohjelmista huolehtiminen, roskaposti sekä haittaohjelmat. Haittaohjelmien kannalta suurin uhka on suojaamattomat koneet, joita käytetään Internetissä. Haittaohjelmien tekemisen motiivina on lähes aina rahanteko. Älypuhelimien haittaohjelmat eivät vielä ole kovin yleisiä, mutta Heljaste ja muut (2008: 71, 79) nostavat älypuhelimet yhdeksi merkittävimmäksi tulevaisuuden tietoturvauhkaksi. Puhelimiin tallennetaan valtava määrä tietoa ja myös sähköpostia käytetään puhelimella. Uhka aiheutuu puhelimen katoamisesta tai varastamisesta sekä älypuhelimia vaanivista haittaohjelmista. Myös puhelimien kohdalla ihminen on suurin tietoturvauhka.

Toimiston ulkopuolella tehtävää työtä voidaan kutsua liikkuvaksi työksi. Jokavuotinen tietoturvaviikko kiinnitti helmikuussa 2009 huomiota pienten ja keskisuurten yritysten liikkuvan työn tietoturvaan. Tällaisen työn tietoturvasta huolehtiminen vaatii erityistä huomiota. Tietoliikenneyhteyksien suojaaminen, laiterikot ja luottamuksellisten tietojen vuotaminen ovat merkittäviä tietoturvariskejä. Tästä huolimatta ihminen on kuitenkin liikkuvan työn tietoturvan suurin riski. Uusien tietokonelaitteiden myynnistä reilusti yli puolet on kannettavia tietokoneita. Varkaille kannettava tietokone on mieluisa kohde. Se on helppo varastaa hotelleissa ja lentokentillä. Esimerkiksi Lontoossa Heathrown lentokentällä katoaa 900 kannettavaa viikossa. Kannettavia varastetaan myös Suomessa keskellä kaupunkia auton takapenkiltä, vaikka kuljettaja istuu autossa. Anastetun kannettavan tietokoneen myynti eteenpäin on helppoa. Joskus kannettavan sisältämä tieto on myytäessä arvokasta. Tietokoneilla säilytetään yrityksen luottamuksellisia tietoja, joita ei ole suojattu katoamisen tai varkauden varalta. (Heljaste ym. 2008: 72–73.)

3.4 Tietoturvakäyttäytyminen

Työntekijät ja heidän tietoturvakäyttäytymisensä ovat merkittävässä asemassa yrityksen tietoturvan onnistumisessa. Tietoturvakäyttäytymisen aikaisemman tutkimuksen ymmärtämiseksi käytiin läpi seitsemän tieteellistä lehteä, jotka ovat MIS Quarterly, Information Systems Research (ISR), Journal of the Association for Information Systems (JAIS), Journal of Management Information Systems (JMIS), European Journal of Information Systems (EJIS), Information Systems Journal (ISJ) ja Journal of Information Technology (JIT). Lisäksi käytiin läpi lehdet Decision Support Systems, Information & Management ja Computers & Security. Tarkastelu rajattiin artikkeleihin, jotka oli julkaistu vuosina 2000–2013. Hakuehtona käytettiin ilmaisuja security awareness, security behavior, security behaviour, security culture, employees' compliance, computer abuse ja computer misuse. Näillä rajauksilla artikkeleita löytyi 125, joista tarkempaan tarkasteluun valittiin 31 artikkelia, joissa esiintyi vähintään yksi annetuista hakuilmaisuista. Tarkasteluun valitut artikkelit on esitetty taulukossa 5 sisällön mukaan teemoittain.

Taulukko 5. Tietoturvakäyttäytymisen artikkeleita.

	Sisällön teema					
Artikkeli	**Tietoturva-tietoisuus**	**Tietoturva-käyttäytyminen**	**Tietoturva-kulttuuri**	**Tietoturvan noudattaminen**	**Tietokoneen hyväksikäyttö**	**Tietokoneen väärinkäyttö**
Mason & Cosh (2008)		**xx**				
Herath & Rao (2009a)		**x**				
Anderson & Agarwal (2010)		**x**				
Johnston & Warkentin (2010)		**x**				
Huigang & Yajiong (2010)		**xx**				
Dey, Lahiri & Zhang (2012)		**xxx**				
Hui, Hui & Yue (2012)		**xxx**				
Temizkan, Kumar, Park & Subramaniam (2012)		**xxx**				
Leach (2003)	**x**	**x**				
Albrechtsen (2007)	**x**	**x**				
Culnan, Foxman & Ray (2008)	**x**	**x**				
Rhee, Kim & Ryu (2009)	**x**	**x**				
Albrechtsen & Hovden (2010)	**x**	**x**				
Mensch & Wilkie (2011)	**x**	**x**				
Da Veiga & Eloff (2007)		**x**	**x**			
Ng, Kankanhalli & Xu (2009)		**x**	**x**			
Da Veiga & Eloff (2010)		**x**	**x**			
Guo, Yuan, Archer & Connelly (2011)		**xx**	**xxx**			
Myyry ym. (2009)		**x**[*)]		**xx**		
Herath & Rao (2009b)		**x**[*)]	x	**xx**		
Bulgurcu, Cavusoglu & Benbasat (2010)	x			**x**		
Karjalainen & Siponen (2011)		**x**		**xx**		
Son (2011)		**x**		**x**		
Cheolho, Jae-Won & Kim (2012)	x	**x**		**x**		
D'Aubeterre, Singh & Iyer (2008)	**xx**					
Rotvold (2008)	**x**		**x**			
Hovav & D'Arcy (2012)	**x**		**x**			
Drevin, Kruger & Steyn (2007)	x		x			**x**
D'Arcy, Hovav & Galletta (2009)	x	x[*)]				**x**
D'Arcy & Herath (2011)					**xx**	**x**
Lowry, Moody, Galletta & Vance (2013)					**xxx**	
Yhteensä	13	24	8	6	2	3

[*)] sisältönä vain "security behavior"

Taulukossa merkintä x tarkoittaa, että kyseinen artikkeli löytyy kyseisellä hakuilmaisulla julkaistuna yhdestä lehdestä, xx julkaistuna kahdesta lehdestä ja xxx julkaistuna kolmesta lehdestä. Taulukosta nähdään, että tarkastelluista artikkeleis-

ta suurin osa (24 kpl) sisälsi vähintään yhtenä aiheena tietoturvakäyttäytymistä. Reilu kolmannes (13 kpl) artikkeleista tarkasteli vähintään yhtenä teemana tietoturvatietoisuutta. Tietoturvakulttuuria tutkittiin 8 artikkelin teemana ja tietoturvan noudattamista 6 artikkelissa. Mukaan valikoitujen artikkelien joukossa oli vain vähän tietokoneen hyväksikäyttöä (3 kpl) ja väärinkäyttöä (2 kpl) tarkastelevia tutkimuksia. Seuraavassa artikkeleiden sisältöä tarkastellaan teemoittain tarkemmin.

Tietoturvakäyttäytyminen

Tietojärjestelmät ja niiden käyttö ovat oleellisessa asemassa puhuttaessa tietoturvakäyttäytymisestä. Mason ja Cosh (2008) analysoivat tutkimuksessaan kehityksessä olevien tuotteiden ja käyttövarmuuden arviointiprosessien yhteyttä tietojenkäsittelyn näkökulmasta. Tulosten mukaan kehityksessä olevien tuotteiden ja käyttövarmuuden arviointiprosessien yhteyden ymmärtäminen on tärkeää, kun luodaan monimutkaisia tietojärjestelmiä. Tietojärjestelmien monimutkaisuus aiheutuu vaatimuksista, joita asetetaan tietojärjestelmän tehokkuudelle, reaaliaikaiselle toiminnalle, tietoturvalle, vikasitoisuudelle ja käyttövarmuudelle.

Herath ja Rao (2009a) toteavat tutkimuksessaan, että loppukäyttäjien tietoturvakäyttäytymiseen on alettu yrityksissä kiinnittää yhä enemmän huomiota. Heidän mukaansa käyttäjien tietoturvakäyttäytymisen huomioiminen on haastavaa. Tutkimuksessa todetaan viimeaikaisten tutkimusten osoittavan, että käyttäjillä on hyvin erilaisia näkemyksiä tietoturvaa ja sen ohjeistuksia kohtaan. Tutkimuksessaan Herath ja Rao pyrkivät ymmärtämään paremmin työntekijöiden tietoturvaohjeiden noudattamisen syitä. Sitä varten he luovat ja testaavat rankaisemiseen, paineeseen ja vaikuttamismahdollisuuteen pohjautuvan mallin työntekijöiden toiminnalle. Tutkimukseen osallistui 312 työntekijää 77 organisaatiosta. Tulosten mukaan työntekijöiden tietoturvakäyttäytymiseen voidaan vaikuttaa sisäisen ja ulkoisen motivoinnin keinoin. Kanssaihmisten mielipiteistä ja käyttäytymisestä aiheutuva paine vaikuttaa työntekijän tietoturvakäyttäytymiseen. Työntekijän tunne mahdollisuudesta vaikuttaa asioihin lisää merkittävästi työntekijän pyrkimystä noudattaa tietoturvaohjeita ja luo sisäistä motivaatiota. Rangaistuksien kohdalla kiinnijäämisen todennäköisyydellä oli merkittävä vaikutus työntekijän pyrkimykseen noudattaa tietoturvaohjeita, mutta rangaistusten koventamisella oli negatiivinen vaikutus työntekijän tietoturvakäyttäytymiseen. Myös Anderson ja Agarwal (2010) ovat tutkineet tietoturvakäyttäytymistä. Heidän tutkimukseensa osallistui 594 kotitietokoneen käyttäjää. Tulosten mukaan tietoturvakäyttäytymiseen vaikuttavat kognitiiviset, sosiaaliset ja psykologiset tekijät. Tutkimuksessa tarkasteltiin tunnollisen tietokonekäyttäjän ilmiötä, jossa käyttäjä on motivoitunut huomioimaan tarvittavat varotoimet tietoturvallisessa tietokonekäytössä.

Tietoturvakäyttäytymiseen liittyvää pelon vaikutusta ovat tutkineet Johnston ja Warkentin (2010). Tutkimukseen osallistui 311 yliopistossa työskentelevää tai opiskelevaa henkilöä, joista 275 henkilön vastauksia voitiin käyttää tutkimuksessa. Tutkimuksen mukaan pelko vaikuttaa ihmisen käyttäytymisaikeisiin. Pelon vaikutuksesta ihminen pyrkii pääsääntöisesti toimimaan turvallisuussuositusten mukaisesti. Ihmisten käyttäytyminen kuitenkin poikkeaa toisistaan. Käyttäytymiseen vaikuttavat havainnot omista kyvyistä toimia, vastatoimien tehokkuus, pelon taso ja sosiaaliset vaikuttimet. Tutkimuksen mukaan tietokoneen käyttäjät tekevät havaintoja teknologioista, jotta he pystyisivät niiden avulla poistamaan uhkia sen sijaan, että havaintoja tehtäisiin omien saavutusten tehostamiseksi.

Tietoturvakäyttäytymisen yksi keskeisimmistä piirteistä liittyy tietoturvauhkien ja niiden vaikutusten ymmärtämiseen. Huigangin ja Yajiongin (2010) tietoturvakäyttäytymiseen liittyvä tutkimus kohdistui tietokonekäyttäjien pyrkimykseen välttää tietoturvauhkia. Tutkimuksen tuloksissa todetaan, että tietoturvauhkia välttävää tietoturvakäyttäytymistä voidaan ennustaa ihmisen motivaatiolla välttää tietoturvauhkia. Motivaatioon vaikuttavat ymmärrys uhkasta, suojauksen tehokkuus ja kustannukset sekä mahdollisuus vaikuttaa itse tilanteeseen. Kun tietokoneen käyttäjillä on ymmärrys mahdollisesta tietoturvauhkasta, he pyrkivät havainnoimaan mahdollista uhkaa. Jos uhka toteutuu, he kokevat negatiiviset seuraamukset ankarina. Kun käyttäjät ovat tiedostaneet tietoturvauhkan olemassaolon, heidän motivaatiota pyrkiä estämään uhkan toteutuminen lisää, jos he pitävät suojauksia tehokkaina ja halpoina sekä, jos he kokevat osaavansa käyttää suojausta. Tutkimuksen tuloksissa esitetään, että uhkan tiedostamisella ja suojauksen tehokkuudella on negatiivinen vaikutus tietoturvauhkan välttämiseen pyrkivään motivaatioon: mitä paremmin työntekijä ymmärtää tietoturvauhkaa sitä vähemmän merkitystä on suojauksen tehokkuudella ja tietoturvauhkan toteutumisen välttämistä pyrkivällä motivaatiolla. Suojauksen tehostaminen puolestaan vähentää motivaatiota pyrkiä ymmärtämään uhkaa ja välttämään sen toteutumista.

Tietoturvakäyttäytymistä pystytään ohjaamaan ja seuraamaan tietoturvaohjelmilla. Dey, Lahiri ja Zhang (2012) toteavat, että tietoturvaohjelmien myynnissä on viime vuosina tapahtunut suuri kasvu ja markkinoista kilpailee suuri joukko myyjiä. Tutkimuksessaan he selvittävät miten tietoturvaohjelmien myynti eroaa muiden ohjelmien myynnistä. Tutkimuksessa luodaan taloudellinen malli, jossa tietoturvaohjelmien määritelmiä tehdään erilaisten tietoturvahyökkäysten ja niiden tietoverkkoon aiheuttamien vaikutusten pohjalta. Tulosten mukaan epäsuorista hyökkäyksistä aiheutuvat negatiiviset vaikutukset tietoverkkoon selittävät jollain tavalla markkinoiden ainutlaatuista rakennetta. Tutkimuksen tuloksissa korostetaan tietoturvaohjelmien markkinoiden ainutlaatuisuutta, yleisesti tietoturva-alalla

vallitsevaa asioiden tarkkaa määrittelyä ja huomioimista maailmalla sekä johdon asettamia näkemyksiä markkinakilpailulle.

Tietoturvakäyttäytymistä ohjeistetaan tietoturvastandardeilla. Hui, Hui ja Yue (2012) toteavat, että tietoverkkojen nopea kasvu on lisännyt tietoturvastandardien määrää. Heidän tekemässä tutkimuksessa analysoidaan tietojärjestelmien keskinäisistä riippuvuuksista aiheutuvien riskien ja standardeista syntyvien tietoturvavaatimusten keskinäistä suhdetta sekä tutkitaan vaikuttaako se tietoturvapalveluntarjoajan ja asiakkaan väliseen käyttäytymiseen. Tulosten mukaan standardeista syntyvät vaatimukset nostavat palveluntarjoajan motivaatiota ja pyrkimystä palvella asiakasta paremmin. Vaikka asiakas hyötyy palveluntarjoajan tietoturvapalvelusta, on huomioitava, että palvelu lisää järjestelmien keskinäisistä riippuvuuksista aiheutuvia riskejä. Standardeista aiheutuvat liian kovat tietoturvavaatimukset ja vaatimus todistettavuudesta alentavat sosiaalista hyvinvointia. Tutkimuksen johtopäätöksenä todetaan, että viimeaikaiset aloitteet tietokoneiden pakollisesta tietoturvasuojauksesta tai tietoturvapalveluntarjoajien valvonnan edistämisestä eivät välttämättä ole suositeltavia.

Yrityksen tietojenkäsittelyssä käytettävien ohjelmistojen päivittäminen on olennaista tietoturvan toteuttamisessa. Temizkan, Kumar, Park ja Subramaniam (2012) ovat luoneet tutkimuksessaan mallin, jolla voidaan analysoida ohjelmistotoimittajien toimintaa ohjelmistojen päivitysten julkaisemisessa. Malli auttaa ymmärtämään miten haavoittuvuudet, päivitykset, ohjelmistotoimittajat ja ohjelmistot vaikuttavat ohjelmistotoimittajien ohjelmistojen päivitysten julkaisukäyttäytymiseen ja kustannuksiin. Tulosten mukaan haavoittuvuudet, joilla on suuri vaikutus ohjelmiston luottamuksellisuuteen tai eheyteen, päivitetään nopeammin kuin ohjelmiston käytettävyyteen vaikuttavat haavoittuvuudet. Erityisesti lainvastaiset haavoittuvuudet korjataan nopeasti. Tuloksista ilmenee, että päivitysten julkaisukäyttäytymisessä on eroja myös sen mukaan onko julkaistava ohjelmisto kokonaan uusi vai onko se vanhaan tuleva päivitys, sekä sen mukaan pohjautuuko ohjelmisto avoimeen lähdekoodiin vai onko ohjelmisto oma.

Tietoturvakäyttäytyminen ja tietoturvatietoisuus

Yrityksissä tietoturvan toteuttamisen keskeisimmässä roolissa ovat yrityksen työntekijät. Positiivinen tietoturvakäyttäytyminen edellyttää yrityksen työntekijöiltä tietoturvatietoisuutta. Leach (2003) toteaa artikkelissaan, että useissa yrityksissä sisäisiä tietoturvauhkia pidetään ulkoisia tietoturvauhkia uhkaavampina. Sisäiset tietoturvauhkat johtuvat yleisimmin työntekijöiden huonosta tietoturvakäyttäytymisestä. Tästä huolimatta tulosten mukaan yritysten tietoturvaohjelmat innostavat työntekijöitä heikosti eikä niillä ole työntekijöiden tietoturvakäyttäy-

tymiseen parantavaa vaikutusta. Nämä tulokset ovat erittäin mielenkiintoisia tämän tutkimuksen yhteydessä.

Myös Albrechtsen (2007) on todennut, että käyttäjä on merkittävässä roolissa yrityksen tietoturvan toteuttamisessa. Aiemmissa tutkimuksissa on korostettu käyttäjän tietoturvatietoisuuden ja käyttäytymisen varovaisuuden tason merkitystä. Albrechtsenin tutkimuksessa selvitettiin käyttäjien kokemusta oman roolin merkityksestä yrityksen tietoturvan toteuttamisessa. Laadullisessa haastattelututkimuksessa haastateltiin yhdeksää it-yrityksen ja pankin käyttäjää. Tulosten mukaan työntekijät ovat yleisesti motivoituneita toimimaan yrityksessä tietoturvallisesti, mutta liiallinen tietoturvasta aiheutuva työmäärä aiheuttaa ristiriitoja työtehtävien toteuttamisen ja tietoturvaohjeiden noudattamisen välille. Tuloksista käy myös ilmi, että pelkästään dokumenteilla ja kampanjatyylisellä tiedottamisella hoidetuilla tietoturvaohjeilla on vain vähän vaikutusta työntekijän tietoturvatietoisuuteen ja -käyttäytymiseen. Tulosten mukaan työntekijät pitävät osallistuvaa tietoturvaohjeiden omaksumista tehokkaampana keinona vaikuttaa työntekijän tietoturvatietoisuuteen ja -käyttäytymiseen. Myös nämä tulokset ovat erittäin mielenkiintoisia tämän tutkimuksen yhteydessä.

Tietoturvan toteuttamiseen ja tietoturvakäyttäytymiseen vaikuttavat olennaisesti työympäristö ja laitteet. Culnan, Foxman ja Ray (2008) toteavat, että suuri osa työntekijöistä työskentelee ainakin osittain etätyönä ja työntekijät tallettavat työtehtäviinsä kuuluvia tietoja kotitietokoneilleen. Tutkimuksessaan he selvittivät voidaanko tietoturvatietoisuudella ja koulutuksella vaikuttaa työntekijöiden haluun turvata tietokoneet myös kotona. Tutkimuksessa tarkasteltiin erityisesti työntekijän asennetta ja käyttäytymistä. Tulosten mukaan tietoturvatietoisuuden lisäämisellä ja koulutuksella pystyttiin vaikuttamaan henkilön tietoturvakäyttäytymiseen kotitietokoneen tietoturvaa parantavalla tavalla. Tutkimuksen johtopäätöksinä ehdotetaan, että yritysten tulisi panostaa myös työntekijöiden kotitietokoneiden tietoturvan parantamiseen lisäämällä työntekijöiden tietoturvatietoisuutta ja -koulutusta. Työntekijöiden kotitietokoneiden käyttö etätyössä tulisi huomioida myös yrityksen riskienhallinnassa.

Rhee, Kim ja Ryu (2009) ovat todenneet, että tietoturvassa onnistuminen vaatii loppukäyttäjältä sopivia tietoturvakäytänteitä ja sopivaa tietoturvakäyttäytymistä. Tutkimuksessa tarkasteltiin työntekijän oman vaikutuksen, tietoturvakäyttäytymisen ja motivaation keskinäistä riippuvuutta sekä työntekijän menneisyyden vaikutusta tehokkaampaan tietoturvatoimintaan. Tulosten mukaan pelkästään listaamalla tietoturvan kannalta kielletty toiminta ja siitä seuraavat rangaistukset vaikuttavat työntekijän positiiviseen tietoturvakäyttäytymiseen heikosti. Siksi yritysten tulisi pyrkiä työntekijöiden parempaan tietoturvakäyttäytymiseen esimerkiksi

ottamalla työntekijät mukaan tietoturvaohjelman laatimiseen. Nämäkin tulokset ovat mielenkiintoisia tämän tutkimuksen yhteydessä.

Positiivinen tietoturvakäyttäytyminen edellyttää kaikkien työntekijöiden osallistumista yrityksen tietoturvan toteuttamiseen. Albrechtsen ja Hovden (2010) ovat käsitelleet artikkelissaan tietoturvatietoisuuden lisäämistä. Siinä painotetaan työntekijöiden osallistumista, vuoropuhelua ja tietoturva-asioiden yhteistä käsittelyä ryhmissä, joiden tavoitteena on parantaa tietoturvatietoisuutta ja -käyttäytymistä. Kokeellisen tutkimuksen tulokset osoittavat, että työntekijöiden osallistumisella, vuoropuhelulla ja tietoturvan-asioiden käsittelyllä yhteisesti ryhmässä pystytään jo lyhyellä aikavälillä merkittävästi muuttamaan työntekijöiden tietoturvatietoisuutta ja -käyttäytymistä. Myös Mensch ja Wilkie (2011) ovat käsitelleet artikkelissaan tietoturvatietoisuuden parantamista tutkiessaan opiskelijoiden tietoturva-asenteita, -käyttäytymistä ja -työkaluja. Tutkimuksen mukaan opiskelijat käyttävät keskinäiseen kommunikointiin pääasiassa sähköpostia ja sosiaalista mediaa. Samalla he altistuvat identiteettivarkauksille.

Tietoturvakäyttäytyminen ja tietoturvakulttuuri

Yksittäisen työntekijän tietoturvakäyttäytymiseen vaikuttaa merkittävästi yrityksessä yleisesti vallitseva tietoturvakulttuuri. Da Veiga ja Eloff (2007) arvioivat tutkimuksessaan yrityksen tietoturvan hallintatapoja. He toteavat artikkelissaan, että yrityksen tietoturvakulttuuri kehittyy yrityksessä toteutettavilla toimenpiteillä. Yrityksen johto kehittää tietoturvaa luomalla työntekijöiden jokapäiväiseen käyttöön tietoturvaelementtejä, joita ovat esimerkiksi tietoturvaohjeet ja tietoturvan mittaamiseen käytettävät tekniset välineet. Tietoturvaelementteihin pohjautuen työntekijä luo itselleen tietynlaisen tietoturvan havainnointi- ja käyttäytymismallin. Tutkimuksen tuloksena syntyy lista hyväksyttävään tietoturvakulttuuriin yrityksissä tarvittavista tietoturvaelementeistä. Elementtien avulla yrityksessä pystytään huomioimaan tietoturva kokonaisvaltaisesti sekä pystytään minimoimaan riskit ja luomaan riittävä tietoturvakulttuuri.

Tietoturvakäyttäytymisen keskiössä ovat käyttäjä ja tietokone. Ng, Kankanhalli ja Xu (2009) ovat tutkineet mitkä asiat vaikuttavat käyttäjän turvalliseen tietokoneen käyttöön. Heidän kyselytutkimukseensa osallistui yhteensä 134 työntekijää kolmesta it-yrityksestä ja yliopistolta. Tulosten mukaan sähköpostin turvalliseen käyttöön vaikuttavat ymmärrys altistumisesta tietoturvauhkille, ymmärrys tietoturvan olemassaolon hyödyllisyydestä ja ymmärrys mahdollisuudesta itse vaikuttaa tilanteeseen. Tuloksissa todetaan myös, että työntekijän kokemus ankarasta tietoturvakulttuurista vaikuttaa negatiivisesti yleiseen suhtautumiseen tietoturvaa kohtaan sekä vähentää ymmärrystä tietoturvan toteuttamisen hyödyllisyydestä ja

mahdollisuudesta itse vaikuttaa tilanteeseen. Negatiivinen tietoturvakulttuuri myös vähentää työntekijöiden antamia vihjeitä tietoturvauhkista.

Myös Da Veiga ja Eloff (2010) ovat todenneet, että työntekijän tietoturvakäyttäytymisen ja yrityksen tietoturvakulttuurin vuorovaikutusta ei ole juurikaan tutkittu. He ovat myös todenneet, että yritysten tulisi keskittyä yrityksen tietoturvatoiminnassa työntekijöiden käyttäytymiseen, koska yrityksen onnistuminen tietoturvatoiminnassa riippuu siitä mitä työntekijät tekevät ja miten heidän toimintansa onnistuu. Yrityksen tietoturvakulttuurilla pystytään vähentämään yrityksen tietopääomaan liittyviä riskejä sekä vähentämään työntekijöiden tietopääoman väärinkäyttöä ja vahingoittamista. Tämä tieto on mielenkiintoista tämän tutkimuksen yhteydessä. Da Veigan ja Eloffin mukaan yritykset tarvitsevat tukea ja ohjeita yrityksen tietoturvaohjeiden julkaisemiseen ja hyvän tietoturvakulttuurin luomiseen yrityksessä. Tutkimuksen tuloksena luodaan malli yrityksen tietoturvakulttuurin luomiselle ja annetaan neuvoja sen soveltamiseen yrityksessä.

Yrityksen tietoturvan tasoon vaikuttavat merkittävästi eniten yrityksen omat työntekijät. Guo, Yuan, Archer ja Connelly (2011) toteavat, että työntekijät käyttäytyvät tietoisesti tietoturvaa uhkaavasti ja toimivat tietoisesti tietoturvaohjeiden vastaisesti. Työntekijöillä ei ole kuitenkaan pahantahtoisia aikomuksia. Tutkimuksessaan Guo ja muut laativat hyväntahtoisen tietoturvarikkomuksen mallin ja testaavat sitä. Tulosten mukaan tietokoneen käyttäjät saadaan sitoutettua malliin kertomalla käytännön hyödyistä, normatiivisista hyödyistä ja tunnistautumisen hyödyistä. Tuloksissa nostetaan esille neljä tekijää, joilla työntekijän asenteisiin voidaan vaikuttaa: korostamalla työtehtävien tavoitteiden ja tietoturvariskien ymmärtämisen tärkeyttä, osoittamalla ryhmätyösääntöjen vaikutus käyttäjän asenteisiin ja käyttäytymiseen, esittelemällä ja testaamalla tunnistautumisen vaikutus käyttäjän asenteisiin ja tavoitteisiin sekä määrittelemällä käsitteiden väliset suhteet. Tutkimuksen tuloksena tuodaan esille myös tietoturvan ja liiketoiminnan tavoitteiden samansuuntaisuuden tärkeys, tietoturvamittareiden vaikutus sekä yrityksen tietoturvakulttuurin merkitys työntekijöille.

Tietoturvakäyttäytyminen ja tietoturvan noudattaminen

Positiivinen tietoturvakäyttäytyminen näkyy yrityksissä käytännössä työntekijöiden tietoturvan noudattamiseen pyrkivänä toimintana ja myönteisessä suhtautumisessa tietoturvan toteuttamiseen. Myyry ja muut (2009) ovat tutkineet miten moraalinen perustelu ja arvot vaikuttavat työntekijään, kun hän pyrkii noudattamaan tietoturvaohjeita. Heidän tutkimuksensa pohjautui moraalisen päättelyn teorioihin ja tutkimuksen kyselyyn vastasi erään yrityksen 163 työntekijää. Tutkimuksen tulosten mukaan järjestelmien tietoturvasääntöjen laiminlyöminen on iso ongelma yrityksissä. Tavanomaisilla moraalisilla perusteluilla on negatiivinen

vaikutus työntekijöiden käyttäytymiseen. Sen sijaan epätavalliset moraaliset perustelut vaikuttavat työntekijöiden tietoturvaohjeiden noudattamiseen positiivisesti. Tuloksien perusteella ehdotetaan, että yrityksillä tulisi olla sopivia rangaistuskeinoja, jotta työntekijät saataisiin noudattamaan tietoturvaohjeita. Tutkimuksen tulokset ovat mielenkiintoisia tämän tutkimuksen yhteydessä.

Myös Herath ja Rao (2009b) ovat tutkineet työntekijöiden tietoturvaohjeiden noudattamista yrityksissä. Tutkimuksessa arvioitiin työntekijöiden motivaatiota kokonaisvaltaisesti suojautua tietoturvauhkilta. Tutkimuksen aineistona kerättiin 312 työntekijältä 77 organisaatiosta. Tutkimuksessa käytettiin pelotemallia. Tuloksista käy ilmi, että työntekijöiden asenteisiin tietoturvaohjeita kohtaan vaikuttaa heidän havaintonsa riskeistä. Resurssien saatavuus on tärkeää työntekijöiden käsitykselle mahdollisuudesta vaikuttaa itse asiaan. Artikkelissa huomautetaan, että suurin osa tutkituista työntekijöistä oli sitä mieltä, että omassa yrityksessä ei ole aukkoja tietoturvassa. Tutkimuksen tulokset ovat mielenkiintoisia tämän tutkimuksen yhteydessä.

Erityisen mielenkiintoinen on tämän tutkimuksen yhteydessä Bulgurcun, Cavusoglun ja Benbasatin (2010) tutkimus tekijöistä, jotka vaikuttavat työntekijän positiiviseen suhtautumiseen yrityksen tietojen ja tietojenkäsittelymenetelmien suojaamiseen laadittujen tietoturvaohjeiden noudattamisessa. He toteavat, että yleisten normatiivisten uskomusten ja omien vaikutusmahdollisuuksien mukaisesti työntekijän asenne tietoturvaohjeiden noudattamiseen on suhteessa tietoturvaohjeiden noudattamisen tavoitteellisuuden tasoon. Heidän tutkimuksensa kyselyyn vastasi 464 työntekijää. Tutkimuksen tulosten mukaan työntekijän pyrkimykseen noudattaa tietoturvaohjeita vaikuttavat merkittävästi asenne, normatiiviset uskomukset ja oma mahdollisuus vaikuttaa asiaan. Tutkimuksen keskeisenä tuloksena todetaan, että työntekijän asenteeseen vaikuttavia tekijöitä ovat noudattamisesta saatava hyöty sekä noudattamisesta ja noudattamatta jättämisestä aiheutuvat kulut. Hyötyjen ja kulujen määrän työntekijät arvioivat siitä, mitä he olettavat aiheutuvan noudattamisen ja noudattamatta jättämisen seurauksista. Noudattamisen hyötyinä työntekijät näkevät todelliset hyödyt, resurssien turvallisuuden ja palkkiot. Noudattamisesta aiheutuvina kuluina työntekijät näkevät haitat työskentelyssä. Noudattamatta jättämisen kulut muodostuvat todellisista kuluista, resurssien haavoittuvuudesta ja sanktioista. Tutkimuksessa korostetaan tietoturvatietoisuuden ja noudattamiseen liittyvien uskomusten merkitystä yrityksen pyrkimyksessä saada työntekijät noudattamaan yrityksen tietoturvaohjeita.

Tietoturvakäyttäytymisen ja tietoturvan noudattamisen yhtenä keskeisenä tekijänä yrityksissä on yrityksen tarjoama tietoturvakoulutus. Tämä korostuu työhöntuloperehdytyksessä. Karjalainen ja Siponen (2011) ovat todenneet, että olemassa

olevassa kirjallisuudessa ei ole tutkittu tietoturvakoulutuksen peruspiirteitä. Kirjallisuudessa ei ole myöskään tutkittu miten tietoturvakoulutus eroaa muusta koulutuksesta. Tutkimuksessaan he selvittävät mitä tietoturvakoulutuksen peruspiirteet ovat ja miten ne vaikuttavat tietoturvakoulutuksen periaatteisiin käytännössä. Lisäksi tutkimuksessa määritellään pedagogisia vaatimuksia tietoturvakoulutuksen suunnitteluun ja arviointiin.

Son (2011) toteaa, että yrityksissä on ymmärretty työntekijän merkittävä rooli tietoturvan toteutumisessa. Sen seurauksena on viime aikoina alettu entistä enemmän kiinnittää huomiota miten työntekijöitä pystytään motivoimaan parempaan tietoturvatoimintaan yrityksessä. Sonin mukaan aiemmissa tutkimuksissa on käytetty peloteteoriaa soveltamalla sitä ulkoisen motivaation teoriaan ja niillä on etsitty vastausta miksi työntekijät toteuttavat tai eivät toteuta yrityksen tietoturvaohjeita. Son uskoo, että työntekijän tietoturvaohjeita noudattavaa käyttäytymistä pystyttäisiin paremmin selittämään sisäiseen motivaatioon pohjautuvalla teorialla, ja siksi hän loi työntekijän tietoturvaohjeiden noudattamista selittävän mallin, jossa yhdistettiin sekä ulkoinen että sisäinen motivaatio. Mallia testattiin tutkimuksessa, johon osallistui 602 amerikkalaista työntekijää. Tulosten mukaan sisäisesti motivoivilla tekijöillä on huomattavasti tehokkaampi vaikutus työntekijän tietoturvaohjeiden noudattamiseen kuin ulkoisesti motivoivilla tekijöillä. Sisäisten ja ulkoisten motivaatiotekijöiden vaikutukset tietoturvaohjeiden noudattamiseen on välttämätöntä ottaa huomioon ja siksi Sonin tulokset ovat tämän tutkimuksen kannalta erittäin mielenkiintoisia.

Internetin käytön jatkuva kasvu on tehnyt tietoturvasta erittäin keskeisen asian yhteiskunnalle. Tämä korostuu nuorilla aikuisilla, joiden asenteissa tietoturvakäytänteitä kohtaan on eroja. Näin toteavat Cheolho, Jae-Won ja Kim (2012) tutkimuksessaan, jossa tarkastellaan toisen asteen opiskelijoiden tietoturvakäyttäytymisen motivointiin vaikuttavia tekijöitä. Tutkimuksessa käytetään Rogersin (1975) kehittämää suojelumotivaatioteoriaa, jota laajennetaan sosiaalisilla normeilla ja käyttäytymistavoilla. Tutkimuksen aineisto muodostui 202 vastaajasta. Tulokset osoittavat, että opiskelijat ovat erittäin motivoituneita toteuttamaan tietoturvaa, jos he ymmärtävät tilanteen vakavuuden, kokevat tietoturvakäytännön tehokkaana ja taloudellisena sekä, jos he kokevat voivansa itse vaikuttaa tilanteeseen. Heidän tietoturvaan liittyviin pyrkimyksiinsä eivät kuitenkaan vaikuta koetut tietoturvahaavoittuvuudet tai sosiaalinen paine. Tulosten mukaan opiskelijoiden motivaatioon voidaan vaikuttaa antamalla heille koulutusta tietoturvatietoisuudesta ja saamalla heidät ymmärtämään tilanteen vakavuuden.

Tietoturvatietoisuus ja tietoturvakulttuuri

Tietoturvatietoisuutta ja -kulttuuria ovat tutkineet D'Aubeterren, Singhn ja Iyern (2008). Heidän tutkimuksessa keskitytään turvallisen liiketoimintaprosessin suunnitteluun. Tutkimuksessa selvitetään miten turvallisuustoiminnan resursseja tulisi koordinoida. Erityisesti tietoturvakulttuuria on tutkinut Rotvold (2008). Hän on kartoittanut mitä keinoja yrityksellä on luoda yritykseen tietoturvakulttuuri. Tulosten mukaan arviointi, tiedossa olevat menettelytavat erilaisissa tilanteissa sekä teknisesti tehty testaaminen ovat tärkeitä keinoja tietoturvatietoisuuden parantamisessa. Lisäksi tietoturvakoulutus koetaan tulosten mukaan yrityksissä tärkeäksi. Koulutuksen tarpeisiin tulisi luoda kattavat ohjeet ja koulutuksessa tulisi keskittyä erityisesti niiden ymmärtämiseen. Tutkimuksen mukaan ohjeissa tulisi kertoa yksityiskohtaisesti mikä on hyväksyttävää tietokoneen käyttöä sekä miten tietoturvatietoisuutta arvioidaan.

Maailmanlaajuisesti tietoturvatietoisuuden ja tietoturvakulttuurin tilannetta ovat tutkineet Hovav ja D'Arcy (2012), jotka kokevat, että työntekijöiden tahallinen huono tietoturvakäyttäytyminen on maailmanlaajuinen ongelma. Lisäämällä vastatoimia, kuten tietoturvan tahallisen laiminlyömisen kiinnijäämisen ja ankaran rankaisemisen todennäköisyyttä, pystytään vähentämään työntekijöiden tahallista huonoa tietoturvakäyttäytymistä. Tutkimuksessaan Hovav ja D'Arcy selvittivät onko kansallisuuteen liittyvällä yleisellä kulttuurilla vaikutusta pyrittäessä ehkäisemään tahallista huonoa tietoturvakäyttäytymistä. Tietoturvakäyttäytymisen tarkastelussa keskityttiin tietoturvaohjeisiin, -koulutukseen, -tietoisuuteen ja -seurantaan. Tulosten mukaan vastatoimien tehokkuudessa on kahden maan välisillä kulttuureilla yhtä paljon vaikutusta tietoturvakäyttäytymiseen kuin mitä ikä ja sukupuoli vaikuttavat tietoturvakäyttäytymiseen.

Tietokoneen hyväksikäyttö ja väärinkäyttö

Tietokoneen väärinkäyttöä ovat tutkineet Drevin, Kruger ja Steyn (2007). Tutkimuksen tavoitteena oli löytää tietoturvaohjelman perustavoitteet ja keskeisimmät ohjeet. Heidän mukaansa tietoturvatietoisuudella on merkittävä rooli, kun pyritään vähentämään työntekijöiden tietokoneiden väärinkäyttöä. Tietoturvatietoisuudella on merkittävä rooli myös silloin, kun pyritään vähentämään työntekijöiden tekemiä virheitä, varkauksia ja petoksia. Jotta yritykseen muodostuu hyvä ja vahva tietoturvakulttuuri, täytyy yrityksen laatia tietoturvaohjelma. Tutkimuksen tulosten mukaan tietoturvaohjelman perustavoitteet liittyvät yleisesti tunnistettuihin tietoturvavaatimuksiin tiedon käytettävyydestä, eheydestä ja luottamuksellisuudesta. Näitä perustavoitteita voidaan käyttää tietoturvaohjelman laadinnassa. Tuloksissa havaittiin myös hallinnon ja sosiaalisuuden huomioimisen merkitys tietoturvaohjelman laadinnassa. Niillä pystytään vaikuttamaan esimerkiksi työn-

tekijän vastuullisuuteen ja tehokkuuteen tietojen käytössä. Erityisesti hallinnon merkityksen korostuminen tuloksissa on merkillepantavaa tämän tutkimuksen yhteydessä.

Työpaikan tietokoneen väärinkäyttö aiheuttaa tietoturvauhkia yrityksen tietoturvalle. D'Arcy, Hovav ja Galletta (2009) toteavat tutkimuksessaan, että jopa 75 % yritysten tietoturvahaavoittuvuuksista tulee yrityksen sisältä. Tämän takia on tärkeää ymmärtää työntekijöiden tietoturvakäyttäytymistä ja miten näiden aiheuttamien haavoittuvuuksien määrää pysyttäisiin alentamaan. Yhtenä keinona nähdään väärinkäytöstä saatavan rangaistuksen todennäköisyyden lisäämistä. D'Arcy, Hovav ja Galletta loivat käsitteellisellä analyysillä tehdyn tutkimuksensa tuloksena mallin, jossa rankaisemisen tukena tietoturvaväärinkäytös määritellään rikolliseksi. Rankaisemisen tukena käytetään myös sosiaalipsykologiaa. Väärinkäytösten havaitsemiseksi hyödynnetään tietojärjestelmiä. Tuloksista ilmenee, että työntekijän tietoisuus tietoturvan seuraamisesta erilaisilla mittareilla lisää väärinkäytöksestä rankaisemisen varmuuden ja ankaruuden tajuamista, minkä seurauksena väärinkäytökset vähenevät. Tulosten pohjalta ehdotetaan, että väärinkäyttöä voidaan vähentää lisäämällä työntekijöiden tietoisuutta tietoturvaohjeista sekä tietoturvakoulutuksella ja -harjoituksilla. Väärinkäyttöä voidaan vähentää myös lisäämällä tietokoneiden käytön seurantaa. Väärinkäytösten vähentämiseksi on tehokkaampaa saada työntekijä ymmärtämään rangaistusten ankaruus kuin se mikä on rangaistusten toteutumisen todennäköisyys. Tulosten mukaan myös työntekijöiden moraalikäsitykset vaikuttivat ymmärrykseen rangaistusten vaikutuksista.

D'Arcy ja Herath (2011) tarkastelevat ja analysoivat tutkimuksessaan tietoturvaa peloteteorian pohjalta. Peloteteorian katsotaan soveltuvan vaativampien tietoturvan hallintastrategioiden pohjaksi. Tutkimuksen tuloksista käy ilmi, että peloteteoriaa käyttävissä tutkimuksissa tuloksiin aiheuttaa merkittävästi eroavaisuuksia tutkimukseen vaikuttavat epävarmat ja ennustamattomat muuttujat. Lowry, Moody, Galletta ja Vance (2013) tutkimuksen tulosten mukaan nimettömyys, luottamus ja riskit ovat keskeisimpiä löydettyjä tietoturvaheikkouksia, jotka tulevat esille yrityksen sisäisessä valvonnassa. Tutkimuksessaan he huomauttavat, että Sarbanes-Oxley-laki vaatii yrityksiä julkaisemaan sisäisessä valvonnassa havaitut heikkoudet julkisesti.

4 TIETOTURVAOHJEISTAJIA JA -OHJEISTUKSIA

Tässä luvussa esitellään Suomessa tietoturvaa ohjeistavia viranomaisia sekä luodaan katsaus niiden tietoturvaohjeistusten sisältöihin. Ohjeistuksissa keskitytään erityisesti pk-yritykselle suunnattuihin tietoturvaohjeistuksiin. Luvussa käytettävä termistö tullaan kuvaamaan alkuperäisessä lähteessä olevan termistön mukaisena, koska dokumenttien sisällön analysointi on yksi tutkimuksen tavoitteista. Sisällön pohjalta muodostetaan myöhemmin kohdassa 5.1 tietoturvakriteerejä.

Suomessa tietoturvaa ohjeistavia viranomaisia ovat muun muassa Suomen eduskunta lakeja säätäessään, Euroopan unioni, Euroopan verkko- ja tietoturvavirasto (ENISA), Kansainvälinen standardisoimisjärjestö ISO, Suomen Standardisoimisliitto SFS, liikenne- ja viestintäministeriö, valtiovarainministeriö, sisäasiainministeriö, puolustusministeriö sekä työ- ja elinkeinoministeriö, Viestintävirasto, CERT-FI, NCSA-FI sekä Valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI). Lisäksi erityisesti Suomen pk-yritysten tietoturvaa ohjeistavia tahoja ovat Elinkeinoelämän keskusliitto EK, Yritysturvallisuus EK Oy, TIEKE Tietoyhteiskunnan kehittämiskeskus ry, Arjen tietoyhteiskunnan tietoturvallisuus -ryhmä sekä Teknologian tutkimuskeskus VTT. Laaksonen ja muut (2006: 125) nimeävät tietoturvaa ohjeistaviksi viranomaisiksi lisäksi ulkoasiainministeriön ja Rahoitustarkastuksen, joka määrittelee tilojen fyysistä suojausta.

Suomessa huomioitavia tietoturvaohjeistuksia ovat muun muassa Suomen lainsäädäntö, EU:n lainsäädäntö, ISO:n tietoturvastandardit, VAHTI-ohjeistukset, Kansallinen turvallisuusauditointikriteeristö (KATAKRI), Kansallinen tietoturvastrategia sekä eri viranomaistahojen tietoturvaoppaat.

4.1 Suomen ja EU:n lainsäädäntö, kansainvälinen normisto sekä Euroopan verkko- ja tietoturvavirasto (ENISA)

Suomen lainsäädännössä ei ole erillistä lakia, jossa säädettäisiin tyhjentävästi tietokoneenkäyttäjien tietoturvaa tai sen velvoitteita ja oikeuksia. Julkisuudessa käydyissä keskusteluissa tällaisen lain säätäminen on todettu tarpeettomaksi. Myöskään yritykset ja lainsäätäjät eivät ole nähneet tarvetta lainsäädännön lisäämiselle erityisenä tietoturvalakina. Sen sijaan lainsäätäjä on sisällyttänyt tietoturvavelvoitteet osaksi muiden lakien sisältöä. Vaikka lainsäätäjä on nähnyt tämän tavan perustellusti parempana, vaikeuttaa se kuitenkin tietoturvan toteuttamista käytännössä, koska tapa hajauttaa tietoturvanormiston lukuisiin lakeihin. (Laaksonen ym. 2006: 21, 27.)

Tietoturvan määritelmä tietojen käytettävyydestä, eheydestä ja luottamuksellisuudesta ei suoraan kerro millaisilla normeilla tietoturvasta olisi säädettävä laissa (Saarenpää ym. 1997: 75). Suomen lainsäädännössä on tietoturvaa koskien määritelty perusteellisesti vain tunnistamistietojen ja viestin sisällön käsittelyt. Muiden tietoturvatoimenpiteiden käsittelyperusteet eivät ole lakiteksteissä yhtä selkeitä. Lakiin perustuvien tietoturvavelvoitteiden hoitaminen vaatii hyvää perehtymistä lainsäädäntöön. Lisäksi on tunnistettava yrityksen käyttämät tietojärjestelmät ja muut viestintävälineet. (Laaksonen ym. 2006: 80–82.)

Laaksosen ja muiden (2006: 23, 28–31, 47–49, 54–79) mukaan tietoturvaa käsitellään Suomen lainsäädännössä seuraavissa kohdissa:

- Perustuslaki (10 § yksityisyyden suoja)
- Sähköisen viestinnän tietosuojalaki
- Laki kansainvälisistä tietoturvallisuusvelvoitteista
- Viestintämarkkinalaki
- Laki viranomaisten toiminnan julkisuudesta (julkisuuslaki)
- Laki tietoyhteiskunnan palvelujen tarjoamisesta
- Laki yksityisyyden suojasta työelämässä
- Henkilötietolaki
- Laki sähköisestä asioinnista viranomaistoiminnassa
- Laki sähköisestä allekirjoituksesta
- Rikoslaki 30: 4–6 § (yritysvakoilu, yrityssalaisuuden rikkominen, yrityssalaisuuden väärinkäyttö)

Suomen lainsäädännön lisäksi on hyvä huomioida OECD:n tietoturvaohjeistus ja Sarbanes-Oxley-laki. OECD:n tietoturvaohjeistus laadittiin ensimmäisen kerran vuonna 1992. Vuonna 2002 ohjeistusta päivitettiin ja tuolloin siihen lisättiin ensimmäistä kertaa käsite tietoturvakulttuuri. Ohjeistuksen lähtökohtana on tietoturvasuunnittelun ja -hallinnon korostaminen. Ohjeistuksessa tuodaan myös esille, että kaikkien tulee ymmärtää tietoturvan tarve. Tällä halutaan korostaa, että hallinnon ja elinkeinoelämän kaikkien tasojen ja tahojen tulisi huolehtia ja ottaa vastuuta tietoturvasta. Ohjeistuksen tietoturvaperiaatteissa tietoturvan rakentaminen, siitä huolehtiminen ja sen kehittäminen nähdään prosessina. Ohjeistuksessa käsitellään seuraavia teemoja: *”turvallisuustietoisuus, vastuullisuus, vastatoimet, eettisyys, demokratia, riskien arviointi, turvallisuuden suunnittelu ja täytäntöönpano, turvallisuuden hallinta sekä uudelleenarviointi”*. Ohjeistus on laajasti huomioitu kansainvälisessä ja Suomen lainsäädännössä. Suomessa ohjeistus huomioidaan VAHTI-ryhmän tietoturvaohjeistuksissa. Myös BS 7799/ISO27002 -standardi huomioi ohjeistuksen tietoturvaperiaatteet. Sarbanes-Oxley-laki (Sarbanes-Oxley Act, SOX) on Yhdysvaltain liittovaltion laki. Mikäli suomalainen yritys on noteerattu Yhdysvaltain pörssissä, tulee sen huomioida käytännöissään

Sarbanes-Oxley-lain määräykset yrityksen hallinnosta, johtamisesta ja tilintarkastusyhtiöiden toiminnasta. (Laaksonen ym. 2006: 23–24; Suomen Standardisoimisliitto 2007.)

EU:n lainsäädännössä on säädetty useita tietoturvaa käsitteleviä direktiivejä, jotka on sittemmin sisällytetty Suomen lainsäädäntöön. Tällaisia ovat esimerkiksi tietosuojaa sekä sähköistä kaupankäyntiä ja allekirjoitusta koskevat direktiivit. EU-lainsäädännön kaksi tärkeintä tietoturvaa käsittelevää direktiiviä koskevat henkilötietojen suojaa ja sähköisen viestinnän tietosuojaa. Sähköisen viestinnän tietosuojassa sähköisen palveluntarjoaja velvoitetaan toteuttamaan tarvittavat toimenpiteet, jotta sen tarjoamat palvelut ovat turvallisia, sekä ilmoittamaan verkon turvallisuuteen vaikuttavista tietoturvariskeistä. (Laaksonen ym. 2006: 26–27.)

Rikoslaissa säädetään, että salassapitorikoksen tunnusmerkit täyttävät annetut tiedot on suojattava. Tällaisia ovat yksityisyyttä käsittelevät tiedot sekä valtio- ja yrityssalaisuudet. (Leppänen 2006: 69.) Lapin yliopisto ja valtiovarainministeriö sopivat maaliskuussa 1997 tietoturvalain säätämistarvetta ja -edellytyksiä käsittelevän oikeudellisen asiantuntijaselvityksen laadinnasta. Tutkimusraportissa vuonna 1997 selvisi, että silloisessa Suomen lainsäädännössä oli vain muutamia selkeästi tietoturvanormeiksi nimettyjä normeja. Tietoturvaa ei ollut käsitelty oikeudellisena käsitteenä ja instituutiona. Tuolloin todettiin myös, että perusoikeuksien toteutuminen informaatiokeskeisessä ja tietotekniikkariippuvaisessa toimintaympäristössä edellyttää, että tietoturva on asianmukaisesti järjestetty. (Saarenpää ym. 1997: xxxii, 417.)

Euroopan unioni perusti Euroopan verkko- ja tietoturvaviraston (ENISA, European Network and Information Security Agency) vuonna 2004. Sen tehtävänä on neuvoa ja koordinoida komissiota ja EU:n jäsenvaltioita toimenpiteissä, joita ne tekevät tietoverkkojen ja -järjestelmien turvaamisessa. Viraston tavoitteena on parantaa Euroopan unionin, EU:n jäsenvaltioiden ja yritysten kykyä ehkäistä ja torjua verkko- ja tietoturvaongelmia ja puuttua niihin. Lisäksi viraston tavoitteena on varmistaa jäsenvaltioille riittävä tietoturvataso. Siihen pyritään helpottamalla ja edistämällä julkisen ja yksityisen sektorin yhteistyötä. Kreikassa sijaitsevan viraston ensimmäinen 8-vuotinen toimikausi päättyi maaliskuussa 2012. (Euroopan unioni 2010.)

4.2 ISO ja Suomen Standardisoimisliitto SFS: Tietoturvastandardit

Suomen Standardisoimisliitto SFS on Suomen standardisoinnin keskusjärjestö. Sen jäseniä ovat Suomen valtio ja joitakin suomalaisia elinkeinoelämän järjestöjä. SFS toimii ISOn (International Organization for Standardization) ja CENin (European Committee for Standardization) jäsenenä. CEN on eurooppalainen ja ISO kansainvälinen standardisoimisjärjestö. ISO on luonut tietoturvastandardeja, joiden tavoitteena on tietoturvasuunnittelun jäsentäminen ja organisointi. Standardit asettavat vaatimukset tietoturvasuunnittelun menettelytavoille. Ne sisältävät selkeän mallin tietoturvasuunnittelun dokumentoinnin rakenteelle, mihin tarkoitukseen ne ovat erityisen hyödyllisiä. Tietoturvastandardit eivät aseta vaatimuksia tietoturvan tasolle ja sisällölle. Tietoturvastandardit ovat kansainvälisiä ja kansallisia. (Hakala ym. 2006: 46; Suomen Standardisoimisliitto 2011a; International Organization for Standardization 2009.) Laaksosen ja muiden (2006: 86) mukaan ISO:n tietoturvastandardit ovat tarkoitettu ja suunniteltu erityisesti yksityisen sektorin käyttöön, mutta ne soveltuvat myös julkiselle sektorille.

ISOn keskeisiä tietoturvatekniikoiden standardisointialueita ovat muun muassa tietoturvan hallintajärjestelmät, suositukset, digitaalinen allekirjoitus, pääsynvalvonta, salaustekniikat ja tietoturvan arviointiperusteet (Suomen Standardisoimisliitto 2011b). Voimassa olevia (tilanne 21.9.2011) tietoturvatekniikan standardeja (IT Security techniques, JTC 1/SC 27) on 96 kappaletta (International Organization for Standardization 2011b).

Tietoturvatekniikoiden standardeista tämän tutkimuksen kannalta keskeisimmät ovat Tietoturvan arviointia käsittelevät standardit ISO/IEC 15408 Evaluation criteria for IT security ja ISO/IEC 18045 Methodology for IT security evaluation sekä Tietoturvan hallintajärjestelmien standardit, jotka julkaistaan ISO/IEC 27000 -sarjassa. ISO/IEC 15408 -standardi on julkaistu 3 osassa vuosina 2008 ja 2009. ISO/IEC 18045 -standardi on julkaistu vuonna 2008. ISO on julkaissut ISO/IEC 27000 -sarjaan viime vuosina useita uusia tietoturvastandardeja. Uusimmat ISO/IEC 27000 -sarjan standardit ovat (tilanne 21.9.2011):

- ISO/IEC 27005 Tietoturvariskien hallinta (julkaistu 19.5.2011)
- ISO/IEC 27031 Guidelines for information and communication technology readiness for business continuity (julkaistu 1.3.2011)
- ISO/IEC 27003 Tietoturvallisuuden hallintajärjestelmän toteuttamisohjeita (vuodelta 2010)
- ISO/IEC 27000 Tietoturvallisuuden hallintajärjestelmät. Yleiskatsaus ja sanasto (vuodelta 2009)

- ISO/IEC 27004 Tietoturvallisuuden hallinta. Mittaaminen (vuodelta 2009). (Suomen Standardisoimisliitto 2011c; International Organization for Standardization 2011a.)

Keskeisimpiä tietoturvastandardeja ovat pitkään olleet tietoturvan hallintaa käsittelevät standardit ISO/IEC 27002 ja ISO/IEC 27001. ISO/IEC 27002 -standardin uusin päivitetty versio on julkaistu vuonna 2005. Standardi tunnettiin vuoteen 2007 asti ISO/IEC 17799 -standardina. ISO/IEC 27001 -standardin uusin päivitetty versio on julkaistu vuonna 2006. Molempien standardien hankkiminen tulee suositeltavaksi, jos yrityksessä tehdään suuria tietoturvahankkeita. (Hakala ym. 2006: 46; Suomen Standardisoimisliitto 2011a; Suomen Standardisoimisliitto 2007; International Organization for Standardization 2009.)

BS 7799 -standardia on pidetty yhtenä tunnetuimmista tietoturvastandardeista. Se on englantilainen standardi, joka ei ole enää niin merkittävä, koska ISO:n standardien ISO/IEC 27002 ja ISO/IEC 27001 voidaan katsoa korvanneen sen ja tietoturvasertifiointi tehdään niiden pohjalta. (Laaksonen 2006: 85, 88; Suomen Standardisoimisliitto 2007.)

ISO/IEC 27002 -standardi on informaatioteknologiaa, turvallisuutta sekä tietoturvan hallintaa koskeva yleinen menettelyohje. Sen avulla organisaatiossa pystytään kehittämään tehokkaita turvallisuusjohtamisen käytäntöjä sekä lisäämään luottamusta organisaatioiden väliseen liiketoimintaan. Standardi tunnettiin pitkään nimellä ISO/IEC 17799, mutta standardin tunnus muutettiin vuonna 2007. (Hakala ym. 2006: 46; Suomen Standardisoimisliitto 2007; Suomen Standardisoimisliitto 2006.)

ISO/IEC 27002 on keskeisin tietoturvasuunnittelun sisältöä ohjaava standardi. Siinä määritellään yrityksen tietoturvan suunnittelussa, ylläpidossa ja kehittämisessä huomioitavat osa-alueet. ISO 27002/IEC -standardi on luotu BS 7799 -standardin ensimmäisen osan pohjalta. ISO 27002/IEC on suunniteltu kaikenkokoisten yritysten käyttöön ja se huomioi OECD:n tietoturvaohjeistuksen. Se laadittiin ensimmäisen kerran vuonna 1992. Vuoden 2002 päivityksessä siihen lisättiin käsite tietoturvakulttuuri ja vuoden 2005 päivityksessä esiintyi ensimmäisen kerran aiheena tietoturvahäiriöiden hallinta. (Hakala ym. 2006: 46; Laaksonen 2006: 85–86, 88; Suomen Standardisoimisliitto 2007.)

ISO 27002/IEC sisältää yleisperiaatteet ja suuntaviivat tietoturvan hallitsemiselle. Siinä kuvataan turvallisuuden parantamistoimien käynnistämis- ja toteutustapoja. Lisäksi siinä kerrotaan turvallisuushallinnon ylläpito- ja kehitystapoja. Standardi painottuu menetelmiin ja turvallisuuden hallinnointiin. Siinä ei kuvata teknisiä ratkaisuja. Standardi ohjeistaa yrityksen turvallisuuskäytäntöjen ja standardien

laatimisen yleisellä tasolla. Se ei siis sisällä määräyksiä mitä käytäntöjen ja standardien tulisi olla. ISO 27002/IEC -standardi voidaan nähdä työvälineenä, jolla voidaan arvioida yrityksen olemassa olevien tietoturvakäytäntöjen kattavuutta. (Hakala ym. 2006: 47; Suomen Standardisoimisliitto 2007.)

ISO 27002/IEC -standardissa tietoturva jaetaan 11 klausuuliin. Jokaisessa klausuulissa on 1–10 pääkategoriaa. Kussakin kategoriassa on määritelty tavoitteet ja ohjaustoiminnot tavoitteisiin pääsemiseksi. Lisäksi kussakin kategoriassa on kuvattu toteutusohjeet sekä annettu lisätietoja. (Hakala ym. 2006: 47; Suomen Standardisoimisliitto 2007.)

Hakalan ja muiden (2006: 47–48; Suomen Standardisoimisliitto 2007) mukaan ISO 27002/IEC -standardi ohjeistaa seuraavia asioita:

1. **riskianalyysi sekä riskien arviointi ja käsittely:** järjestelmällinen riskien kartoittaminen ja vaikutusten (myös taloudellisten) arviointi: varautuminen, pienentäminen, ehkäisy, siirtäminen ja hyväksyminen
2. **turvallisuuspolitiikka:** määrittely, sisältö ja levittäminen, korostetaan johdon sitoutumista sekä tiedon levittämistä koko yrityksessä ja sen sidosryhmille
3. **tietoturvan organisointi:** sisäinen ja ulkoinen organisointi erikseen, tietoturva sisällytetään yrityksen kaikkiin toimintaprosesseihin, vastuuhenkilöt nimetään, toimintaa koordinoidaan ja tarkastellaan säännöllisesti
4. **omaisuuden hallinta:** omaisuutta on yrityksen arvokas omaisuus, joka voi olla aineellista tai aineetonta, omaisuuden inventointi, omistajan eli vastuuhenkilön nimeäminen, sallitun ja kielletyn käytön määrittely sekä tietojen luokittelujärjestelmän luominen
5. **henkilöstöturvallisuus:** johdon vastuu, työntekijöiden ja sidosryhmien roolien ja vastuiden määrittely, sopimukset, taustaselvitykset, kurinpitotoimet ja työsuhteen päättyminen
6. **fyysinen ja ympäristöturvallisuus:** kulun- ja käytönvalvonnan toteuttaminen, tietojenkäsittelytilojen määrittely ja suojaaminen, laitteistojen ja kaapelointijärjestelmän suojaus, etätyöskentely sekä laitteistojen kierrätys ja hävittäminen
7. **käytön hallinta:** toimintatavat ja vastuut, käytön valvonnan menetelmät, tietojen varmistus, tietoliikenneturvallisuuden hallinta, tiedon välitys yrityksen ja sen sidosryhmien välillä, muutosten hallinta, tehtävien, kehityksen, testauksen ja tuotannon eriyttäminen, ulkoisten palveluiden hallinta, järjestelmien suunnittelu ja hyväksyttäminen, haittaohjelmilta suojautuminen, tietovälineiden käsittely, järjestelmädokumenttien turvallisuus ja sähköinen kauppa

8. **pääsyn valvonta:** pääsynvalvontapolitiikka, pääsynvalvonnan hallinta, järjestelmien käyttäjien vastuut, verkon pääsynvalvonta, käyttöjärjestelmien, varusohjelmien, sovellusten ja tietojen käytön rajoittaminen sekä mobiilikäytön rajoitukset
9. **tietojärjestelmien hankinta, kehittäminen ja ylläpito:** turvallisuusvaatimusten analysointi ja määrittely, eheyden varmistaminen, salaustekniikoiden käyttö, järjestelmätiedostojen turvallisuus, sovelluskehityksen ja tukiprosessien turvallisuus sekä tekninen haavoittuvuuden hallinta
10. **tietoturvatapahtumien hallinta:** tietoturvatapahtumien ja heikkouksien raportointi, ei-toivottujen tapahtumien hallinta ja turvallisuuden parantaminen
11. **toiminnan jatkuvuuden hallinta:** tietoturvan saaminen osaksi yrityksen yleistä jatkuvuuden hallintaa
12. **yhteensopivuus:** yhteensopivuus lainsäädännön ja sopimusten kanssa, standardien mukaisuus, yrityksen käytäntöjen vastaavuus, tekninen yhteensopivuus ja auditointi.

ISO/IEC 27001 -standardi käsittelee informaatioteknologiaa, turvallisuustekniikoita, tietoturvan hallintajärjestelmiä sekä yleiskatsauksen tietoturvastandardeihin ja sanaston. Sen tärkein tavoite on auttaa luomaan ja ylläpitämään jatkuvan parantamisen lähestymistapaa, johon pyritään käyttämällä tehokasta tietoturvan hallintajärjestelmää. (International Organization for Standardization 2009; Suomen Standardisoimisliitto 2006.)

Hakalan ja muiden (2006: 46, 49) mukaan ISO 27001/IEC -standardi kuvaa tietoturvan hallintajärjestelmää, josta käytetään lyhennettä ISMS (Information Security Management System). BS 7799 -standardin toinen osa BS 7799-2 sisälsi aiemmin ISO 27001/IEC -standardin sisällön. ISO 27001/IEC -standardin seuraaminen edellyttää ISO 27002/IEC -standardia. ISO 27001/IEC on sitovampi kuin ISO 27002/IEC. ISO 27001/IEC antaa suuntaviivat tietoturvatoiminnalle. Sen perustana on tietoturvan hallintajärjestelmän kehittäminen prosessinomaisesti. (Hakala ym. 2006: 46, 49; Laaksonen 2006: 88; Suomen Standardisoimisliitto 2007.)

ISO 27001/IEC -standardin klausuulien 4–8 asiat ovat:

4. **tietoturvan hallintajärjestelmä**: perustaminen, käyttöönotto ja käyttö, järjestelmän valvonta ja katselmointi sekä sen ylläpito ja kehittäminen, dokumentointi ja dokumenttien hallinta
5. **johdon vastuut**: sitoutuminen, resurssien varmistaminen, lainsäädännön ja sopimusten vaikutusten arviointi, katselmointien järjestäminen ja sen tu-

loksiin reagointi, turvallisuustietoisuuden edistäminen sekä koulutuksen järjestäminen ja sen tulosten kirjaaminen
6. **sisäinen tietoturvan hallintajärjestelmän auditointi**
7. **johdon katselmointi tietoturvan hallintajärjestelmään**: vaadittavat lähtötiedot ja syntyvät tulokset
8. **tietoturvan hallintajärjestelmän kehittäminen**: jatkuva kehittäminen sekä ehkäisevät ja korjaavat toimenpiteet.

Klausuulit sisältävät kohdat, jotka tulee sisältyä yrityksen tietoturvan hallintajärjestelmään, mikäli se halutaan auditoida ja sertifioida. (Hakala ym. 2006: 49–50.)

4.3 Yritysturvallisuus EK Oy: Käytännön tietoturvallisuusopas pk-yrityksille

Yritysturvallisuus EK Oy on joulukuussa 2005 rekisteröity toiminimi. Yhtiö järjestää yrityksille turvallisuusalan koulutusta sekä valmistaa ja myy turvallisuusalan materiaalia. Lisäksi yhtiö harjoittaa turvallisuusalan konsultointi- ja julkaisutoimintaa. Yritysturvallisuus EK pyrkii yhdessä Yritysturvallisuuden neuvottelukunnan ja Elinkeinoelämän keskusliiton yritysturvallisuustoimiston kanssa parantamaan yritysturvallisuutta koskevan tiedon saatavuutta ja käyttöä sekä lisäämään tietoisuutta turvallisuusasioista. Lisäksi ne pyrkivät edistämään yrityksissä tehtävää turvallisuustyötä. (Yritysturvallisuus EK Oy 2010; Yritysturvallisuus EK Oy 2009b.)

Yritysturvallisuus EK:n www-sivuston tiedotteissa on julkaistu pk-yrityksille tarkoitettu tietoturvaopas *Ovatko yrityksesi tietoriskit hallinnassa? Käytännön tietoturvallisuusopas pk-yrityksille*. Sen on kirjoittanut Elinkeinoelämän Keskusliiton yritysturvallisuustoimiston päällikkö. Oppaan saatetekstissä, joka on kirjoitettu vuonna 2001, todetaan, että tietoturvan vastuut ja vaatimukset kasvavat. Oppaan tarkoitus on ohjeistaa tietoturvakäytäntöjen suunnittelua sekä kertoa tietoturvavastuista, tiedon luokittelusta ja tietoturvan asettamista vaatimuksista sopimusten laatimiselle. Osaaminen ja huoli tietoturvasta ovat suurimpia ongelmia uuden tietotekniikan käyttöönotossa. Yrityksille on erittäin tärkeää ymmärtää, mitä yrityksen tietoa pitää turvata ja miten se tehdään. Reilut puolet (55 %) tietojen menetystapauksista aiheutuu käyttäjän aiheuttamasta inhimillisestä virheestä. Tietoja menetetään myös sisäisen hakkeroinnin ja työntekijän koston seurauksena. Vaikka virukset aiheuttavat saatteen mukaan melko harvoin tietojen menetystä, aiheuttavat ne toteutuessaan tietojärjestelmille yleensä suurimmat kertakustannukset. Kaikki edellä mainitut syyt tietojen menetykselle ovat tavalla tai toisella ihmisen aiheuttamia, minkä yhteenvetona voidaan todeta, että ihminen on säh-

köisten tietojärjestelmien tietojen menetyksen aiheuttajana noin 80 %:ssa tapauksista. Lopuissa, noin joka viidennessä tapauksessa tietoja menetetään fyysisten ongelmien takia. (Yritysturvallisuus EK Oy 2008.)

Oppaan saatteessa todetaan myös, että yritysten ja niiden sidosryhmien välinen verkottunut toimintaympäristö aiheuttaa yrityksien tietoturvalle yhä suurempia vaatimuksia ja vastuita. Yritykset ovatkin usein vastuussa oman tietoturvansa lisäksi myös sidosryhmiensä tietoturvasta. Yritysten keskeiset toiminnot ovat riippuvaisia tiedoista ja tietojärjestelmä, mikä tekee niistä myös haavoittuvaisia. Tiedon, työn ja palvelujen verkottuminen lisää yritysten mahdollisuuksia, mutta vaatii myös niihin liittyvien riskien huomioimista ja hallintaa. Tietoturvasta on tullut merkittävä osa koko yrityksen riskienhallintaa. Tekninen tietoturva on hyvin nopeasti kasvava yrityksen tietoturvan osa. Tietoturvaa ei kuitenkaan pystytä ratkaisemaan pelkästään teknisellä tietoturvalla. Merkittävässä roolissa ovat myös käyttäjien toiminta ja turvallisuustietoisuus sekä käyttäjien tietojen hallinta. (Yritysturvallisuus EK Oy 2008.)

Ovatko yrityksesi tietoriskit hallinnassa? Käytännön tietoturvallisuusopas pk-yrityksille -oppaassa todetaan, että tietoturvalla on merkittävä rooli määriteltäessä yrityksen laatua ja luotettavuutta. Oppaassa käsitellään aluksi tietoturvan merkitystä yritystoiminnalle sekä pohditaan mitä tietoturva on. Oppaassa käsitellään myös lain asettamia vaatimuksia tietoturvalle. Sen jälkeen yrityksen yleistä tietoturvaa käsittelevässä luvussa pohditaan tietoturvan laatua, yrityksen tietoturvaperiaatteita ja -politiikkaa, tietoturvaohjelmaa, tietoturvavastuita, tietoaineiston luokittelua, työntekijöiden tietoturvaa, kulunvalvontaa ja vierailuja sekä työ- ja liikematkoja. Seuraavaksi otetaan esille tietotekniseen turvallisuuteen liittyen Internet ja sähköposti sekä tiedon käyttö- ja hallintalaitteiden turvallisuus. Oppaan viimeisessä luvussa kerrotaan tietoturvamenettelyn soveltamisesta yritystoimintaan. (Yritysturvallisuus EK Oy 2001: 6.)

4.4 TIEKE Tietoyhteiskunnan kehittämiskeskus ry: Tietoturvaopas

TIEKE Tietoyhteiskunnan kehittämiskeskus ry (myöh. TIEKE) on riippumaton yhdistys, joka pyrkii kehittämään suomalaista tietoyhteiskuntaa käynnistämällä ja toteuttamalla erilaisia kehittämishankkeita elinkeinoelämän ja kansalaisten parhaaksi. TIEKEn tavoitteena on tunnistaa tietoyhteiskunnan kehittämisen hidasteita ja kohteita. Toiminnalle ominaista on vahva jäsentoiminta, menestyvät olemassa olevat palvelut ja niiden kehittäminen, lisäarvon tuottaminen sekä asiakas- ja

sidosryhmien hyvän tyytyväisyystason säilyttäminen. (TIEKE Tietoyhteiskunnan kehittämiskeskus ry.)

TIEKEn (2004k) mukaan tietoturvan tavoitteena on tila, jossa tietojen kerääminen, käsittely ja siirtäminen tehdään nykyaikaisella tekniikalla siten, että tiedot säilyvät ja pysyvät oikeina ja ovat käytettävissä silloin, kun niitä tarvitaan. Tiedot tulee olla kuitenkin vain niihin oikeutettujen saatavilla. Erityisesti päätöksentekoon ja erilaisten järjestelmien toiminnan ohjaamiseen käytettävien tietojen kohdalla tietoturvasta huolehtiminen on tärkeää.

TIEKEn (2004a) sivustolta löytyy tietoturvaopas. Sen kohderyhmänä on erityisesti ihminen tietokoneen peruskäyttäjänä. Otsikolla *Tietoturvaopas, Tietoturvaa peruskäyttäjälle* kirjoitettu ohjeisto löytyy TIEKEn sivustolta Oppaat yrityksille -linkin takaa. Sivustolta löytyy myös Oppaat kansalaisille -linkki, joten tietoturvaoppaan voidaan katsoa suunnatun enemmän yrityksille kuin tavallisille kansalaisille. Tietoturvaoppaassa on tietoturvaa käsitelty valtionhallinnon tietoturvasanaston määritelmien mukaisesti. Oppaan etusivulla todetaan, että opas on tarkoitettu yleisluonteisesti korostamaan tärkeimpiä perusasioista ja antamaan joitakin käytännöllisiä neuvoja – ei käsittelemään tietoturvaa kaikenkattavasti. Eri yrityksissä ja tilanteissa on erityisiä tietoturva-asioita, joita on painotettava. Yrityskohtaisten ohjeiden tunteminen ja noudattaminen on erittäin keskeistä. Tietoturvaopasta on viimeksi päivitetty tammikuussa 2004. (TIEKE 2004a; TIEKE 2004m.)

Tietoturvaoppaan johdannossa on laadittu niin sanottu tietoturvan huoneentaulu, joka on tarkoitettu tietoturvan muistilistaksi. Siihen on otettu mukaan 8 kohtaa, jotka muodostavat myös varsinaisen oppaan rungon. Muistilistan ja oppaan sisältönä on:

1. *”Selvitä tiedon ja tiedoston alkuperä ennen käyttöä.*
2. *Muista, että seinillä on korvat – useammat kuin arvaatkaan.*
3. *Lukitse ovesi ja tietokoneesi, kun lähdet muualle.*
4. *Käytä salasanoja, joissa on muitakin merkkejä kuin kirjaimia, ja pidä ne salassa.*
5. *Älä hätäile, äläkä varsinkaan toimi hätiköidysti.*
6. *Ota talteen kaikki tarpeellinen, ennen kuin vahinko sattuu.*
7. *Käytä ajantasaisia viruksentorjuntaohjelmia ja muita turvajärjestelyjä.*
8. *Selvitä itsellesi oman organisaatiosi tietoturvajärjestelyt.”* (TIEKE 2004b.)

Tietoturvaoppaan johdannossa perustellaan miksi panostus tietoturvaan kannattaa. Perusteluissa todetaan, että tietokoneet ja tietoliikenne ovat tällä hetkellä monen asian taustalla. Tietoturvalla tarkoitetaan tietojen, tietojärjestelmien ja tietoliikenteen suojaamista erilaisilta uhkilta. Tietoturvaa uhkaavat esimerkiksi turmeltumi-

nen, luvaton käyttö, häirintä ja urkinta. Tietoturvan merkitys korostuu yrityksissä, koska tietojenkäsittelyllä on niiden toiminnassa keskeinen rooli. Tietokoneiden käyttö on tuonut yrityksille suuria etuja. Toisaalta vakavat häiriöt tietojenkäsittelyssä aiheuttavat yrityksille isoja ongelmia. Yritystiedot sisältävät usein liikesalaisuuksia. Yritykset ovat lailla velvoitettuja turvaamaan myös ihmisten yksityisyyden. Yrityksissä käsiteltävät tiedot tulee olla luotettavasti saatavilla. Ne eivät kuitenkaan saa olla kenen tahansa saatavilla. (TIEKE 2004c.)

Tietoturvan uhat eivät ole itsestään selviä. Käytännön toiminnassa tietoturvan tärkeyttä ei tunneta tai oteta huomioon. Julkisten laitosten tietojen salaamisessa on erilainen intressi kuin yritysten tietojen salaamisessa. Kaikilla tahoilla on kuitenkin jotakin tietoa, joka on pidettävä salassa. Jokaisella on paljon säilytettävää ja asiattomalta muuttamiselta suojattavaa tietoa. Tiedon turvaamistaso tulee miettiä erikseen kuhunkin tilanteeseen sopivaksi. Suhteellisuudentaju on tarpeen myös siksi, että tietoturvajärjestelyt vaativat aina lisätyötä ja rajoituksia. Valitettavasti tietoturvajärjestelyt joskus myös vaikeuttavat tietokoneiden ja tietoliikenteen asiallista käyttöä. Täydellistä tietoturvaa on mahdotonta saavuttaa, mutta kuhunkin tilanteeseen sopiva järkevä tietojen turvaamisen taso on mahdollista löytää. (TIEKE 2004c.)

Yrityksissä äärimmäisen tärkeitä tietoturva-asioita hoitavat aihealueen asiantuntijat. Tavallisella käyttäjällä on kuitenkin erittäin tärkeä rooli tietoturvan toteutumisessa. Asiantuntijoiden antamien toimintaohjeiden ymmärtäminen ja noudattaminen vaatii tavalliseltakin käyttäjältä tietoturvan perustietämystä. Esimerkiksi tärkeiden tiedostojen varmuuskopioiminen keskitetysti asiantuntijoiden toimesta ei onnistu, mikäli käyttäjä on tallentanut tiedostonsa väärään paikkaan. Asiantuntijat eivät myöskään pysty korjaamaan tietoturvassa ilmenneitä ongelmia, mikäli käyttäjät eivät sellaisen huomatessaan kerro heille asiasta. Käyttäjille annettava yleistieto tietoturvasta ja sen ongelmista auttaa käyttäjää tunnistamaan epäilyttävät tilanteet ja kertomaan niistä asiantuntijoille. (TIEKE 2004c.)

Tietoturva on kokonaisvaltaista. Yhden osan turvattomuudella voi olla laaja vaikutus. Koko perheen käyttöön ostetulta kotitietokoneelta voi olla yhteys työpaikan tietojärjestelmään, jolloin, jos tietoturva ei ole kotikoneessa kunnossa, luodaan aukko yrityksen tietoturvamuuriin. Tavallista kotikonetta saatetaan käyttää apuvälineenä myös yleiseen tietorikollisuuteen. Näiden esimerkkien takia tietoturvan minimitaso on kaikille tarpeen. Kaikki tietokoneet ja tietojärjestelmät on syytä suojata ja varmistaa. Kaikkien tietokoneiden kovalevy voi lakata toimimasta ja tällöin, jos varmuuskopiota ei ole, on tiedot auttamattomasti menetetty. Tietoturvan minimitason saavuttaminen toteutuu melko pienillä järjestelyillä. Suuren luotettavuuden saavuttaminen vaatii enemmän työtä. Mitä suurempaan tietoturvan

tasoon pyritään, sitä enemmän asiaan täytyy paneutua ja siihen kuluu myös rahaa. Tämän takia tulee tavoitella sopivaa tietoturvatasoa, jossa panostus tietoturvaan on järkevässä suhteessa saavutettavaan hyötyyn. (TIEKE 2004c.)

Tietoturvan panostamisen perusteluissa otetaan esille, että suuri osa tietoturvaan kohdistuvista uhkista aiheutuu käyttäjistä. Tietoturvaa varten ostettavat palvelut, ohjelmat ja laitteet sekä monipuoliset tietoturvapaketit parantavat tietoturvaa ja ovat hyödyllisiä, mutta tietoturva ei tule ikinä kuntoon pelkästään niillä. Yritykset tarvitsevat lisäksi omaa tietoisuutta ja valmiuksia tietoturvan saavuttamiseksi. Tekniset tietoturvatoimet menettävät merkityksensä, jos ulkopuolinen saa esimerkiksi salasanan tietoon yksinkertaisella puhelinsoitolla. (TIEKE 2004c.)

Tietoturvaoppaan ensimmäisessä osassa, *1. Selvitä tiedon ja tiedoston alkuperä ennen käyttöä,* käsitellään liitetiedostoja, tiedon levittämistä ja tiedon sisällön uskomista, roskapostin tunnistamista, sinisilmäisyyden vaaroja, Internetin haitta-ohjelmia, ohjelman salakavaluutta, selainten ongelmia, lomakkeen tietojen lähettämistä sekä Internet-sivujen ja -kumppaneiden totuudenmukaisuutta ja aitoutta. Tietoturvaoppaan toisessa osassa, *2. Muista, että seinillä on korvat – useammat kuin arvaatkaan,* muistutetaan, että kuuntelemisen lisäksi yrityksesi tietoihin päästään käsiksi roskakorivakoiluna, verkkokaapeleita pitkin sekä sähköpostin, etäyhteyden ja modeemin kautta. Kohdassa tuodaan esille, että yhteiset tiedostot ovat joustavia, mutta myös riski. Lisäksi kohdassa käsitellään salakirjoittamisen vaatimuksia ja vaihtoehtoja sekä omalle kotikoneelle asennetun Internet-palvelimen tietoturvariskejä. (TIEKE 2004d; TIEKE 2004e.)

Kunkin käyttäjätunnuksilla tehdyistä asioista on vastuussa aina käyttäjä. Tietoturvaoppaan kolmannessa osassa, *3. Lukitse ovesi ja tietokoneesi, kun lähdet muualle,* nostetaan esille, että tietokone on hyvä sulkea tai vähintäänkin lukita aina, kun poistuu edes pieneksi hetkeksi koneen äärestä. Yhteiskäyttöisillä yleisillä tietokoneilla, esimerkiksi kirjastossa, tämä on erityinen riski. Salasanalla suojatun joutonäytön käyttäminen suojaa tietokoneen tietoja. Joutonäyttö voidaan määritellä käynnistymään myös automaattisesti tietyn käyttämättä oloajan jälkeen. Ohjelmat on hyvä sulkea ja palveluista poistua aina, kun niitä ei enää tarvitse. Kun tietokoneelta kirjaudutaan kokonaan ulos, on siihen varattava aikaa ja on tärkeää odottaa, että kone varmasti kirjautuu ulos. Tyhjänä oleviin työhuoneisiin ei saa päästää ulkopuolisia henkilöitä, esimerkiksi roskakorivakoilun takia. Eikä ulkopuolisia pidä jättää työhuoneisiin hetkeksikään yksin. Lisäksi on hyvä muistaa, että lukot eivät ole varkaita vaan rehellisiä ihmisiä varten. Kolmannen osan lopussa esitellään kannettavaan tietokoneeseen liittyviä fyysisiä tietoturvauhkia, kuten unohtaminen, varkaus ja rikkoutuminen. Uhkiin voi varautua esimerkiksi salakirjoitta-

malla tiedostot, sekä ottamalla heti varmuuskopiot erilliseen laitteeseen ja säilyttämällä sitä eri paikassa tietokoneen kanssa. (TIEKE 2004f.)

Tietoturvaoppaan neljännessä osassa, *4. Käytä salasanoja, joissa on muitakin merkkejä kuin kirjaimia, ja pidä ne salassa,* neuvotaan heti alussa ytimekkäästi, että salasanan täytyy olla salainen ja se ei saa olla mikään sana, lyhenne tai mitään luonnollista. Luonnollinen salasana on helppo muistaa, mutta myös helppo arvata. Se löytyy helposti myös järjestelmällisillä murtomenetelmillä. Salasanan tulee oikeammin kuvattuna olla koodimainen salakoodi sisältäen sekaisin numeroita, isoja ja pieniä kirjaimia ja erikoismerkkejä. Sivulla kerrotaan aluksi mistä salasanassa on kyse: salasanaa käytetään suojaamaan esimerkiksi tietokoneita, ohjelmia ja palveluita ja se on merkkijono, joka on vain kyseisen luvallisen käyttäjän tiedossa. Mikäli käyttöluvan saamisen yhteydessä annettu salasana kehotetaan itse vaihtamaan, on vaihtaminen erittäin tärkeää. Salasanalle annetaan usein teknisesti laatuvaatimukset, esimerkiksi salasanan tulee olla vähintään 8 merkkiä pitkä. Eri kohteissa tulee käyttää eri salasanaa. Salasana on käytännössä ainoa este luvallisen ja luvattoman käytön välillä. Salasana liittyy käyttäjätunnukseen, jolle myönnetään tietyt käyttöoikeudet. Käyttäjätunnuksella ja salasanalla kirjaudutaan käyttämään kohdetta. Käytön lopuksi on tietoturvan kannalta erityisen tärkeää kirjautua myös ulos kohteesta. Salasanan syöttämistä ei koskaan pidä tehdä toisten nähden. Syöttäessäsi salasanaa varmista, että olet todella kirjautumassa oikeaan järjestelmään. Salasana on vaihdettava säännöllisesti muutaman kuukauden välein yrityksen ohjeiden mukaan. Salasanaa ei tule milloinkaan luovuttaa toisen käyttöön. (TIEKE 2004g.)

Tietoturvaoppaan viidennessä osassa, *5. Älä hätäile, äläkä varsinkaan toimi hätiköidysti,* neuvotaan huolestumaan kummallisuuksista, mutta ei hätääntymään niistä. Tällaisia ovat esimerkiksi tiedoston muuttuminen, uusien tiedostojen ilmestyminen ja levytilan katoaminen. Hätäilyn seurauksena tietomurron jäljet saattavat hävitä, vioittunut tiedosto saatetaan tuhota lopullisesti tai saatetaan avata uusia aukkoja turvallisuuteen. Tietoturvaongelmatilanteissa ota yhteys asiantuntijaan, ja selvitä rauhallisesti mistä on kyse. Hyödynnä ohjeita ja käsikirjoja. Ongelman selvittämistä myöhemmin helpottaa, kun kirjoitat muistiin mitä teit ja mitä tapahtui. Kirjoita sanatarkasti ylös myös järjestelmän antamat ilmoitukset. Rauhallisena pysymiseen auttaa, kun tietää perustiedot tietotekniikasta. Viidennen osan lopussa varoitetaan vääristä varoituksista ja huijauksesta. Tällaisia ovat esimerkiksi väärät virusvaroitukset. (TIEKE 2004h.)

Seuraavassa osassa, *6. Ota talteen kaikki tarpeellinen, ennen kuin vahinko sattuu,* käsitellään tietojen tallentamista ja varmistamista. Tallentamalla pyritään varautumaan ongelmiin, jotka aiheutuvat esimerkiksi sähkökatkoksesta, järjestelmävir-

heestä tai verkkoyhteyden katkeamisesta. Tietokoneella työtä tehtäessä neuvotaan meneillään oleva työ tallentamaan aika-ajoin kovalevylle. Varmistamisella huolehditaan, että työn tulokset säilyvät, vaikka kovalevy lakkaisi toimimasta tai tiedosto vahingossa hävitettäisiin tai poistettaisiin. Varmuuskopioinnilla pyritään varautumaan myös tietomurtojen ja haittaohjelmien aiheuttamiin muutoksiin tiedostojen sisällössä tai niiden katoamisessa kokonaan. Aineiston varmuuskopiointi voidaan tehdä esimerkiksi muistitikulle, CD-levylle, ulkoiselle kovalevylle tai palvelimelle. Tärkeistä tiedoista tulisi olla kaksi toisistaan riippumatonta varmuuskopiota ja erittäin tärkeistä tiedoista kolme kopiota, joista ainakin yksi fyysisesti turvallisessa paikassa, eri rakennuksessa. Myös varmuuskopioista tulee huolehtia. Niiden hävittäminen tai päällekirjoittaminen vahingossa tulee estää. Tietoturvaoppaassa neuvotaan laatimaan oma varmuuskopiointisuunnitelma. Suunnitelmaa laadittaessa tulee aluksi selvittää yrityksen yleinen automaattinen varmuuskopiointi. Sen jälkeen tulee suunnitella laajan varmuuskopioinnin sekä erityisen tärkeiden ja usein muuttuvien tietojen varmuuskopioinnin aikataulutus. Suunnitelmaa laadittaessa on hyvä muistaa myös tietokoneen varastamisen tai tulipalossa vaurioitumisen mahdollisuus. (TIEKE 2004i.)

Tietoturvaoppaan seitsemännessä osassa, *7. Käytä ajantasaisia viruksentorjuntaohjelmia ja muita turvajärjestelyjä,* käsitellään virusten torjunnan käytäntöä, haittaohjelmia sekä palomuuria ja roskapostin suodatusta. Virusten torjunta on melko helppoa ja vaivatonta, koska siihen on saatavilla viruksentorjuntaohjelmia. Ne tehoavat monenlaisiin viruksiin ja haittaohjelmiin, mutta mikään ohjelma ei tehoa niihin kaikkiin. Torjuntaohjelmat käyttävät virustietokantoja. Viruksia tulee koko ajan lisää, minkä takia myös tietokannat muuttuvat. Siksi ohjelman asentaminen (sisältäen sen hetkisen virustietokannan) kerran ei riitä, vaan virustietokantaa tulee päivittää jatkuvasti. Kuitenkin, vaikka torjuntaohjelmien käyttö on siis välttämätöntä, ei päivityksistäkään huolimatta pelkästään torjuntaohjelman käyttö riitä varmistamaan, että taistelu viruksia ja haittaohjelmia vastaan on hallinnassa. Huomioitavaa on, että haittaohjelman kaltainen vahinkoa tai harmia aiheuttava ohjelma voidaan koodata tahattomasti myös vahingossa. Tietoturvaoppaassa neuvotaan ilmoittamaan yrityksen tietoturvahenkilölle, mikäli viruksentorjuntaohjelma ilmoittaa järjestelmässä olevasta ongelmasta. Viruksesta tulisi ilmoittaa myös taholle, jolta virus on tullut, mikäli sellainen on osoitettavissa. Virusten kanssa neuvotaan erityisesti pysymään rauhallisena. Yrityksissä on tärkeää selvittää viruksentorjunnan periaatteet ja käytänteet. Ne olisi hyvä olla kirjattuna täsmälliseksi toimintaohjeeksi. Tietoturvaoppaan tässä osassa käsitellään vielä palomuuria, jonka kerrotaan olevan järjestelmä, jolla turvataan ja valvotaan Internetin ja oman tietokoneen tai lähiverkon välistä yhteyttä. Lopuksi kerrotaan roskapostin suodatuksesta. Vaikka roskaposti ei ole varsinainen tietoturvaongelma, voi vääränlaiset yritykset torjua roskapostia aiheuttaa tietoturvauhkia. Roskapostikin

saattaa sisältää viruksia. Yrityksissä roskapostia vastaan on yleensä käytössä yleinen suodatus. (TIEKE 2004j.)

Tietoturvaoppaan viimeisessä osassa, *8. Selvitä itsellesi oman organisaatiosi tietoturvajärjestelyt,* tuodaan esille, että osa yrityksen tietoturvajärjestelyistä saattaa virallisesti velvoittaa käyttäjää esimerkiksi tehdyn työsopimuksen perusteella. Tietoturvaoppaassa neuvotaan yrityksen työntekijää selvittämään ainakin seuraavat tietoturva-asiat:

1. Kuka on lähin tietoturvahenkilö, johon otat yhteyden tietoturvaongelmissa?
2. Millainen salasana käy ja kuinka usein se on vaihdettava?
3. Minkä ohjelmien käyttö on pakollista ja millä tavoin (esimerkiksi viruksentorjunta- ja salakirjoitusohjelmat)?
4. Mitä ohjelmia ei saa käyttää?
5. Millaisia asetuksia ohjelmissa on käytettävä?
6. Mihin tarkoituksiin tietokonetta saa käyttää?
7. Mitä tiedostomuotoja saa käyttää sähköpostissa?
8. Millaisia säännöllisiä tarkistuksia ja muita tietoturvatoimia käyttäjän on tehtävä (esimerkiksi varmuuskopiointien tarkistukset)?
9. Minne tiedostot on tallennettava?
10. Onko yritys järjestänyt yleisen varmuuskopioinnin ja miten se on järjestetty? (TIEKE 2004k.)

Tietoturvajärjestelyjen luonne ja yksityiskohtaisuus voi vaihdella eri yrityksissä paljon. Yrityksen tietoturvajärjestelyt tulisi kertoa heti uudelle työntekijälle. Tähän tarkoitukseen voidaan laatia tietoturvapolitiikka ohjeineen. Julkisesti ulkopuolisille esitetyt yrityksen tietoturvajärjestelyt voivat poiketa esimerkiksi suppeudellaan huomattavasti siitä, mitä yrityksen työntekijöille kerrotaan yrityksen sisällä. Tavallisen käyttäjän ei tulisikaan kertoa ulkopuolisille mitään yrityksen tietoturva-asioista. Oppaassa huomioidaan, että tietoturvaohjeiden noudattaminen on tärkeää silloinkin, vaikka niiden perusteita ei ymmärtäisi. Ohjeiden taustalla on yleensä tekniset perusteet. Niin kutsuttujen paikallisten tietoturvaohjeiden tarkoitus on kertoa paikalliset erityisjärjestelyt täydentämään tietoturvan yleisiä perusteita ja korostaa yrityksen paikallista tilannetta. Oppaassa neuvotaan myös laatimaan oma tietoturvapolitiikka, minkä tarkoituksena on saada käyttäjä miettimään yrityksen tietoturvaohjeiden vähimmäisturvan noudattamista ja toteuttamista omassa toiminnassa. Lisäksi tällä pyritään löytämään mahdolliset lisätietoturvajärjestelyt, jotka oma toiminta vaatii. Politiikkaa laadittaessa tulisi pohtia hyväksyttävät riskit. Tietokoneen yhteiskäyttötilanteissa kunkin käyttäjän tiedot kannattaa suojata muilta käyttäjiltä esimerkiksi vahinkojen varalta. Tietoturvaoppaan lopuksi todetaan, että tietoturvaan tarvitaan useita järjestelyjä, tekniikoita ja ihmi-

siä. Tietoturvassa ketjun heikoin lenkki on usein tavallinen käyttäjä, joka ei tiedä mitä pitäisi tehdä. Merkittävin parannus yrityksen tietoturvaan saadaan, kun tavallinen käyttäjä huolehtii tietoturvasta omalta osaltaan ja parhaimmassa tapauksessa auttaa vielä työkaveriaankin asiassa. (TIEKE 2004k.)

Tietoturvaoppaan etusivulla on otettu esille vielä palvelinten asentamisessa tarvittava ohjeistus sekä pohdittu miksi viruksia ja muita tietoturvaongelmia on. Virusten ja muiden tietoturvaongelmien olemassa oloon mainitaan useita syitä. Suuri osa esimerkiksi tietokoneviruksista ja tietomurroista tehdään usein nuoruuden poikamaisena kujeiluna. Monet tietokoneharrastajat kokevat haastavana murtautua tietoturvajärjestelyn läpi tai tehdä taidokas virus. Tilanteeseen liittyy usein myös näyttämisen halu, jolloin esimerkiksi tietomurrossa jätetään murtautumisesta tahallaan jälki, jotta se huomattaisiin. Tietoturvaongelmien taustalta saattaa löytyä myös turhautuneisuus. Tietokonealan osaajalla ei ole kunnollisia töitä tai hän aiheuttaa tietoturvaongelman kostaakseen kokemansa vääryyden. Lopputuloksena saattaa olla, että aiheutetaan paljon suurempaa vahinkoa kuin oli alun perin tarkoitus. Aiheutettua vahinkoa ei lievennä nuoruuden ajattelemattomuus tai tietojen puutteellisuus. (TIEKE 2004a; TIEKE 2004l.)

Monet tietoturvaongelmat ovat riippumattomia ihmisten tahdosta. Fyysisen uhkan toteutuminen esimerkiksi kovalevyn rikkoutumisena ei riipu kenenkään tahdosta. Tietokoneohjelmien ja -järjestelmien monimutkaistuminen aiheuttaa myös tietoturvauhkia. Ohjelma saattaa tehdä tuhoja silloinkin, vaikka kukaan ei sitä suoranaisesti toivoisi. Ohjelmavirheiden seuraukset saattavatkin olla yhtä vakavia kuin tahallisesti tehtyjen haittaohjelmien seuraukset. (TIEKE 2004l.)

Tietotekniikkaa käytetään myös todellisen rikollisuuden, terrorin ja sodankäynnin välineenä. Laajamittaiset sotilasoperaatiot aloitetaan nykyisin lamauttamalla vihollisen tietoliikenne ja tietojenkäsittely kokonaan tai ainakin häiritsemällä sitä, mikäli se vain on mahdollista. Vihollisen tietoliikenneverkko saatetaan myös pyrkiä ottamaan omaan käyttöön tai siihen saatetaan syöttää väärää tietoa. Eriasteista häirintää tietoturvassa saatetaan pyrkiä tekemään julkisuuden saavuttamiseksi jollekin asialle, vastustajan hermostuttamiseksi tai jonkin muun laajemman tavoitteen saavuttamiseksi. Iso osa tietoturvahyökkäyksistä on tunnusteluhyökkäyksiä. Niillä selvitetään järjestelmän heikkoja kohtia myöhemmin aiheutettavaan vahinkoon pyrittäessä. (TIEKE 2004l.)

4.5 Arjen tietoyhteiskunnan tietoturvallisuus -ryhmä: Kansallinen tietoturvastrategia

Liikenne- ja viestintäministeriö ylläpitää Arjen tietoyhteiskunnan neuvottelukuntaa, jonka tavoitteena on tehdä Suomesta kilpailukykyinen ja ihmisläheinen tietoyhteiskunta (Liikenne- ja viestintäministeriö 2010b). Neuvottelukunnan alaisuudessa toimi Arjen tietoyhteiskunnan tietoturvallisuus -ryhmä, jonka toimintakausi oli 1.9.2007–28.2.2011. Ryhmä pohti tietoturvaan liittyviä nykyisiä ja tulevia kysymyksiä. Tietoturvaa käsittelevät kysymykset ovat laajoja ja koskevat useita sektoreita. Ryhmän tehtävänä oli luoda uusi kansallinen tietoturvastrategia ja koordinoida sen toimeenpanoa. Ryhmän tehtävänä oli myös tuoda esille kiistanalaisia näkökulmia, minkä takia se osallistui aktiivisesti julkiseen tietoturvakeskusteluun. Ryhmän keskeisenä tavoitteena oli vahvistaa yritysten ja ihmisten luottamusta tietoyhteiskuntaan, jossa tärkeitä ovat laadukkaat palvelut, jotka toimivat teknisesti hyvin ja ovat turvallisia. Tietoturvaongelmat ja rikollisuus ovat uhka koko yhteiskunnan toiminnalle. Ryhmä seurasi tietoturvan kehittymistä ja pyrki parantamaan sitä tekemällä aloitteita. (Liikenne- ja viestintäministeriö 2010c.)

Uusi Valtioneuvoston periaatepäätös kansallisesta tietoturvastrategiasta hyväksyttiin 4.12.2008. Strategia nimettiin *Turvallinen arki tietoyhteiskunnassa – Ei tuurilla vaan taidolla*. Sen tavoitteena on tehdä suomalaisten yritysten ja ihmisten arjesta tietoyhteiskunnassa turvallinen. Tietoturvastrategian visioksi on kirjattu yritysten ja ihmisten kyky voida luottaa tietojen turvallisuuteen tieto- ja viestintäverkoissa ja niissä tarjottavissa palveluissa. Yleisellä tietoturvaosaamisella halutaan saavuttaa korkea taso ja tietoturvan edistäminen halutaan nähdä saumattomana yhteistyönä eri yhteiskunnan tahojen välillä. Strategiassa Suomi nähdään tietoturvan edelläkävijämaana maailmassa vuonna 2015. Strategiassa on kolme painopistealuetta, jotka ovat ”*perustaidot arjen tietoyhteiskunnassa, tietoihin liittyvien riskien hallinta ja toimintavarmuus sekä kilpailukyky ja kansainvälinen verkostoyhteistyö”*. Edellinen vastaava tietoturvastrategia hyväksyttiin vuonna 2003. (Liikenne- ja viestintäministeriö 2010c; Liikenne- ja viestintäministeriö 2008.)

Painopiste 1 – Perustaidot arjen tietoyhteiskunnassa -tavoitteesta valtioneuvosto toteaa, että jokaisen tietoyhteiskunnan toimijan teot vaikuttavat tietoturvaan. Siksi kaikilla pitäisi olla riittävät perustiedot ja -taidot tietoturvasta ja jokaisen tulisi ymmärtää omat vastuunsa, oikeutensa ja velvollisuutensa tietoyhteiskunnan palveluiden käyttäjinä ja tuottajina. Käyttäjien tulisi tunnistaa ja tiedostaa turvallinen ja luotettava palvelu. Turvallinen verkon käyttö edellyttää sähköisen asioinnin kansalaistaitoja ja verkkolukutaitoa. Myös riskien ennakointi ja tunnistaminen

sekä niihin varautuminen on tärkeää. Palvelun tarjoajan täytyy huolehtia luottamuksellisten tietojen tunnistamisesta ja suojaamisesta sekä varmistaa ja ylläpitää palvelujen turvallinen käyttäminen. Luottamus palvelun tietoturvasta saavutetaan avoimella ja selkeällä viestinnällä, joka sisältää myös mahdollisten riskien kertomisen. Tietoturvan tulee olla kiinteä osa tietoyhteiskunnan perusrakenteita, mihin päästään yleisen tietoturvatietoisuuden ja -osaamisen vahvistamisella sekä tietoturvanäkökohtien huomioimisella järjestelmähankinnoissa ja sopimusprosesseissa. (Liikenne- ja viestintäministeriö 2008.)

Painopiste 2 – Tietoihin liittyvien riskien hallinta ja toimintavarmuus -tavoitteeseen liittyvät keskeisesti sähköiset palvelut ja asiointi, ja siten myös tietotekniikka. Palvelun käyttö ja luottamuksellisten tietojen turvallisuus täytyy tapahtua luotettavasti ja tietoturvallisesti. Palvelun ulkoistaminen ja hankintojen ketjuttaminen edellyttävät tietoturvan kokonaisvaltaista hallintaa ja erityisesti tietojen luottamuksellisuus, eheys ja käytettävyys ovat oleellisia. Yritysten toiminnan jatkuvuus ja palveluiden saatavuus on varmistettava sekä normaali- että poikkeusoloissa. (Liikenne- ja viestintäministeriö 2008.)

Painopiste 3 – Kilpailukyky ja kansainvälinen verkostoyhteistyö -tavoitteen mukaan kilpailukykyinen tietoyhteiskunta edellyttää, että keskeinen tietopääoma on suojattu. Kansallista kilpailukykyä lisää kansallisen lainsäädännön selkeys ja liiketoiminnan esteiden poistaminen. Siksi kansallinen sääntely tulisi olla yritysten kannalta mahdollisimman yksinkertaista ja sen kehityksen tulisi edetä ennustettavasti. Suomen tulisi osaltaan pyrkiä vaikuttamaan myös kansainväliseen sääntelyyn. Strategian mukaan suurin osa tietoturvauhkista ja -hyökkäyksistä tehdään Suomen rajojen ulkopuolelta. Niiden torjumiseen tulee varautua ennakoivasti ja kattavasti ja resurssit tulee kohdistaa tietoturvan keskeisiin kysymyksiin. Tämä edellyttää kansainvälisiä yhteistyöverkostoja sekä kansallista yhteistyötä ja etukäteisvaikuttamista. (Liikenne- ja viestintäministeriö 2008.)

Kansallisen tietoturvastrategian toteuttamiseksi suunnittelut toimenpiteet hyväksyttiin 18.11.2009. Toimenpideohjelma käsitti yhdeksän hanketta, jotka oli jaettu neljään ryhmään: Perustaidot arjen tietoyhteiskunnassa, Tietoihin liittyvien riskien hallinta ja toimintavarmuus, Kilpailukyky ja kansainvälinen verkostoyhteistyö sekä muut hankkeet. Hankkeet olivat:

”Hanke 1. Tietoturvatietoisuuden lisääminen
Hanke 2. Palveluntarjoajan vastuut, oikeudet ja velvollisuudet
Hanke 3. Tietoihin liittyvien riskien tunnistaminen ja tietojen suojaamiseen liittyvien vaatimusten tunnistaminen
Hanke 4. Yritysten toiminnan jatkuvuuden ja kansalaisten palveluiden saatavuuden varmistaminen

Hanke 5. Suomalaisen tietoturvaosaamisen levittäminen ja aktiivinen osallistuminen standardien kansainväliseen kehittämistyöhön
Hanke 6. Yritysten kilpailukyky ja NCSA
Hanke 7. Kansallisen yhteistyön tehostaminen ja aktivointi kansainvälisissä tietoturva-asioissa
Hanke 8. Tutkimushanke lähitulevaisuuden tietoturvatrendeistä
Hanke 9. Tietoturvallisuuden mittaaminen."

Viimeisin hanke päättyi 28.2.2011. (Liikenne- ja viestintäministeriö 2010c.)

4.6 Elinkeinoelämän keskusliitto EK, sisäasiainministeriö ja puolustusministeriö: Kansallinen turvallisuusauditointikriteeristö (KATAKRI)

Elinkeinoelämän keskusliitto EK, sisäasiainministeriö ja puolustusministeriö (2009: 1–2) julkaisivat 20.11.2009 *Kansallinen turvallisuusauditointikriteeristö (KATAKRI)* -julkaisun yritysten turvallisuuden ohjaamiseen ja kehittämiseen. Koska tietoturva on yritysturvallisuuden osa, Kansallinen turvallisuusauditointikriteeristö luo kriteerejä myös tietoturvalle. Kriteeristön kolme muuta pääosaa ovat hallinnollinen turvallisuus (turvallisuusjohtaminen), henkilöstöturvallisuus ja fyysinen turvallisuus. Kriteeristö sisältää yritysturvallisuuden suositukset ja vaatimukset. Suositukset ovat vaatimukselle asetettavia lähtötason suosituksia. Vaatimusluokittelu on tehty vastaamaan turvallisuustasokäsitettä kolmiportaiseksi – perustaso, korotettu taso ja korkea taso. Tietoturvan käsittely on jaettu 7 osioon tietoturvan yleisen jaottelun mukaisesti: hallinnollinen tietoturva ja fyysinen turvallisuus sekä henkilöstö-, tietoliikenne-, tietojärjestelmä- tietoaineisto- ja käyttöturvallisuus. Tietojärjestelmäturvallisuus käsittää ohjelmisto- ja laitteistoturvallisuuden.

Hallinnollisen tietoturvan vaatimuksia lähestytään 10 pääkysymyksellä:
"Onko organisaation tietoturvallisuudella johdon tuki?"
"Onko yrityksellä dokumentoitu ohjelma tietoturvallisuuden johtamiseksi ja turvallisuustyön tavoitteiden saavuttamiseksi?"
"Onko toiminnalle tärkeät suojattavat kohteet (toiminnot, tiedot, järjestelmät) tunnistettu?", minkä lisäkysymyksiksi on asetettu *"Mitä uhkia niihin kohdistuu? Onko suojattaville kohteille määritetty vastuuhenkilöt?"*
"Miten suojattaviin kohteisiin kohdistuvia riskejä arvioidaan?"
"Miten organisaation tietoturvallisuutta arvioidaan?", minkä lisäkysymykseksi on asetettu *"Kehitetäänkö toimintaa havaintojen perusteella?"*

”Onko tietoturvallisuudesta huolehdittu alihankinta-, palveluhankinta- ja muissa vastaavissa yhteistyökuvioissa?”
”Miten organisaatiossa toimitaan tietoturvapoikkeamatilanteissa?”
”Onko toiminnan lakisääteiset vaatimukset huomioitu?”, minkä lisäkysymykseksi on asetettu *”Ovatko esimerkiksi henkilötietojen käsittelyn prosessit henkilötietolain edellyttämällä tasolla?”*
”Onko yrityksessä menettely, jonka avulla varmistetaan, että merkittävät tietojenkäsittely-ympäristön muutokset tapahtuvat hallitusti?”
”Ovatko kaikki tietoverkot ja -järjestelmät yrityksen tietoturvaperiaatteiden mukaisesti suojattuja?”. Liitteessä 1 on nähtävissä myös kriteereille asetettavat lähtötason suositukset. (Elinkeinoelämän keskusliitto EK ym. 2009: 62–68.)

Henkilöstöturvallisuuden vaatimuksia lähestytään 7 pääkysymyksellä, fyysisen turvallisuuden 5, tietoliikenneturvallisuuden 8, tietojärjestelmäturvallisuuden 13, tietoaineistoturvallisuuden 7 ja käyttöturvallisuuden vaatimuksia lähestytään 10 pääkysymyksellä. (Elinkeinoelämän keskusliitto EK ym. 2009: 68–107.) Näiden osa-alueiden pääkysymysten aiheet ja lähtötason suositukset on luettavissa liitteessä 1.

4.7 Viestintävirasto, CERT-FI ja NCSA-FI: Yrityksen tietoturvaopas

Liikenne- ja viestintäministeriön alaisuudessa toimii Viestintävirasto. Viestintävirastossa toimivat CERT-FI- ja NCSA-FI-yksiköt. CERT-FI:n tehtävänä on ennaltaehkäistä, havainnoida ja ratkaista tietoturvaloukkauksia sekä tiedottaa tietoturvauhkista. Tietoturvaloukkauksella tarkoitetaan esimerkiksi oikeudetonta vaikuttamista organisaation, yrityksen, yhteisön tai yksityisen henkilön tietojärjestelmässä olevien tietojen käytettävyyteen, eheyteen tai luottamuksellisuuteen. NCSA-FI:n tehtävänä on valmistella kansalliseen turvallisuustoimintaan liittyvät ohjeistukset ja sopimukset sekä ohjeistaa kansainvälisen turvaluokitellun tietoaineiston käsittely, hallinnoida salausteknisen aineiston jakeluverkko ja ohjeistaa aineiston turvallinen käsittely sekä hoitaa sen kirjanpito. NCSA-FI:n tehtävänä on myös kansainvälisen turvaluokitellun tiedon suojaamiseen ja käsittelyyn tarkoitettujen salaustuotteiden ja tietojärjestelmien hyväksyntä. Huomioitavaa on, että liikenne- ja viestintäministeriön alainen Viestintävirasto toimii kansallisena tietoturvaviranomaisena, mutta ulkoasiainministeriöllä on kansainvälisten tietoturvavelvoitteiden kokonaisvastuu. (Viestintävirasto 2011; Liikenne- ja viestintäministeriö 2010a; CERT-FI 2010a; CERT-FI 2010b.)

Viestintäviraston (2010a) www-sivustolta löytyy yrityksille suunnattu *Yrityksen tietoturvaopas*. Oppaan etusivulla todetaan, että tietoturvan ylläpito on jatkuvaa ja suunnitelmallista toimintaa eikä sitä pystytä toteuttamaan yhdellä yksittäisellä toimenpiteellä. Opas on luotu antamaan neuvoja tietoturvan ylläpitämiseen. Oppaan lähtökohta on, että tietoturva on osa yrityksen liiketoimintaa. Jokaisella yrityksellä on suojattavaa tietoa. Yrityksen liiketoiminnan kannalta tärkeä tieto on sähköisessä muodossa, paperilla ja myös puhuttuna. Tietoturvaa ylläpidetään tekniikalla ja ihmisten työskentelytavoilla. Oppaassa korostetaan, että kaikkien työntekijöiden täytyy huolehtia tietoturvasta. Isojen investointien lisäksi jo pienikin panostus tietoturvaan hyödyttää yrityksen liiketoimintaa.

Tietoturvan toteuttaminen aloitetaan suojattavien kohteiden kartoittamisella, joka tehdään riskianalyysillä ja tiedon luokittelulla. Toimivan tietoturvan tavoitteena on säästää rahaa ja aikaa. Pyrkimyksenä on, että yritys pystyisi keskittymään ydinliiketoimintaansa. Tavoitteena on myös lisätä yrityksen uskottavuutta sekä hallita yrityksen tietojen siirtämistä yrityksen sisällä ja ulkopuolella. Lisäksi pyritään estämään luottamuksellisten tietojen joutuminen vääriin käsiin sekä tietojen vahingoittuminen. Tavoitteena on, että tiedot ja laitteet ovat käytettävissä, kun niitä tarvitaan. Lisäksi pyritään karsimaan turhat huolto- ja korjauskustannukset. (Viestintävirasto 2010e.)

Yrityksen tietoturvaoppaassa toimivan tietoturvan avainkysymyksiksi nostetaan seuraavat:

> *”Onko johto määritellyt yrityksen tietoturvan periaatteet ja tehnyt siihen liittyvät päätökset?*
> *Tietääkö henkilöstö mikä tieto on suojattava?*
> *Tietääkö henkilöstö missä tietoa säilytetään ja ketkä tiloihin pääsevät?*
> *Tietääkö henkilöstö miten toimitaan eri tilanteissa ja mitkä ovat tietoturvan pelisäännöt.*
> *Ovatko tietokoneiden ja verkon suojaukset ajan tasalla?*
> *Noudatetaanko ohjeita?”* (Viestintävirasto 2010e.)

Tietoturvaoppaassa neuvotaan panostamaan työntekijöiden osaamiseen. Työntekijöiden arkirutiinien kehittämisellä luodaan 80 % yrityksen liiketoiminnan tietojen turvallisuudesta ja vain 20 % tietojen turvallisuudesta pystytään luomaan teknisillä ratkaisuilla. Kaikilla työntekijöillä on vastuu tietoturvasta ja mitä paremmin työntekijät tuntevat toimintaohjeet, sitä parempi on tietoturva. Työntekijöiden perehdyttämiseen kannattaa käyttää eniten resursseja. Pelkät ohjekirjat eivät motivoi työntekijöitä ylläpitämään tietoturvaa. Hyvinkään toteutetut tekniset tietoturvaratkaisut eivät takaa tietoturvaa, jos työntekijät ovat välinpitämättömiä. Tietoturvan osana tulee varautua myös työntekijöiden väärinkäytöstapauksiin. Pereh-

dyttämisen lisäksi tietoturvariskejä pystytään vähentämään huolellisella rekrytoinnilla, salassapitosopimuksella ja työtehtävien vaatimilla tietojen käyttöoikeuksilla. Lisäksi tietoturvariskejä aiheuttavaan toimintaan tulee aina puuttua. Toimivan tietoturvan osana tulee suunnitella myös miten yritys hoitaa mahdolliset irtisanomiset. (Viestintävirasto 2010e.)

Tietoturvaoppaassa nostetaan esiin, että toimivan tietoturvan varmistamiseksi yrityksen tulee selvittää mihin laki velvoittaa yritystä ja sen liiketoimintaa tietoturvaan liittyen. Tietoturvaa (ja tietosuojaa) käsitellään Suomen lainsäädännössä muun muassa henkilötieto-, työsopimus-, kilpailu- ja rikoslaissa. Myös tietoturvarikokset ja -rikkomukset on määritelty lainsäädännössä kattavasti. (Viestintävirasto 2010e.)

Hyvin toteutetussa tietoturvassa tietojenkäsittely ja siihen liittyvät toiminnot on kartoitettu ja suunniteltu etukäteen. Tiedot on pyritty suojaamaan riittävästi ja tietoturvariskit on minimoitu. Toimiva tietoturva voidaan toteuttaa vaiheittain. Ensin kartoitetaan suojattavat kohteet. Sen jälkeen tehdään riskianalyysi ja tiedon luokittelu. Näiden pohjalta laaditaan tietoturvasuunnitelma. Tietoturvasuunnitelman julkaisun jälkeen tietoturva otetaan käyttöön perehdyttämällä työntekijät yrityksen tietoturvakäytäntöihin. Tietoturvasuunnitelma mahdollistaa tietoturvan jatkuvan kehittämisen yrityksessä. Tietoturvan toteuttaminen vaatii jatkuvaa seurantaa. Tietoturvan toteutumisen jatkuvuus on varmistettava, myös muuttuneissa olosuhteissa. (Viestintävirasto 2010e.)

Yrityksen tietoturvaoppaassa ohjeistetaan myös miten tietoturvakartoitus tulisi tehdä. Tietoturvan parantaminen aloitetaan kartoittamalla yrityksen tietoturvariskit. Riskien kartoittaminen ja ehkäiseminen tekevät liiketoiminnan jatkumisen mahdolliseksi. Kartoitus voidaan tehdä suppeasti tai laajasti. Laajuus riippuu yrityksestä ja sen haluamasta kartoituksen tasosta. Oppaassa neuvotaan, että kartoituksen kysymysten käsittelyyn ja tulosten tulkintaan kannattaa varata riittävästi aikaa. Vaikka paras tieto yrityksen toiminnasta ja tarpeista on yrityksen sisällä, voi kartoituksen teetättää myös ulkopuolisella taholla. Kartoituksen tekemisessä tarvitaan mukaan joka tapauksessa yrityksen työntekijöitä. Oppaassa huomautetaan, että valmis tietoturvakartoitusraportti sisältää erittäin kriittistä tietoa yrityksestä. (Viestintävirasto 2010f.)

Riskien kartoittamisen jälkeen tietoturvan parantamista jatketaan tiedon luokittelulla. Siinä selvitetään mitä tietoa yrityksellä on sekä miten, miltä ja miksi se tulee suojata. Tiedot selvitetään kartoittamalla käsiteltävät tiedot sekä yrityksen sisällä tai sen läpi kulkevat tietovirrat. Oleellista on selvittää tiedon taloudellinen merkitys yritykselle. Lisäksi on oleellista erottaa yrityksen toiminnalle kriittinen tieto muusta tiedosta. Sen löytäminen voi olla tiedon luokittelua yksinkertaisimmillaan.

Usein tieto jaetaan kuitenkin neljään luokkaan: julkinen, sisäinen, luottamuksellinen ja salainen. Tiedon luokittelu toimii pohjana tiedon käsittely- ja menettelyohjeille. Tiedon luokittelu ja tietovirtojen selvittäminen mahdollistavat selkeiden ohjeiden tekemisen tietojen käsittelylle. (Viestintävirasto 2010f.) Tiedon luokittelusta on aiemmin kerrottu kohdassa 3.3.

Tiedon käsittelyohjeessa kuvataan tiedon määrittely ja rajoitukset tietoon kohdistuvien toimenpiteiden ja tiedon luokittelun perusteella. Tietoon kohdistuvia toimenpiteitä ovat esimerkiksi tilaa tai tapahtumaa koskevan tiedon tunnistaminen sekä tiedon tallennus, arkistointi, tulostus, kopiointi ja jakelu. Myös paperimuotoisen ja elektronisen materiaalin lähetys ja tuhoaminen ovat tietoon kohdistuvia toimenpiteitä. Lisäksi henkilön matkustaminen ja tietojen kulkeminen hänen mukanaan tulee huomioida tietoon kohdistuvana toimenpiteenä. (Viestintävirasto 2010f.)

Yrityksen tietoturvaoppaassa huomioidaan, että tietoturvasta huolehtiminen edellyttää myös yksityisyyden suojan varmistamista eli henkilötietojen suojaamista käsiteltäessä esimerkiksi työntekijöiden tai asiakkaiden henkilötietoja. Velvollisuudesta suojata henkilötiedot on säädetty henkilötietolaissa ja erityislaeissa. Henkilörekisterin ylläpitäjää kutsutaan rekisterinpitäjäksi. (Viestintävirasto 2010f.)

Yrityksen tietoturvaoppaassa ohjeistetaan myös, että tietoturvakartoituksen yhteydessä tulee laatia tiedon elinkaari. Elinkaaren loppuvaiheessa on tärkeää muistaa, että tieto on yhä saatavilla jäteastiassa tai käytöstä poistetun tietokoneen kovalevyllä, minkä takia tiedon turvalliseen hävittämiseen tulee kiinnittää erityistä huomiota. Erityisesti yrityksen liiketoiminnan kannalta kriittinen tieto tulee turvata koko sen elinkaaren ajan. (Viestintävirasto 2010f.)

Yrityksen tietoturvaoppaassa neuvotaan kuinka tietoturvasuunnittelua tehdään. Oppaassa kerrotaan, että tietoturvasuunnitelma mahdollistaa yrityksen liiketoiminnan jatkumisen. Tietoturvasuunnitelma perustuu tietoturvakartoitukseen ja riskianalyysiin. Se toteutetaan tietoturvakartoituksessa löydettyjen tietojen perusteella. Suunnitelmassa tulee tuoda esille yritysjohdon periaatteet, joihin tietoturvakäytäntö perustuu. Oleellista suunnitelmassa on, että se vastaa kysymykseen ”Mitä, miksi ja miten tehdään?”. Tietoturvasuunnitelman tulisi sisältää ainakin seuraavat tietoturvan osa-alueet:

- Hallinnollinen turvallisuus (tietoturvaperiaatteet, toimintaohjeet ja seuranta)
- Fyysinen turvallisuus
- Henkilöturvallisuus
- Tietoaineistoturvallisuus

- Tietotekninen turvallisuus (sisältäen laitteistot, ohjelmistot, tietoliikenne ja käyttö). (Viestintävirasto 2010g.)

Tietoturvasuunnitelmaa tehtäessä yritysjohdon on tuotava esille tietoturvan merkitys yrityksen liiketoiminnalle ja maineelle sekä saatava työntekijät ymmärtämään sen tärkeys. Johdon perehtyminen tietoturvaan ja sitoutuminen tietoturvariskien hallintaan vaikuttaa suoraan onnistumiseen yrityksen tietoturvariskien torjumisessa. Vastuuta tietoturvasta ei voi ulkoistaa. Yritysjohdon toimiminen esimerkkinä tietoturvaa toteuttavissa työtavoissa ja toiminnassa on erityisen tärkeää. Esimerkkinä toimimisen lisäksi yritysjohdon tulisi huomioida tietoturvasuunnittelua tehtäessä seuraavat asiat:

- Tietoturva on osa laatujärjestelmää.
- Tietoturvan varmistamista varten tarvitaan riittävä osaaminen, jota tulee myös hyödyntää.
- Tietoturvatoimintaa on kehitettävä jatkuvasti.
- Laeilla on omat velvoitteensa tietoturvalle.
- Tietoturvariskien hallinta.
- Tietoturvaperiaatteet ja toimintaohjeet.
- Käyttöoikeuksien hallinta.
- Poikkeustilanteisiin (esimerkiksi häiriöt ja onnettomuudet) varautuminen.
- Tiedon luokittelu. (Viestintävirasto 2010g.)

Yrityksen tietoturvaoppaassa ohjeistetaan ottamaan työntekijät mukaan tekemään tietoturvasuunnittelua. Ohjeiden ja toimintatapojen käyttöönotto helpottuu, kun työntekijät ovat päässeet vaikuttamaan tietoturvaratkaisuihin jo suunnitteluvaiheessa. Yrityksen tietoturvasuunnittelussa kannattaa nimetä tietoturvan avainhenkilöt, jotka vastaavat yrityksen tietoturvan ylläpitämisestä. Avainhenkilöille on nimettävä myös varahenkilöt. (Viestintävirasto 2010g.)

Tietoturvasuunnitelmassa laaditaan selkeät ohjeet tietoturvan varmistamiselle. Ohjeiden tavoitteena on estää tietoturvaongelmien syntyminen. Ohjeet voivat käsitellä esimerkiksi yrityksen tietojen käsittelyä, Internetin ja sähköpostin käyttöä, laitteiden ja järjestelmien käyttöä sekä vierailijoiden tulemista yritykseen. Normaalikäytäntöjen lisäksi ohjeet tulee tehdä ongelmatilanteille ja poikkeusolosuhteita varten. Ohjeiden vieminen käytäntöön vaatii selkeästi määritellyt vastuut. Työntekijöiden tulee tietää, kenen vastuulla mikin asia on. (Viestintävirasto 2010g.)

Internetiä koskevia ohjeita laadittaessa tulisi ohjeistaa ainakin seuraavat asiat:

- sähköpostin käyttö
- tietojen selailu ja tiedostojen lataaminen Internetistä
- Internetin käyttö yleisenä tiedonsiirtoverkkona

- osallistuminen keskustelufoorumeihin
- Internetin käyttö tiedotukseen ja neuvontaan
- yrityksen luottokorttien käyttö maksuvälineenä Internetissä (Viestintävirasto 2010h).

Tietoturvan toimimista käytännössä ja tekniikan kunnossa olemista tulee seurata yrityksen sisäisillä tarkastuksilla. Havaittuihin väärinkäytöksiin tulee puuttua välittömästi. Ongelmatilanteet tulee käsitellä, ja mikäli ohjeistukset ovat siltä osin puutteelliset, tulee niitä tarkentaa. Tietoturvasuunnitelmaa tulee päivittää. Tietoturvasta tehdään yrityksen toimintakulttuurin osa suunnitelmallisella työllä ja työntekijöiden huolellisella perehdyttämisellä. Erityisesti työntekijöiden perehdyttämiseen tulee panostaa. (Viestintävirasto 2010g.)

Tietoturvasuunnittelua tehtäessä tulee suunnitella myös yrityksen toimitilojen turvallisuus. Tätä ohjeistusta tehtäessä kannattaa huomioida ainakin seuraavat kohdat:

”Valvotaanko tiloissa kulkemista?
Kuka työntekijä saa käsitellä tietoa ja missä tarkoituksessa?
Onko muussa kuin sähköisessä muodossa oleva tieto suojattu?
Onko yrityksellä erilliset neuvottelutilat?
Kuka hoitaa eri laitteiden huollon?
Miten kiinteistön vartiointi ja murtosuojaus on hoidettu ja kuka niitä ylläpitää?
Miten palo- ja pelastustoimi on hoidettu?
Onko pelastussuunnitelma laadittu?
Ovatko tilat omassa kiinteistössä tai erotettavissa muusta kiinteistöstä?
Kuka vastaa jätehuollosta ja siivouksesta?” (Viestintävirasto 2010g.)

Tietoturvakysymykset tulee huomioida myös laite- ja ohjelmahankinnoissa. Inhimilliset tekijät ovat usein suurin tietoturvariski, mutta myös tekniikan pettäminen saattaa aiheuttaa yritykselle suuria ongelmia. Palomuuri suojaa tietokonetta ulkopuolisilta tunkeilijoilta, kuten vakoiluohjelmilta ja viruksilta, mutta ei inhimillisiltä erehdyksiltä. Tämän takia verkon kautta tulevien hyökkäysten ja tietoturvauhkien estäminen edellyttää käyttäjien huolellista toimintaa ja palomuurin ylläpitoa. Palvelimet ovat tietojärjestelmien sydämiä, minkä takia palvelinten tietoturvasta tulee huolehtia erityisesti. Fyysisesti tulee huolehtia, että palvelimet ovat lukkojen takana ja niiden sijoitustilaan pääsevät vain tietyt henkilöt. Palvelinten sijoitustila tulee ilmastoida koneiden kuumenemisen estämiseksi. Sijoitustilalle tulee tehdä myös riskianalyysi tulipalon, vesivahingon ja varkauden varalta. (Viestintävirasto 2010g.)

Yrityksen tietoturvaoppaassa annetaan palvelimia koskevia vinkkejä:

1. Palvelinten hallinnointi on teknisesti haasteellista, minkä takia tulee panostaa osaavaan tietojenkäsittelyhenkilöstöön. Vaihtoehtoisesti palvelintoiminto voidaan ulkoistaa luotettavalle yhteistyökumppanille.
2. Palvelinten ylläpitäjien (eli ylläpito-oikeudet omaavien henkilöiden) määrä tulee rajata.
3. Palvelimelle tulee asentaa palomuuri ja virustorjuntaohjelma ja niitä täytyy päivittää. Myös palvelimen käyttöjärjestelmää ja sen varusohjelmistoja tulee päivittää.
4. Palvelin on vain palvelin-käytössä – ei koskaan samanaikaisesti työasemakäytössä.
5. Palvelimen käyttö tulee raportoida säännöllisesti. Raportoinnista vastaa palvelimesta vastaava henkilö.
6. Palvelin tulee varmuuskopioida säännöllisesti ja varmuuskopioita tulee säilyttää sovitulla tavalla lukitussa tilassa. Varmuuskopioiden tulee olla vain siihen oikeutettujen henkilöiden saatavilla. (Viestintävirasto 2010g.)

Tietoturvasuunnittelua tehtäessä tulee laatia ohjeet myös varmuuskopioinnille. Tiedon katoamisesta tai vahingoittumisesta aiheutuvat taloudelliset seuraukset voivat olla vakavia, minkä takia siihen pitää varautua ottamalla varmuuskopiot tiedoista. Varmuuskopion olemassa olo tällaisessa tilanteessa säästää työaikaa ja kustannuksia. Varmuuskopiot tulee säilyttää kokonaan eri rakennuksessa kuin alkuperäiset tiedot ovat. Tieto varmuuskopioiden säilytyspaikasta ja palautustavasta tulee olla vähintään kahden työntekijän tiedossa. Varmuuskopioiden toimivuus tulee tarkastaa säännöllisesti. (Viestintävirasto 2010g.)

Yrityksen tietoturvaoppaassa ohjeistetaan myös salausmenetelmien käyttöä tiedonsiirrossa. Tiedonsiirron salausmenetelmiä tulee käyttää, kun siirrettävä tieto on omaa, asiakkaan tai yhteistyökumppanin salassa pidettävää tietoa. Sähköisenä olevan tiedon muuttamista salakirjoitettuun muotoon voidaan kutsua kryptaamiseksi. Salaamisessa tieto muutetaan muotoon, jota ulkopuoliset eivät voi päästä näkemään tai ymmärtää. Salausmenetelmiä käytetään yleensä tietoliikenteen ja tietoaineistojen suojauksessa, esimerkiksi verkkokaupoissa, sähköpostissa, kannettavien tietokoneiden kovalevyissä ja muistitikuissa. Salattava tieto voi olla tiedosto, sähköpostiviesti tai jopa kokonainen kovalevy. Salattu tieto muutetaan ymmärrettävään muotoon salauksen purkavalla avaimella. Salaustekniikoita on useita ja niiden salauksen taso vaihtelee. Mitä vahvemmin tieto salataan, sitä vaikeampi sitä on ulkopuolisen saada auki ilman avainta. (Viestintävirasto 2010g.)

Yrityksen tietoturvaoppaassa käsitellään myös sähköisen asioinnin tekemistä turvalliseksi. Siinä korostuvat henkilöllisyyden varmentaminen ja palvelun turvallisuus. Luotettava henkilöllisyyden varmentaminen sähköisessä asioinnissa verk-

kopalvelussa on mahdollista esimerkiksi verkkopankkitunnuksilla. Sähköisessä asioinnissa korostuu, että asiakas voi luottaa verkkopalveluun. (Viestintävirasto 2010g.)

Onnistuneet tietoturvakäytännöt merkitsevät liike-elämässä hyvää mainetta ja laatua. Yhteistyösopimuksia laadittaessa tietoturvakysymykset nousevat yhä useammin esille. Yhteiset käytännöt ja vastuut turvataan tietoturvasopimuksilla. Lain mukainen tiedon suojaamisen vastuu on hyvä selvittää tarkkaan, mikäli tiedon käsittely ulkoistetaan. Työntekijöiden perehdyttäminen yrityksen tietoturvakäytäntöihin on tärkeää. Kaikkien työntekijöiden toimenkuvissa on työtehtäviä, joissa tietoturva pitää varmistaa. Työntekijän työsopimuksessa sovitaan salassapidosta ja tarvittaessa kilpailukiellosta. Työsopimuksen sisällöstä on tärkeää keskustella ja antaa työntekijälle riittävästi tietoa. (Viestintävirasto 2010i.)

Heti liikeneuvottelujen alussa tehdään salassapitosopimus. Näin turvataan esiin tulevan tiedon luottamuksellisuus. (Viestintävirasto 2010i.) Salassapitosopimus tulisi sisältää esimerkiksi seuraavat kohdat:

- *”sopijapuolet*
- *sopimuksen pääsisältö ja tavoite*
- *tehtävät, toiminnan luonne, osapuolten keskinäinen suhde*
- *työntekijän ja työnantajan aseman määrittely*
- *salassapitovelvoite (tietoa ei ilmaista eikä käytetä)*
- *menettelyt: asiakirjojen luovuttaminen ja palauttaminen, tietojenkäsittely, patentit, oikeudet keksintöön*
- *kilpailurajoitukset*
- *korvausvelvollisuudet: sopimussakko, vastuut vahingosta, rangaistuksen vaatiminen*
- *sopimuksen soveltaminen: pääyhtiö, muut yksiköt, työsuhteen päättymistavan vaikutus, jatkuminen työsuhteen päätyttyä*
- *referenssien käyttö*
- *riitaisuuden ratkaiseminen*
- *päiväys, allekirjoitukset, todistajat*
- *yhteyshenkilöt*
- *mahdolliset muut ehdot”* (Viestintävirasto 2010j).

Yrityksen tietoturvaoppaassa ohjeistetaan myös henkilötietojen käsittelyn ulkoistamista. Ulkoistaminen voi kohdistua esimerkiksi palkanlaskentaan tai postitukseen. Vaikka henkilötietojen käsittely ulkoistettaisiin, henkilörekisterin määräysvalta säilyy rekisterinpitäjällä eli toimeksi antaneella yrityksellä itsellään. Siksi se on myös vastuussa henkilötietolain asettamien velvoitteiden täyttämisestä henkilötietojen käsittelyssä. Toimeksi antanut yritys ja ulkoistetun toiminnon toimek-

siannon saanut yritys solmivat kirjallisen sopimuksen, jossa määritellään vastuut ja tehtävät käsittelyvaiheittain. Lisäksi he sopivat henkilötietojen käsittelyyn liittyvästä tietoturvasta ja miten tietoturvajärjestelyt tarkistetaan ja päivitetään. Erityishuomiota tulee kiinnittää salassapitoa, vaitiolovelvollisuutta ja tietojen suojaamista koskeviin säännöksiin ja määräyksiin. Toimeksi saanutta yritystä sitovat lisäksi henkilötietolain huolellisuus- ja suojaamisvelvoitteet. (Viestintävirasto 2010i.)

Yrityksen tietoturvaoppaassa käsitellään myös liikkuvan työn tietoturvaa. Liikkuvalla työllä kerrotaan oppaassa tarkoitettavan kaikkea työtä, joka tehdään yrityksen toimitilojen ulkopuolella. Näitä ovat kotoa käsin tehty työ, matkoilla työpaikan ja kodin välillä sekä työmatkoilla tehty työ. Myös WLAN- ja Bluetooth-yhteyksien käyttö katsotaan liikkuvaksi työksi. Liikkuvan työn laitteiksi mainitaan esimerkiksi kannettavat tietokoneet ja älypuhelimet. Tietoturvan perusasioiden lisäksi tietoturvaoppaassa neuvotaan kiinnittämään liikkuvassa työssä erityistä huomiota tietoliikenneyhteyksien suojaamiseen, laiterikkoihin varautumiseen ja luottamuksellisten tietojen vuotamisen estämiseen. Suurimmiksi tietoturvauhkiksi liikkuvalle työlle nimetään inhimilliset tekijät, suojaamattomat yhteydet, haittaohjelmat ja fyysiset uhat, kuten laiterikot ja varkaudet. (Viestintävirasto 2010k.)

Liikkuvassakin työssä tulee toteutua tiedon käytettävyys. Matkustaessa on tärkeää käsitellä tietoja sisältävää laitetta siten, että se ei vahingoitu. Kotoa käsin töitä tehtäessä tulee kiinnittää huomiota työtietokoneen käyttöön. Esimerkiksi lasten salliminen käyttää työtietokonetta ei ole tietoturvan ja erityisesti fyysisen tietoturvan kannalta viisasta riippumatta siitä miten yksinkertaista tietokoneen käyttö olisi. Laitteen rikkoutumisesta tai muusta fyysisestä syystä aiheutuva tiedon katoaminen tai vahingoittuminen voi aiheuttaa yritykselle merkittäviä taloudellisia seuraamuksia. Siksi tärkeät tiedostot on varmuuskopioitava riittävän usein myös liikkuvassa työssä käytettävistä laitteista. (Viestintävirasto 2010k.)

Liikkuvan työn uhkana on tietojen joutuminen sivullisten käsiin. Tästä johtuvat taloudelliset vahingot voivat aiheutua esimerkiksi yrityksen maineen kärsimisestä. Jotta tieto ei joutuisi sivullisten tietoon, ensimmäinen huomioitava asia on, että yrityksen asioista ei puhu kovalla äänellä. Julkisissa kulkuvälineissä ja tiloissa esimerkiksi puhelusi tai keskustelusi voi kuulla esimerkiksi kilpailija tai toimittaja. Työpaperien ja kannettavan näytön näkeminen tulee estä sivullisilta. Erittäin salaisten tietojen säilyttäminen mukana kulkevissa laitteissa kannattaa pitää mahdollisimman vähäisenä. Tietovarkaat anastavat laitteita taloudellisesti merkittävien tietojen toivossa. Kuitenkin inhimillinen riski on vielä suurempi. Pelkästään pääkaupunkiseudulla unohdettiin taksiin puolen vuoden aikana yli 3700 matkapu-

helinta, kannettavaa tietokonetta tai kämmenmikroa. (Viestintävirasto 2010k; Tietokone 2005.)

Haittaohjelmien siirtyminen muistitikun mukana on liikkuvassa työssä erityisen helppoa. Tämän aiheuttaa se, että muistitikun käyttö tehdään yrityksen palomuurin ja muun verkkotietoturvan ohi. Windowsin autorun-ominaisuuden päällä oleminen on erityisen vaarallista muistitikkua käytettäessä. Tällöin Windows käynnistää muistitikulla olevat haittaohjelmat automaattisesti, kun muistitikku kytketään tietokoneeseen. Erityisen hankalaksi tilanteesta tekee sen, että haittaohjelman käynnistyminen tai asentuminen ei välttämättä näy käyttäjälle millään tavalla. Autorun-ominaisuuden pitäminen poissa päältä olisikin tietoturvan kannalta paras ratkaisu. (Viestintävirasto 2010k.)

Yhteyksien suojaamisessa tulee huolehtia tietojen lähettämisestä ja vastaanottamisesta turvallisesti sekä palomuuri- ja virustorjuntaohjelmien asentamisesta ja jatkuvasta päivittämisestä. Yhteyksien suojaamisessa tulee huomioida lisäksi erityisesti langattoman verkkoyhteyden salaaminen. Salaamattomassa langattomassa verkossa ulkopuolinen verkkokäyttäjä kykenee pääsemään käsiksi esimerkiksi verkkoa käyttävän tietokoneen sähköposteihin. Tietojen suojaaminen salaamattomassa WLAN-verkossa voidaan tehdä esimerkiksi SSL-suojauksella, https-pohjaisella webmaililla tai VPN-yhteydellä. Mobiililaajakaistan käyttö on turvallisempaa, koska samassa verkossa ei ole muita käyttäjiä. (Viestintävirasto 2010k.)

Yrityksen tietoturvaoppaassa otetaan liikkuvan työn kohdalla esille myös Bluetooth-yhteyden käyttäminen. Oppaassa todetaan, että myös matkapuhelimet ovat alttiita haittaohjelmille. Ne voivat muun muassa tuhota puhelimessa olevia tietoja. Puhelimeen tallennettuihin numeroihin lähetetyt häiritsevät viestit ovat haittaohjelmien tekoa. Ongelmalliseksi tilanteen tekee se, että puhelin ja siinä oleva haittaohjelma toimii käyttäjän tietämättä. Yrityspuhelimen kohdalla tämä saattaa aiheuttaa merkittävää taloudellista haittaa. Myös yrityksen maine saattaa kärsiä. Oppaassa neuvotaan tarkistamaan tietokoneen ja matkapuhelimen Bluetooth-asetukset sallimaan laitteen näkyvyys Bluetooth-yhteydellä vain silloin, kun käyttäjä itse haluaa muodostaa uusia laitepareja tai vastaanottaa tietoa. Useimmissa laitteissa oletusasetuksena on, että laite näkyy kaikille. Lisäksi oppaassa neuvotaan harkitsemaan jokaisen uuden Bluetooth-yhteyden hyväksyminen aina erikseen. Erityisesti tuntemattomalta taholta tulevien yhteydenottopyyntöjen hyväksymisessä kannattaa käyttää harkintaa, ja pääsääntöisesti ne kannattaakin hylätä. (Viestintävirasto 2010k.)

Liikkuvaa työtä koskevien ohjeiden yhteenvetona voidaan todeta, että liikkuvassa työssä tärkeän tiedon tunnistaminen ja suojaaminen on erityisen oleellista. Myös työntekijöiden ohjeistaminen liikkuvan työn riskeistä on erityisen tärkeää. Kan-

nettavissa laitteissa säilytettävän tiedon määrää kannattaa rajata, ja erityisen salaisen tiedon määrä kannattaa pitää mahdollisimman pienenä. Liikkuvan työn laitteissa varmuuskopioinnista huolehtiminen on erityisen tärkeää. Lisäksi avoimessa verkossa liikkuva tieto tulee suojata. (Viestintävirasto 2010k.)

Yrityksen tietoturvaoppaan etusivulta löytyy linkki PDF-tiedostoon, joka sisältää mallin tietoturvaohjeista. Mallin avulla yritys pystyy luomaan oman yrityksensä tietoturvaohjeistuksen. Mallissa on nostettu esille seuraavat kohdat:

7. toimitiloihin kulkeminen
8. yleiset ohjeet toimimisesta yrityksen tiloissa
9. verkkosalasanat
10. virustorjunta erityisesti sähköpostissa ja verkosta ladattavien ohjelmien asentamisessa
11. varmuuskopiointi
12. tulostaminen
13. luottamuksellinen materiaali
14. työaseman ja kannettavan tietokoneen käyttö
15. tietoturva palavereissa ja esityksissä
16. Internetin käyttö
17. vierailijat
18. alihankkijat ja freelancerit. (Viestintävirasto 2010b.)

4.8 Teknologian tutkimuskeskus VTT

Teknologian tutkimuskeskus VTT (myöh. VTT) (aiemmin Valtion teknillinen tutkimuskeskus 30.11.2010 saakka) on työ- ja elinkeinoministeriön alaisuuteen kuuluva moniteknologinen tutkimuskeskus, joka tekee soveltavaa tutkimusta. Tutkimuksen visioiksi on valittu digitalisoituminen ja kestävä kehitys. Tietoturva on yksi VTT:n tutkimuksen ja teknologioiden kärki- ja innovaatio-ohjelmista, joihin se on keskittänyt noin puolet strategisesta tutkimuksestaan. Näissä ohjelmissa VTT kuuluu tutkimuksen kansainväliseen kärkeen. Tietoturvan suuressa innovaatio-ohjelmassa VTT tutkii ja kehittää menetelmiä ohjelmistokeskeisten järjestelmien tietoturvaominaisuuksien hallintaan, minkä keskeisiä osa-alueita ovat ohjelmiston tietoturvan varmistaminen, luotettavat alustat ja tietoturvan valvonta järjestelmän käytön aikana. Ohjelman moniulotteisempana näkökulmana tutkitaan ja kehitetään menetelmiä tietoturvariskien, -uhkien ja -haavoittuvuuksien analysointiin ja hallintaan. Kehitystyön perustana on visio, jossa tietotekniikalla ja sen ohjelmistoilla ja Internetillä on merkittävä rooli yhteiskunnan toiminnassa. Tietoturvan tutkimusalueella päätutkimuskohteita ovat tietoturvan analysointimenetelmät, tietoturvan varmistaminen ohjelmistossa, tietoturvan seuranta

ja varmistaminen toiminnallisessa järjestelmässä sekä tietoturvan mittaaminen eli tietoturvametriikat. Lisäksi tutkimuksen kohteena ovat tietoturvan hallinta, haavoittuvuusanalyysi, järjestelmän luotettavuusanalyysi ja kriittisen infrastruktuurin suojaaminen. Tietoturvatutkimuksen tuloksena syntyy sovelluksia, joiden hyödyntäjänä on ICT-toimiala ja erityisesti sen tietoliikenne, ohjelmistotuotanto ja teollisuusautomaatio sekä liiketoimintaan liittyvän tietoturvan hallinta. VTT näkee, että tehokkaiden tietoturvaratkaisuiden kehittämisessä täytyy tulevaisuudessa pyrkiä poistamaan epäjatkuvuuskohdat liiketoiminnan, tietoturvahallinnan, riskianalyysin ja teknisen tietoturvan väliltä. Tämä mahdollistetaan uusien menetelmien ja työkalujen kehittämisellä. (VTT 2010; VTT 2009a; VTT 2009b; VTT 2009c; VTT 2009d).

4.9 Valtionhallinnon tietoturvallisuuden johtoryhmä: VAHTI-ohjeistus

Valtiovarainministeriö vastaa valtion tietoturvan ohjauksesta ja kehittämisestä. Ministeriö on asettanut Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) koordinoimaan, ohjaamaan ja kehittämään hallinnon tietoturvaa. VAHTI ohjaa valtionhallinnon tietoturvatoimenpiteitä. Se käsittelee valtionhallinnon tietoturvaa koskevat tavoitteet sekä säädökset, ohjeet, suositukset ja linjaukset. VAHTIn tavoitteena on parantaa valtionhallinnon toimintojen luotettavuutta, laatua, jatkuvuutta, riskienhallintaa ja varautumista. Sen tavoitteena on myös tehdä tietoturvasta osa hallinnon toimintaa, johtamista ja tulosohjausta. Näihin tavoitteisiin se pyrkii parantamalla tietoturvaa. (Suomi.fi-portaali 2008; Valtiovarainministeriö 2010a.)

Valtiovarainministeriön (2010a) julkaisussa luetellaan VAHTIn tehtävät seuraavasti:

- valtionhallinnon tietoturvan tavoitteiden, toiminnan, organisoinnin, resurssilinjausten, normien, ohjeiden ja suositusten kehittäminen, yhteensovittaminen ja ylläpitäminen
- tietoturvan kehittäminen osana hallinnon kaikkea toimintaa sekä tietoturvan integroimisen edistäminen osaksi hallinnon prosesseja, tehtäviä, palveluita ja järjestelmiä
- valtioneuvoston ja valtiovarainministeriön hallinnon tietoturvan linjausten valmistelu ja yhteensovittaminen sekä niiden toimeenpanon seuranta ja edistäminen
- hallinnon tietoturvakulttuurin ja työntekijöiden tietoturvatietoisuuden edistäminen

- hallinnon organisaatioiden tietoturvan tavoitetasojen valmistelu ja käsittely sekä niiden toimeenpanon ja auditoinnin edistäminen
- hallinnon tietoturvan ja siihen varautumisen sekä kansallisen ja kansainvälisen kehityksen seuraaminen ja arviointi sekä tietoturvan linjausten, normien ja toimenpiteiden määrittely
- hallinnon kansainvälisen tietoturvayhteistyön linjausten ja kansainvälisessä tietoturvatyössä vaikuttamisen käsittely ja yhteensovittaminen
- valtion tietojenkäsittelystrategian toimeenpanon tietoturvan ja varautumisen ohjaaminen ja käsittely sekä näiden kehittämisohjelman ohjauksen organisointi.

VAHTI-ohjeistus on kaikki tietoturvan osa-alueet kattava valtionhallinnon tietoturvaohjeisto, josta VAHTI on vastuussa. Ohjeistus muodostuu useista julkaisuista, joita tulee koko ajan lisää. Voimassa olevia tietoturvaohjeita ja -määräyksiä on 46 kappaletta ja ne on julkaistu vuosina 2000–2012 (tilanne 4.1.2013). Julkaisut on tarkoitettu valtionhallinnolle, mutta ne soveltuvat hyödynnettäväksi myös muilla sektoreilla ja elinkeinoelämässä. Julkaisut löytyvät sähköisesti valtiovarainministeriön sivustolta ja ne ovat saatavissa myös painotuotteina pääsääntöisesti ilmaiseksi. VAHTI-ohjeistus on tarkoitettu erityisesti julkiselle sektorille. Aiemmin on kerrottu, että ISO:n tietoturvastandardit on tarkoitettu ja suunniteltu erityisesti yksityisen sektorin käyttöön. (Suomi.fi-portaali 2008; Valtiovarainministeriö 2013; Valtiovarainministeriö 2011; Valtiovarainministeriö 2010b; Laaksonen ym. 2006: 86.) Viimeisen viiden vuoden (tilanne 4.1.2013) aikana on julkaistu seuraavat VAHTI-ohjeet:

Vuonna 2012 julkaistiin kaksi ohjeistusta:
”Teknisen ICT-ympäristön tietoturva-ohje, VAHTI 3/2012
ICT-varautumisen vaatimukset, VAHTI 2/2012”. (Valtiovarainministeriö 2013.)

Vuonna 2011 julkaistiin kaksi ohjeistusta:
”Valtion ICT-hankintojen tietoturvaohje, VAHTI 3/2011
Johdon tietoturvaopas, VAHTI 2/2011”. (Valtiovarainministeriö 2011.)

Vuonna 2010 julkaistiin kolme ohjeistusta:
”Sosiaalisen median tietoturvaohje, VAHTI 4/2010
Sisäverkko-ohje, VAHTI 3/2010
Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, VAHTI 2/2010”. (Valtiovarainministeriö 2011.)

Vuonna 2009 julkaistiin viisi ohjeistusta:
”Kohdistetut hyökkäykset, VAHTI 6/2009

Effective Information Security, VAHTI 5/2009
Information Security Instructions for Personnel, VAHTI 4/2009
Lokiohje, VAHTI 3/2009
ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin, VAHTI 2/2009".
(Valtiovarainministeriö 2011.)

Vuonna 2008 julkaistiin viisi ohjeistusta:
"Hankkeen tietoturvaohje, VAHTI 9/2008
Valtionhallinnon tietoturvasanasto, VAHTI 8/2008
Informationssäkerhetsanvisning för personalen, VAHTI 7/2008
Valtionhallinnon salauskäytäntöjen tietoturvaohje, VAHTI 3/2008
Tärkein tekijä on ihminen - henkilöstöturvallisuus osana tietoturvallisuutta, VAHTI 2/2008". (Valtiovarainministeriö 2011.)

Voimassa olevista tietoturvaohjeista ja -määräyksistä vuonna 2007 on julkaistu kolme, vuonna 2006 yhdeksän, vuonna 2005 kolme, vuonna 2004 neljä ja vuonna 2003 neljä julkaisua. Lisäksi voimassa on vuodelta 2002 kaksi VAHTI-ohjeistusta, vuodelta 2001 yksi ja vuodelta 2000 kolme ohjeistusta. (Valtiovarainministeriö 2011). Laaksonen ja muut (2006: 81) tuovat esille, että kaikista VAHTI-ohjeistuksessa listatuista ja suositelluista toimenpiteistä ei ole saatavana Suomen lakiin perustuvaa virallista laintulkintaa.

5 MOTIVAATIO TIETOTURVAKRITEERIEN NOUDATTAMISESSA

Luvuissa 3 ja 4 käsiteltiin tietoturvaa ja sen ohjeistuksia. Tarkastelu rajattiin käsittelemään erityisesti hallinnollista tietoturvaa. Tässä luvussa muodostetaan aluksi tietoturvakriteerit luvuissa 3 ja 4 esitetyissä aineistoissa esiintyneistä hallinnollisen tietoturvan sisällöistä. Sen jälkeen muodostettuja kriteerejä käytetään empiirisen tutkimuksen toteutuksessa. Empiirinen tutkimus aloitetaan tietoturvakriteerien motivoivuutta testaavan kyselytutkimuksen toteutuksen ja tulosten kuvaamisella. Näiden tulosten pohjalta lukua jatketaan esittämällä vähiten motivoineiden tietoturvakriteerien motivaatiotekijöitä tutkivan haastattelututkimuksen toteutus ja tulokset. Luku päätetään kuvaamalla tietoturvakriteerien noudattamisen motivaation syntymiseen ja muuttumiseen vaikuttavia tekijöitä tutkivan haastattelun toteutus ja tulokset.

5.1 Hallinnollisen tietoturvan tietoturvakriteerien muodostaminen

Tietoturvakriteerillä tarkoitetaan tässä tutkimuksessa sellaisia nimettyjä yksittäisiä toimenpiteitä, joilla pyritään varmistamaan tietoturvan toteutuminen yrityksessä. Tähän tarkoitukseen ei ole olemassa yleisesti käytössä olevaa yhtä termiä. Elinkeinoelämän keskusliitto EK julkaisi vuonna 2009 Kansallisen turvallisuusauditointikriteeristön tietoturvalle (liite 1), johon viitaten tässä tutkimuksessa käytetään yksittäisestä toimenpiteestä yksikkömuotona termiä tietoturvakriteeri. Tutkimuksen yleisen rajauksen mukaisesti tietoturvakriteerit muodostetaan vain hallinnolliselle tietoturvalle. Kriteerien muodostamisen (liite 2) metodologiana käytetään dokumenttianalyysiä luvuissa 3 ja 4 esitettyihin dokumentteihin. Dokumenttien sisällöistä muodostetaan ensin luvussa 3 esitetyn kirjallisuuskartoituksen pohjalta alustavat kriteerit. Sen jälkeen alustavien kriteerien esiintymistä tarkastellaan luvussa 4 esitettyjen ohjeistusten sisällöissä. Lopullisiksi kriteereiksi valitaan ne kriteerit, jotka esiintyvät aineistoissa yhteensä vähintään kolme kertaa. Kolmen esiintymän perusteena on, että tällöin kriteeri on mainittu kirjallisuuden lisäksi vähintään kahdessa ohjeessa. Muodostettavia tietoturvakriteerejä käytetään ensin tutkittaessa millä tasolla yrityksen työntekijät pyrkivät tietoturvakriteerien noudattamiseen. Myöhemmin tietoturvakriteerejä käytetään tutkittaessa tekijöitä, jotka motivoivat yrityksen työntekijöitä pyrkimään tietoturvakriteerien noudattamiseen.

Muodostettavat tietoturvakriteerit jaetaan yleisiin ja hallinnollisiin tietoturvakriteereihin sen mukaan, koskeeko kriteeri *yleistä* hallinnollista tietoturvaa, jolloin

toteuttajina ovat *kaikki yrityksen työntekijät*, vai selkeästi *hallinnollista* tietoturvaa, jolloin toteuttajina ovat pelkästään yrityksen *hallinnossa työskentelevät työntekijät*. Tämän jaottelun sisällä kriteerit jaetaan tässä luvussa vielä pienempiin ryhmiin helpottamaan kriteerien myöhempää käyttöä. Ryhmien nimet on laadittu ainoastaan tämän tutkimuksen tarkoituksiin, koska ei ole olemassa yhtä yleistä käsitystä hallinnollisen tietoturvan tietoturvakriteerien ryhmittelemiseksi.

5.1.1 Yleiset tietoturvakriteerit

Yleiset tietoturvakriteerit jaetaan kuuteen ryhmään, jotka ovat työntekijälle asetettavat yleiset tietoturvakriteerit, yrityksen yleistä toimintaa koskevat tietoturvakriteerit, yrityksen toimintaa koskevat yleiset tietoturvakriteerit, yrityksen tietoja koskevat tietoturvakriteerit, työntekijän oikeuksia ja velvollisuuksia koskevat yleiset tietoturvakriteerit sekä työntekijän oikeuksia ja velvollisuuksia koskevat tietoturvakriteerit.

Työntekijälle asetettaviin yleisiin tietoturvakriteereihin sijoitetaan sellaiset yrityksen kaikkia työntekijöitä koskevat hallinnolliset tietoturvakriteerit, jotka työntekijöiden tulisi huomioida yleisesti kaikessa omassa toiminnassaan työsuhteeseen liittyen. Työntekijälle asetettavia yleisiä tietoturvakriteerejä nimetään 12 ja ne ovat:

> Tietoturvalle on luotava pelisäännöt.
> Työntekijän on ymmärrettävä tietoturvaan liittyvät yleiset oikeudet ja velvollisuudet.
> Työtietokoneen käytöllä on oltava tietyt käyttötarkoitukset ja -oikeudet.
> Työntekijällä on vastuu käyttäjätunnuksilla tehdyistä asioista.
> Salasanalle on määriteltävä vaatimuksia.
> Työtietokoneen ohjelmiin on liitettävä vaatimuksia.
> Yrityksen palomuurin ja virustorjuntaohjelmiston käyttöön on liitettävä vaatimuksia.
> Työsähköpostin ja roskapostin käsittelyyn on liitettävä vaatimuksia.
> Tietoturvatarkastuksia on tehtävä säännöllisesti.
> Tiedostojen tallentamiseen on liitettävä vaatimuksia.
> On ymmärrettävä tiedon ja tiedoston alkuperän selvittämisen tärkeys.
> On ymmärrettävä, että salakuuntelu on mahdollista.

Yrityksen yleistä toimintaa koskeviin tietoturvakriteereihin sijoitetaan sellaiset yrityksen kaikkia työntekijöitä koskevat hallinnolliset tietoturvakriteerit, jotka työntekijöiden tulisi huomioida yrityksen toimintaan liittyen yleisesti kaikessa

omassa toiminnassaan. Yrityksen yleistä toimintaa koskevia tietoturvakriteerejä on yhdeksän ja ne ovat:

Tietoturvan on varmistettava yrityksen liiketoiminnan ja palveluiden jatkuvuus.
Tietoturvaa on kehitettävä tietoturvatoiminnan prosessikuvauksia hyödyntäen.
Tietoturvan toteuttamisen tulee tukea ajan ja rahan säästämistä.
Tietoturvan toteuttamisessa tulee huomioida yleinen käsitys tietoturvan jakautumisesta tekniseen (20 %) ja hallinnolliseen (80 %) työhön.
Tietoturvatavoitteita ja -vaikutuksia on mitattava.
Tietoturvariskejä on ennakoitava ja niihin on varauduttava.
Tietokoneiden ja verkkojen suojaukset on oltava ajan tasalla.
Yrityksen arvojen tulee tukea tietoturvaa.
Tietoturvaa varten on luotava tietoturvapolitiikka ja -ohjeet.

Yrityksen toimintaa koskeviin yleisiin tietoturvakriteereihin sijoitetaan sellaiset yrityksen kaikkia työntekijöitä koskevat hallinnolliset tietoturvakriteerit, jotka työntekijöiden tulisi huomioida yleisesti kaikessa yrityksen toiminnassa. Yrityksen toimintaa koskevia yleisiä tietoturvakriteerejä on kahdeksan ja ne ovat:

Tietoturva on oltava kiinteä ja keskeinen osa koko yrityksen toimintaa.
Tietoturva on oltava yrityksen liiketoiminnan osa.
Tietoturvan toteuttamisen tulee olla suunniteltua ja seurattua toimintaa.
Tietoturva on sisällytettävä perehdytykseen.
Tietoturvassa on huomioitava työntekijän maalaisjärki ja päätöksentekotaidot.
Yrityksen johdon on määriteltävä tietoturvaperiaatteet.
Yrityksen johdon on tehtävä tietoturvapäätökset.
On ymmärrettävä, että tietoturvan suurin uhka on työntekijä ja hänen inhimillinen toimintansa.

Yrityksen tietoja koskeviin tietoturvakriteereihin sijoitetaan sellaiset yrityksen kaikkia työntekijöitä koskevat hallinnolliset tietoturvakriteerit, jotka työntekijöiden tulisi huomioida omassa toiminnassaan yrityksen tietoihin liittyen. Yrityksen tietoja koskevia tietoturvakriteerejä nimetään seuraavat seitsemän kriteeriä:

Tiedolle on laadittava elinkaari.
Asiakastiedot on varmistettava.
Taloudellisesti ja toiminnallisesti merkittävä tieto on selvitettävä tiedon luokittelulla.
Suojattava tieto on kartoitettava riskianalyysillä.

Keskeinen tieto on suojattava.
Tärkeä tieto on salakirjoitettava, jos siihen käsiksi pääseminen on mahdollista.
Varmuuskopioinnille on laadittava suunnitelma.

Työntekijän oikeuksia ja velvollisuuksia koskeviin yleisiin tietoturvakriteereihin sijoitetaan sellaiset yrityksen kaikkia työntekijöitä koskevat hallinnolliset tietoturvakriteerit, jotka yrityksessä tulisi yleisesti huomioida kaikille työntekijöille kuuluvina oikeuksina ja velvollisuuksina. Työntekijän oikeuksia ja velvollisuuksia koskevia yleisiä tietoturvakriteerejä nimetään yhdeksän ja ne ovat:

Työntekijälle on annettava koulutusta yrityksen tietoturvakäytäntöihin.
Työntekijälle on annettava tietoturvan sisältävää ohjausta ja ohjeita työhön.
Työntekijän tietoturvaosaamista on kehitettävä jatkuvasti.
Työntekijän on huomioitava tietoturva osana päivittäistä toimintaansa.
Työntekijän on tunnettava yrityksen tietoturvatoimenpiteet.
Työntekijän on ymmärrettävä, että tietoturvaa seurataan hallinnollisesti.
Työntekijän on tiedettävä toimintatavat eri tietoturvatilanteissa.
Työntekijän on osattava toimia rauhallisesti tietoturvapoikkeustilanteessa.
Vanhempien kollegojen on toimittava hyvänä esimerkkinä tietoturvakäyttäytymisessä.

Työntekijän oikeuksia ja velvollisuuksia koskeviin tietoturvakriteereihin sijoitetaan sellaiset yrityksen kaikkia työntekijöitä koskevat hallinnolliset tietoturvakriteerit, jotka työntekijöiden tulisi huomioida omaan toimenkuvaansa liittyvinä oikeuksina ja velvollisuuksina. Työntekijän oikeuksia ja velvollisuuksia koskevia tietoturvakriteerejä ovat seuraavat seitsemän kriteeriä:

Työntekijän on noudatettava yrityksen tietoturvakäytäntöjä.
Työntekijän on tiedettävä lähin tietoturvahenkilö.
Työntekijän on tiedettävä, mikä tieto on suojattavaa, missä se säilytetään ja kuka säilytystilaan pääsee.
Työntekijän on tunnettava yrityksen yleinen varmuuskopiointikäytäntö.
Työntekijän on noudatettava puhtaan pöydän periaatetta.
Työntekijän on lukittava lukituiksi ohjeistetut ovet.
Työntekijän on lukittava tietokone, kun hän ei ole käyttämässä sitä.

Yleisiä tietoturvakriteerejä nimettiin kuudessa ryhmässä yhteensä 52 kappaletta.

5.1.2 Hallinnolliset tietoturvakriteerit

Hallinnolliset tietoturvakriteerit jaetaan neljään ryhmään, jotka ovat yleiset hallinnolliset tietoturvakriteerit, yrityshallinnon tietoturvakriteerit, hallinnolliset tietoturvakriteerit sekä hallinnollisen toteuttamisen tietoturvakriteerit.

Yleisiin hallinnollisiin tietoturvakriteereihin sijoitetaan sellaiset hallinnolliset tietoturvakriteerit, joiden toteutuminen yrityksen johdon toiminnassa tulisi varmistaa yrityksen hallinnossa työskentelevien työntekijöiden toimesta. Yleisiä hallinnollisia tietoturvakriteerejä on seitsemän ja ne ovat:

Yrityksen johdon tietoisuus tietoturvauhkista on varmistettava.
Yrityksen johdon tuki tietoturvalle on osoitettava selkeästi.
Yrityksen toimintaan vaikuttavat lakisääteiset vaatimukset on huomioitava yrityksen hallinnossa.
Yrityksen hallinnon on huomioitava henkilöstöturvallisuus.
Yrityksen hallinnon on huomioitava toimitilaturvallisuus.
Yrityksen hallinnon on huomioitava tietoturvajohtamisen laajuus.
Yrityksen hallinnon on huomioitava tietoturvajohtamisen hyvä tietohallintotapa (IT Governance).

Yrityshallinnon tietoturvakriteereihin sijoitetaan sellaiset hallinnolliset tietoturvakriteerit, joiden toteutuminen yrityksen hallinnossa työskentelevien työntekijöiden tulisi varmistaa yrityksen toiminnassa ja tehdä näkyväksi kaikille työntekijöille. Yrityshallinnon tietoturvakriteerejä nimetään seuraavat seitsemän kriteeriä:

Yrityksen hallinnon on määriteltävä selkeästi tahot, jotka johtavat tietoturvaa.
Yrityksen hallinnon on määriteltävä selkeästi tahot, jotka vastaavat tietoturvasta.
Yrityksen hallinnon on määriteltävä menettelyt, joilla tietoturvaa hallitaan.
Yrityksen hallinnon on määriteltävä tietoturvan resursointi.
Yrityksen hallinnon on määriteltävä tietoturvan yhteys yrityksen liiketoimintastrategiaan.
Yrityksen hallinnon on määriteltävä yrityksen toiminnan kehittämisen jatkotoimenpiteet.
Yrityksen hallinnon on määriteltävä käytännön tietoturvatoimenpiteet.

Hallinnollisiin tietoturvakriteereihin sijoitetaan sellaiset hallinnolliset tietoturvakriteerit, joiden toteutuminen yrityksen hallinnossa tulisi huolehtia yrityksen

hallinnossa työskentelevien työntekijöiden toimesta. Hallinnollisia tietoturvakriteerejä on seitsemän ja ne ovat:

Yrityksellä on oltava selkeä tavoite yrityksen liiketoiminnalle.
Yrityksellä on oltava selkeät tavoitteet, jotka tukevat yrityksen toiminnan tuloksen syntymistä.
Yrityksellä on oltava tietoturvaohjelma tietoturvajohtamisen ja turvallisuustyön tavoitteiden saavuttamiseksi.
Yrityksellä on oltava tietoturvapolitiikka, -ohjeistukset ja -dokumentaatio.
Yrityksellä on oltava menettely kriittisten tapahtumien johtamiselle.
Yrityksellä on oltava toipumissuunnitelmat.
Yrityksellä on oltava menettelyt sidosryhmien tietoturvan hallintaan.

Hallinnollisiin toteuttamisen tietoturvakriteereihin sijoitetaan sellaiset hallinnolliset tietoturvakriteerit, joiden toteutuminen yrityksen hallinnossa työskentelevien työntekijöiden tulisi varmistaa yrityksen kaikessa toiminnassa. Hallinnollisia toteuttamisen tietoturvakriteerejä nimetään seuraavat kahdeksan kriteeriä:

Tietoturvan tavoitteita ja toteutumista on seurattava ja arvioitava.
Työntekijöille on kerrottava tietoturvariskeistä.
Tietoturvapoikkeamatilanteisiin on varauduttava.
Toiminnalle tärkeät ja siten suojattavat kohteet on tunnistettava.
Toiminnalle tärkeiden ja siten suojattavien kohteiden riskit on arvioitava.
Tietoverkot ja tietojärjestelmät on suojattava.
Merkittäviä tietojenkäsittely-ympäristöjä on muutettava hallitusti.
Asiakkaisiin ja sidosryhmiin on pidettävä yhteyttä tietoturvaa varten.

Hallinnollisia tietoturvakriteerejä nimettiin neljään ryhmään yhteensä 29 kappaletta. Yhteensä tietoturvakriteerejä nimettiin 81 kappaletta ja ne jaettiin kymmeneen ryhmään. Muodostettuja yleisiä ja hallinnollisia tietoturvakriteerejä käytetään seuraavissa alaluvuissa tutkittaessa niiden noudattamaan pyrkimisen tasoa sekä motivoivuutta.

5.2 Kyselytutkimuksen toteutus

Oy Kaha Ab:n (myöh. Kaha) työntekijöille tehtiin kvantitatiivinen kyselytutkimus, jonka tavoitteena oli selvittää millä tasolla työntekijät pyrkivät noudattamaan tietoturvakriteerien toteuttamista omassa työssään. Kaha on pääkaupunkiseudulla toimiva maahantuonti- ja tukkuliike, jonka tuotteita ovat henkilö- ja hyötyajoneuvojen varaosat ja lisävarusteet sekä työkalut ja ajoneuvoteollisuuden

komponentit. Yritys on perustettu vuonna 1934. Henkilöstöä yrityksessä on 150 ja liikevaihto vuonna 2011 oli 98,6 M€. Kaha kuuluu K.G. Knutsson -konserniin, joka on pohjoismaiden suurin vapaan varaosakaupan konserni. (Kaha 2013.) Aineistonkeruumenetelmänä käytettiin kyselyä, koska kyselyyn haluttiin vastaajiksi kaikki yrityksen omat käyttäjätunnukset omistavat työntekijät. Kyselytutkimus toteutettiin Webropol-ohjelmistoa apuna käyttäen helmikuussa 2013 sähköisellä lomakkeella, jonka täyttämispyyntö lähetettiin kaikille yrityksen omat käyttäjätunnukset omistaville työntekijöille sähköpostilla (liite 3). Pyynnön vastata kyselyyn lähetti yrityksen IT-päällikkö yhteensä yrityksen 119 työntekijälle. Näistä 15 oli nk. johtoryhmä-esimies -tasoon (myöhemmin esimies) luokiteltavia työntekijöitä ja loput 104 nk. työntekijöitä. Vastausaikaa oli 2 viikkoa. Vastausajan puolivälissä IT-päällikkö lähetti sähköpostilla muistutuksen kyselystä. Myös vastausajan viimeisenä päivänä muistutettiin sähköpostilla vastausajan päättymisestä. Kaikkien kyselyyn vastanneiden ja lisäksi erilliseen jatkokyselyyn yhteystietonsa täyttäneiden kesken arvottiin illalliskortteja.

Kyselylomakkeessa (liite 4) oli kysymyksiä yhteensä 82 kappaletta, joista kysymys 1 käsitteli vastaajan asemaa yrityksessä ja loput 81 kysymystä tietoturvakriteerejä. Tietoturvakriteerejä koskevat 81 kysymystä johdettiin suoraan kohdassa 5.1 esitetyistä hallinnollisen tietoturvan tietoturvakriteereistä. Syynä oli pyrkimys käyttää tietoturvakirjallisuudesta ja -ohjeistuksista analysoituja ja muodostettuja kriteerejä mahdollisimman alkuperäisessä muodossa empiirisessä tutkimuksessa. Kun lomake oli valmis, sen teknisen toimivuuden testasivat tutkija ja yrityksen IT-päällikkö tekemällä kumpikin harjoitusvastaamisen koko kyselyyn. Samalla yrityksen IT-päälliköllä varmistettiin lomakkeen ymmärrettävyys. IT-päällikkö huomautti ainoastaan kysymyksen 1 vastausvaihtoehdosta, johon hän halusi muutettavan esimies-vastausvaihtoehdon muotoon johtoryhmä/esimies yrityksessä olevan nimeämiskäytännön takia. Kriteerejä koskevissa kysymyksissä vastaajan piti arvioida omaa pyrkimystä noudattaa kutakin tietoturvakriteeriä. Vastausvaihtoehdot olivat kussakin kohdassa: en ollenkaan, melko harvoin, melko usein ja lähes aina. 4-portaista asteikkoa käytettiin, jotta vastaaja ei voi valita keskimmäistä vaihtoehtoa, vaan hän joutuu päättämään onko pyrkimyksen taso enemmin heikkoa vai vahvaa. Lisäksi kussakin kohdassa oli mahdollista vastata: en osaa sanoa. Jokaiseen kysymykseen vastaaminen oli määritelty pakolliseksi. Tällaiset kysymykset ja vastausvaihtoehdot valittiin, koska modernin motivaatioteorian mukaan motivaatiota tutkitaan määrittelemällä ihmisen tavoitteet ja pyrkimykset. Sen jälkeen selvitetään ihmisen omat mahdollisuudet toteuttaa ne ja vaikuttaa niihin. Lisäksi modernin motivaatioteorian tavoitteena on, että ihminen arvioi miten tärkeiksi hän kokee määritellyt tavoitteet ja pyrkimykset.

Vastauksia kyselyyn tuli yhteensä 58 kappaletta, joten vastausprosentti on 48,7 %. Näistä 13 vastaajaa oli esimies-tason työntekijöitä, jolloin esimiesten vastausprosentti on 86,7 % ja 45 vastaajaa oli nk. työntekijöitä, eli työntekijöiden vastausprosentti on 43,2 %. Tulokset raportoidaan niin, ettei yksittäistä vastaajaa voida tunnistaa. Vastaajia käsitellään kokonaisuuden lisäksi kahtena ryhmänä: esimiehinä ja työntekijöinä. Vastauksista koostetut tulokset on esitelty kokonaisuudessaan liitteessä 5.

Tulosten tarkastelussa kiinnitettiin erityisesti huomiota tietoturvakriteereihin, joiden noudattamispyrkimyksessä ilmeni heikkoutta tämän tutkimuksen tulosten analysointiin asetetulla kahdella **mittarilla**: 1) en ollenkaan/melko harvoin -vastauksia oli määrällisesti paljon (yhteensä enemmän kuin 33 % vastaajista) ja/tai 2) en osaa sanoa -vastauksia oli määrällisesti paljon (enemmän kuin 33 % vastaajista).

5.3 Tulokset tietoturvakriteerien noudattamispyrkimyksestä

Tässä kohdassa kuvataan ohjeistuksista muodostettujen tietoturvakriteerien motivoivuutta testaavan kyselytutkimuksen tulokset. Kyselytutkimuksen tulokset on esitetty kokonaisuudessa liitteessä 5, josta on nähtävissä sekä kaikki tulokset että erikseen eroteltuna tulokset aseman mukaan esimiesten ja työntekijöiden tuloksiin.

5.3.1 Yleiset tietoturvakriteerit

Yleiset tietoturvakriteerit esitettiin kyselyn kysymysryhmissä 2–7. Näiden aiheina olivat työntekijälle asetettavat yleiset tietoturvakriteerit, yrityksen toiminnassa olevat yleiset tietoturvakriteerit, yrityksen tietoja koskevat tietoturvakriteerit sekä työntekijän oikeuksia ja velvollisuuksia käsittelevät tietoturvakriteerit. Tulokset on esitetty kokonaan liitteessä 5, kysymysten 2–7 kohdalla.

Taulukossa 6 on käsitelty kysymyksen 2 vastaukset. Taulukosta on nähtävissä, että kokonaisuutena yrityksen työntekijät pyrkivät usein toteuttamaan heille asetettuja yleisiä tietoturvavaatimuksia. Ainoastaan pyrkimyksessä noudattaa tietoturvakriteeriä ”joku voi salakuunnella minua” on en ollenkaan/melko harvoin -vastausten määrä suuri (26 kpl).

Taulukko 6. Tietoturvakriteerit työntekijälle asetettavista yleisistä tietoturvavaatimuksista.

2. Minä pyrin työtehtävissäni ymmärtämään, että	**En ollenkaan**	**Melko harvoin**	**Melko usein**	**Lähes aina**	**En osaa sanoa**
tietoturvalle on olemassa pelisäännöt.	0	1	6	51	0
tietoturvaan liittyy yleisiä oikeuksia ja velvollisuuksia.	0	2	6	50	0
työtietokoneellani on tietyt käyttötarkoitukset ja -oikeudet.	0	1	7	50	0
minulla on vastuu käyttäjätunnuksillani tehdyistä asioista.	0	0	4	54	0
salasanalle on vaatimuksia.	0	1	10	47	0
työtietokoneen ohjelmiin liittyy vaatimuksia.	0	1	9	46	2
yrityksemme palomuuriin ja virustorjuntaohjelmistoon liittyy vaatimuksia.	0	1	6	47	4
työsähköpostiin ja roskapostiin liittyy vaatimuksia.	0	1	14	42	1
tietoturvatarkastuksia on tehtävä säännöllisesti.	0	3	17	35	3
tiedostojen tallentamiseen liittyy vaatimuksia.	0	7	12	37	2
tiedon ja tiedoston alkuperän selvittäminen on tärkeää.	1	7	17	31	2
joku voi salakuunnella minua.	6	20	6	15	11

En ollenkaan- ja melko harvoin -vastaukset (26 kpl) jakautuvat esimiesten ja työntekijöiden kesken (liite 5) siten, että esimiehissä näitä vastauksia on yhteensä 5 kpl (38 % esimiehistä) ja työntekijöissä 21 kpl, joka on lähes puolet työntekijöistä (47 %). Taulukosta 7 on nähtävissä, että myös yrityksen yleistä toimintaa koskevien yleisten tietoturvakriteerien toteuttamiseen pyritään usein.

Taulukko 7. Yrityksen yleistä toimintaa koskevat yleiset tietoturvakriteerit.

3. Minä pyrin työtehtävissäni tukemaan yrityksemme yleistä toiminnallista tavoitetta, että	**En ollenkaan**	**Melko harvoin**	**Melko usein**	**Lähes aina**	**En osaa sanoa**
tietoturva varmistaa yrityksen liiketoiminnan ja palveluiden jatkuvuuden.	0	1	12	42	3
tietoturvaa kehitetään tietoturvatoiminnan prosessikuvauksia hyödyntäen.	1	5	15	24	13
tietoturva säästää aikaa ja rahaa.	1	8	19	29	1
tietoturva on teknistä (20 %) ja hallinnollista (80 %) työtä.	1	7	12	23	15
tietoturvatavoitteita ja -vaikutuksia mitataan.	1	13	13	21	10
tietoturvariskejä ennakoidaan ja niihin varaudutaan.	0	3	14	37	4
tietokoneiden ja verkkojen suojaukset ovat ajan tasalla.	0	1	12	38	7
tietoturvaa tuetaan yrityksen arvoilla.	1	4	14	30	9
tietoturvaa varten luodaan tietoturvapolitiikka ja -ohjeet.	0	6	13	31	8

Kuitenkin, kun tulokset esitetään taulukossa 8 erikseen esimiesten ja työntekijöiden vastauksiin, on nähtävissä, että kriteerille ”tietoturva on teknistä (20 %) ja hallinnollista (80 %) työtä” on esimiehiltä tullut suhteessa paljon (38 %) en osaa sanoa -vastauksia (5 kpl).

Taulukko 8. Yrityksen yleistä toimintaa koskevat yleiset tietoturvakriteerit eriteltynä.

3. Minä pyrin työtehtävissäni tukemaan yrityksemme yleistä toiminnallista tavoitetta, että	En ollenkaan		Melko harvoin		Melko usein		Lähes aina		En osaa sanoa	
	Esimies	Tt	Esimies	Tt	Esimies	Tt	Esimies	Tt	Esimies	Tt
tietoturva varmistaa yrityksen liiketoiminnan ja palveluiden jatkuvuuden.	0	0	0	1	4	8	9	33	0	3
tietoturvaa kehitetään tietoturvatoiminnan prosessikuvauksia hyödyntäen.	0	1	0	5	6	9	5	19	2	11
tietoturva säästää aikaa ja rahaa.	0	1	1	7	5	14	7	22	0	1
tietoturva on teknistä (20 %) ja hallinnollista (80 %) työtä.	0	1	1	6	2	10	5	18	5	10
tietoturvatavoitteita ja -vaikutuksia mitataan.	0	1	4	9	3	10	3	18	3	7
tietoturvariskejä ennakoidaan ja niihin varaudutaan.	0	0	0	3	3	11	10	27	0	4
tietokoneiden ja verkkojen suojaukset ovat ajan tasalla.	0	0	0	1	4	8	9	29	0	7
tietoturvaa tuetaan yrityksen arvoilla.	0	1	1	3	4	10	7	23	1	8
tietoturvaa varten luodaan tietoturvapolitiikka ja -ohjeet.	0	0	1	5	5	8	7	24	0	8

Yrityksen toiminnallista tavoitetta tukevien tietoturvakriteerien pyrkimystaso on myös hyvä (taulukko 9). Heikkoa noudattamispyrkimystä on havaittavissa ainoastaan ”tietoturva sisältyy perehdytykseen” -kriteerissä, jossa 18 vastaajaa ilmoittaa ei pyri ollenkaan tai pyrkii melko harvoin kriteerin noudattamiseen. Liitteestä 5 on nähtävissä, että näistä vastaajista lähes kaikki ovat työntekijä-asemassa (ei ollenkaan 5 kpl, melko harvoin 10 kpl).

Taulukko 9. Yrityksen toimintaa koskevat yleiset tietoturvakriteerit.

4. Minä pyrin työtehtävissäni tukemaan yrityksemme toiminnallista tavoitetta, että	En ollenkaan	Melko harvoin	Melko usein	Lähes aina	En osaa sanoa
tietoturva on kiinteä ja keskeinen osa koko yrityksen toimintaa.	1	4	13	39	1
tietoturva on yrityksen liiketoiminnan osa.	2	6	12	36	2
tietoturva on suunniteltua ja seurattua toimintaa.	0	9	8	38	3
tietoturva sisältyy perehdytykseen.	5	13	16	17	7
tietoturvassa huomioidaan työntekijän maalaisjärki ja päätöksentekotaidot.	4	3	20	25	6
yrityksen johto määrittelee tietoturvaperiaatteet.	2	4	17	28	7
yrityksen johto tekee tietoturvapäätökset.	0	8	12	33	5
työntekijä ja inhimillinen toiminta ymmärretään tietoturvan suurimpana uhkana.	0	6	18	24	10

Taulukoissa 10 ja 11 on esitetty kysymyksen 5 tulokset yrityksen tietoja koskevien tietoturvakriteerien noudattamispyrkimyksen tasosta. Kaikista vastauksista (taulukko 10) ainoastaan kriteerille ”tärkeä tieto salakirjoitetaan, jos siihen käsiksi pääseminen on mahdollista” on tullut paljon en ollenkaan- tai melko harvoin -vastauksia (yhteensä 21 kpl). Kriteerille on tullut myös paljon en osaa sanoa -vastauksia (15 kpl).

Taulukko 10. Tietoja koskevat tietoturvakriteerit.

5. Minä pyrin työtehtävissäni tukemaan yrityksemme tietoihin liittyvää tavoitetta, että	**En ollen-kaan**	**Melko harvoin**	**Melko usein**	**Lähes aina**	**En osaa sanoa**
tiedolle laaditaan elinkaari.	4	15	17	12	10
asiakastiedot varmistetaan.	1	5	11	37	4
taloudellisesti ja toiminnallisesti merkittävä tieto selvitetään tiedon luokittelulla.	1	6	17	24	10
suojattava tieto kartoitetaan riskianalyysillä.	5	7	15	20	11
keskeinen tieto suojataan.	1	1	13	38	5
tärkeä tieto salakirjoitetaan, jos siihen käsiksi pääseminen on mahdollista.	11	10	10	12	15
varmuuskopioinnille laaditaan suunnitelma.	3	8	8	27	12

Kun vastauksia tarkastellaan eriteltynä (taulukko 11) huomataan, että tärkeän tiedon salakirjoittamiseen liittyvään kriteerin en ollenkaan- ja melko harvoin -vastausten määrä on suhteessa suuri molemmissa ryhmissä sekä työntekijöillä (16 kpl) että esimiehillä (5 kpl). Kaikista (21 kpl) en ollenkaan- ja melko harvoin -vastauksista kaikki 11 en ollenkaan -vastausta on tullut työntekijöiltä. Melko harvoin -vastaukset (10 kpl) puolittuvat tasan esimiesten ja työntekijöiden kesken. Työntekijä-asemassa olevien vastaajien määrä on suuri (16 kpl) myös kaikista ”tiedolle laaditaan elinkaari” -tietoturvakriteerille tulleista 19 en ollenkaan- ja melko harvoin -vastauksista.

Taulukko 11. Tietoja koskevat tietoturvakriteerit eriteltynä.

5. Minä pyrin työtehtävissäni tukemaan yrityksemme tietoihin liittyvää tavoitetta, että	En ollenkaan		Melko harvoin		Melko usein		Lähes aina		En osaa sanoa	
	Esimies	Tt	Esimies	Tt	Esimies	Tt	Esimies	Tt	Esimies	Tt
tiedolle laaditaan elinkaari.	1	3	2	13	5	12	3	9	2	8
asiakastiedot varmistetaan.	0	1	0	5	2	9	11	26	0	4
taloudellisesti ja toiminnallisesti merkittävä tieto selvitetään tiedon luokittelulla.	0	1	0	6	8	9	4	20	1	9
suojattava tieto kartoitetaan riskianalyysillä.	0	5	4	3	3	12	4	16	2	9
keskeinen tieto suojataan.	0	1	1	0	4	9	8	30	0	5
tärkeä tieto salakirjoitetaan, jos siihen käsiksi pääseminen on mahdollista.	0	11	5	5	3	7	2	10	3	12
varmuuskopioinnille laaditaan suunnitelma.	0	3	1	7	3	5	7	20	2	10

Taulukossa 12 on käsitelty työntekijän oikeuksia ja velvollisuuksia koskevia yleisiä tietoturvakriteerejä. Tämän ryhmän kriteerien noudattamaan pyrkiminen on kokonaisuutena melko heikkoa, sillä yhdeksästä kriteeristä ainoastaan kolmella ei ole nähtävissä kummankaan mittarin määrittelemää heikkoutta.

Taulukko 12. Työntekijän oikeuksia ja velvollisuuksia koskevat yleiset tietoturvakriteerit.

6. Minä pyrin työtehtävissäni huomioimaan, että yrityksessämme	En ollenkaan	Melko harvoin	Melko usein	Lähes aina	En osaa sanoa
minä saan koulutusta yrityksen tietoturvakäytäntöihin.	10	17	15	13	3
minä saan tietoturvan sisältävää ohjausta ja ohjeita työhöni.	4	20	19	12	3
minun tietoturvaosaamistani kehitetään jatkuvasti.	5	23	17	8	5
minä huomioin tietoturvan osana päivittäistä toimintaani.	0	6	19	31	2
minä tunnen yrityksen tietoturvatoimenpiteet.	7	13	19	15	4
tietoturvaa seurataan hallinnollisesti.	0	12	11	20	15
minä tiedän toimintatavat eri tietoturvatilanteissa.	5	12	21	12	8
minä osaan toimia rauhallisesti tietoturvapoikkeustilanteessa.	1	5	14	27	11
vanhemmat kollegat toimivat hyvänä esimerkkinä tietoturvakäyttäytymisessä.	6	21	14	9	8

Taulukosta 12 nähdään, että viidellä kriteerillä on paljon en ollenkaan/melko harvoin -vastauksia. Lisäksi yhdellä kriteerillä on paljon en osaa sanoa -vastauksia. Tuloksia on tarkasteltu tarkemmin taulukossa 13, jossa on esitetty erikseen esimiesten ja työntekijöiden vastaukset. Taulukosta 13 nähdään, että kaikissa taulukon kriteereissä heikkoa pyrkimystä osoittavista vastauksista erityisesti työntekijöiden osuus on suuri. ”Minä saan koulutusta yrityksen tietoturvakäytäntöihin” -

kriteerissä työntekijöiden en ollenkaan/melko harvoin -vastauksia on yhteensä 22 kpl, joka on lähes puolet (49 %) työntekijöiden vastauksista. ”Minä saan tietoturvan sisältävää ohjausta ja ohjeita työhöni” -kriteerillä työntekijöiden en ollenkaan/melko harvoin -vastauksia on 21 kpl, ”minun tietoturvaosaamistani kehitetään jatkuvasti” -kriteerillä 24 kpl, ”minä tunnen yrityksen tietoturvatoimenpiteet” -kriteerillä 16 kpl (36 %) sekä ”vanhemmat kollegat toimivat hyvänä esimerkkinä tietoturvakäyttäytymisessä” -kriteerillä 21 kpl. Lisäksi työntekijöillä on tietoturvan hallinnollista seuraamista käsittelevässä kriteerissä paljon (15 kpl) en osaa sanoa -vastauksia.

Taulukko 13. Työntekijän oikeuksia ja velvollisuuksia koskevat yleiset tietoturvakriteerit eriteltynä.

	En ollenkaan		**Melko harvoin**		**Melko usein**		**Lähes aina**		**En osaa sanoa**	
6. Minä pyrin työtehtävissäni huomioimaan, että yrityksessämme	**Esimies**	**Tt**	**Esimies**	**Tt**	**Esimies**	**Tt**	**Esimies**	**Tt**	**Esimies**	**Tt**
minä saan koulutusta yrityksen tietoturvakäytäntöihin.	1	9	4	13	4	11	3	10	1	2
minä saan tietoturvan sisältävää ohjausta ja ohjeita työhöni.	0	4	3	17	7	12	2	10	1	2
minun tietoturvaosaamistani kehitetään jatkuvasti.	0	5	4	19	7	10	1	7	1	4
minä huomioin tietoturvan osana päivittäistä toimintaani.	0	0	2	4	5	14	6	25	0	2
minä tunnen yrityksen tietoturvatoimenpiteet.	1	6	3	10	6	13	3	12	0	4
tietoturvaa seurataan hallinnollisesti.	0	0	5	7	4	7	4	16	0	15
minä tiedän toimintatavat eri tietoturvatilanteissa.	1	4	4	8	5	16	2	10	1	7
minä osaan toimia rauhallisesti tietoturvapoikkeustilanteessa.	1	0	2	3	2	12	7	20	1	10
vanhemmat kollegat toimivat hyvänä esimerkkinä tietoturvakäyttäytymisessä.	1	5	5	16	7	7	0	9	0	8

Taulukosta 13 nähdään myös, että esimiesten vastauksissa neljässä kriteerissä on tullut paljon en ollenkaan/melko harvoin -vastauksia. ”Minä saan koulutusta yrityksen tietoturvakäytäntöihin” ja ”minä tiedän toimintatavat eri tietoturvatilanteissa” -kriteereissä molemmissa on yhteensä 5 en ollenkaan- tai melko harvoin -vastausta sekä ”vanhemmat kollegat toimivat hyvänä esimerkkinä tietoturvakäyttäytymisessä” -kriteerissä 6 vastausta. Lisäksi ”tietoturvaa seurataan hallinnollisesti” -kriteerissä on 5 esimiestä antanut melko harvoin -vastauksen.

Viimeinen yleisten tietoturvakriteerien kysymys käsitteli työntekijän oikeuksia ja velvollisuuksia koskevia tietoturvakriteerejä, joiden kokonaistulokset on esitelty taulukossa 14.

Taulukko 14. Työntekijän oikeuksia ja velvollisuuksia koskevat tietoturvakriteerit.

7. Minä pyrin työtehtävissäni huomioimaan, että toiminnassani	**En ollenkaan**	**Melko harvoin**	**Melko usein**	**Lähes aina**	**En osaa sanoa**
minä noudatan yrityksen tietoturvakäytäntöjä.	0	1	8	48	1
minä tiedän lähimmän tietoturvahenkilön.	3	3	13	36	3
minä tiedän, mikä tieto on suojattavaa, missä se säilytetään ja kuka säilytystilaan pääsee.	5	10	18	15	10
minä tunnen yrityksen yleisen varmuuskopiointikäytännön.	12	11	17	12	6
minä noudatan puhtaan pöydän periaatetta.	3	10	21	14	10
minä lukitsen lukituiksi ohjeistetut ovet.	1	2	8	42	5
minä lukitsen tietokoneen, kun en ole käyttämässä sitä.	0	3	15	40	0

Taulukosta 14 nähdään, että lähes kaikkien kriteerien noudattamaan pyrkimisen taso on hyvä. Vain yhdellä kriteerillä, ”minä tunnen yrityksen yleisen varmuuskopiointikäytännön”, on paljon en ollenkaan/melko harvoin -vastauksia (23 kpl). Näistä vastauksista suurin osa (19 kpl) on työntekijöiden antamia, mikä on nähtävissä taulukossa 15, jossa on eroteltu esimiesten ja työntekijöiden vastaukset.

Taulukko 15. Työntekijän oikeuksia ja velvollisuuksia koskevat tietoturvakriteerit eriteltynä.

	En ollenkaan		**Melko harvoin**		**Melko usein**		**Lähes aina**		**En osaa sanoa**	
7. Minä pyrin työtehtävissäni huomioimaan, että toiminnassani	**Esimies**	**Tt**	**Esimies**	**Tt**	**Esimies**	**Tt**	**Esimies**	**Tt**	**Esimies**	**Tt**
minä noudatan yrityksen tietoturvakäytäntöjä.	0	0	0	1	2	6	11	37	0	1
minä tiedän lähimmän tietoturvahenkilön.	0	3	1	2	4	9	8	28	0	3
minä tiedän, mikä tieto on suojattavaa, missä se säilytetään ja kuka säilytystilaan pääsee.	1	4	4	6	4	14	4	11	0	10
minä tunnen yrityksen yleisen varmuuskopiointikäytännön.	1	11	3	8	7	10	2	10	0	6
minä noudatan puhtaan pöydän periaatetta.	1	2	3	7	6	15	1	13	2	8
minä lukitsen lukituiksi ohjeistetut ovet.	1	0	1	1	2	6	9	33	0	5
minä lukitsen tietokoneen, kun en ole käyttämässä sitä.	0	0	2	1	4	11	7	33	0	0

Esimiesten vastauksissa taulukossa 15 kiinnittyy huomio ”minä tiedän, mikä tieto on suojattavaa, missä se säilytetään ja kuka säilytystilaan pääsee” -kriteeriin, jossa

yhteensä 5 esimiestä on vastannut pyrkivänsä kriteerin toteuttamiseen en ollenkaan- ja/tai melko harvoin.

5.3.2 Hallinnolliset tietoturvakriteerit

Hallinnollisia tietoturvakriteerejä käsiteltiin kyselyssä kysymysnumeroissa 8–11. Niiden aiheina olivat yleiset hallinnolliset tietoturvakriteerit sekä hallinnollisen tietoturvan määritystä, luomista ja toteuttamista koskevat tietoturvakriteerit. Kaikissa hallinnollisissa tietoturvakriteereissä on nähtävissä, että esimiehillä on kaikkien näiden kriteerien toteuttamiseen hyvä pyrkimystaso, ja heikkouksia esiintyy lähinnä työntekijä-aseman työntekijöillä (liite 5, kysymykset 8-11).

Taulukossa 16 on esitetty kaikkien vastaajien yleisten hallinnollisten tietoturvakriteerien tulokset. Kaikkien vastaajien tuloksissa ei ole löydettävissä yhtään kriteeriä, joilla noudattamaan pyrkimisen taso olisi määriteltyjen mittarien perusteella heikkoa.

Taulukko 16. Yleiset hallinnolliset tietoturvakriteerit.

8. Minä pyrin työtehtävissäni huomioimaan, että yrityksemme hallinnossa	**En ollenkaan**	**Melko harvoin**	**Melko usein**	**Lähes aina**	**En osaa sanoa**
varmistetaan yrityksen johdon tietoisuus tietoturvauhkista.	2	8	14	20	14
osoitetaan selkeästi yrityksen johdon tuki tietoturvalle.	2	6	15	19	16
huomioidaan yrityksen toimintaan vaikuttavat lakisääteiset vaatimukset.	2	5	17	22	12
huomioidaan henkilöstöturvallisuus.	2	0	20	27	9
huomioidaan toimitilaturvallisuus.	2	0	20	26	10
huomioidaan tietoturvajohtamisen laajuus.	2	5	14	20	17
huomioidaan tietoturvajohtamisen hyvä tietohallintotapa (IT Governance).	2	4	17	16	19

Kun taulukossa 17 tarkastellaan erikseen esimiesten ja työntekijöiden vastauksia, on näiden kriteerien toteuttamispyrkimys esimiehillä kaikilta osin hyvää. Työntekijöillä sen sijaan on nähtävissä heikkoa toteuttamispyrkimystä kolmessa kriteerissä, mitä osoittaa en osaa sanoa -vastausten suuri määrä. Kriteerit ovat ”osoitetaan selkeästi yrityksen johdon tuki tieto-turvalle” (15 kpl en osaa sanoa -vastausta), ”huomioidaan tietoturvajohtamisen laajuus” (15 kpl) ja ”huomioidaan tietoturvajohtamisen hyvä tietohallintotapa (IT Governance)” (18 kpl).

Taulukko 17. Yleiset hallinnolliset tietoturvakriteerit eriteltynä.

8. Minä pyrin työtehtävissäni huomioimaan, että yrityksemme hallinnossa	En ollenkaan		Melko harvoin		Melko usein		Lähes aina		En osaa sanoa	
	Esimies	Tt	Esimies	Tt	Esimies	Tt	Esimies	Tt	Esimies	Tt
varmistetaan yrityksen johdon tietoisuus tietoturvauhkista.	0	2	3	5	3	11	6	14	1	13
osoitetaan selkeästi yrityksen johdon tuki tietoturvalle.	0	2	2	4	4	11	6	13	1	15
huomioidaan yrityksen toimintaan vaikuttavat lakisääteiset vaatimukset.	0	2	2	3	4	13	7	15	0	12
huomioidaan henkilöstöturvallisuus.	0	2	0	0	4	16	8	19	1	8
huomioidaan toimitilaturvallisuus.	0	2	0	0	5	15	6	20	2	8
huomioidaan tietoturvajohtamisen laajuus.	0	2	2	3	3	11	6	14	2	15
huomioidaan tietoturvajohtamisen hyvä tietohallintotapa (IT Governance).	0	2	1	3	5	12	6	10	1	18

Kysymysryhmässä 9 käsiteltiin yrityshallinnon tietoturvakriteerejä. Kaikkien tämän ryhmän kriteerien noudattamaan pyrkimys oli kokonaisuutena hyvää, mikä on nähtävissä liitteessä 5. Taulukossa 18 on esitetty tulokset eriteltynä esimiesten ja työntekijöiden vastauksiin, jolloin on nähtävissä, että myös erikseen molemmissa ryhmissä on noudattamaan pyrkimisen taso hyvää.

Taulukko 18. Yrityshallinnon tietoturvakriteerit eriteltynä.

9. Minä pyrin työtehtävissäni huomioimaan, että yrityksemme hallinnossa määritellään	En ollenkaan		Melko harvoin		Melko usein		Lähes aina		En osaa sanoa	
	Esimies	Tt	Esimies	Tt	Esimies	Tt	Esimies	Tt	Esimies	Tt
selkeästi tahot, jotka johtavat tietoturvaa.	0	3	1	1	4	14	8	19	0	8
selkeästi tahot, jotka vastaavat tietoturvasta.	0	3	1	1	4	10	8	23	0	8
menettelyt, joilla tietoturvaa hallitaan.	0	3	1	2	3	12	8	18	1	10
tietoturvan resursointi.	0	3	1	7	4	10	6	13	2	12
tietoturvan yhteys yrityksen liiketoimintastrategiaan.	0	3	2	4	3	9	7	16	1	13
yrityksen toiminnan kehittämisen jatkotoimenpiteet.	0	3	1	3	4	10	7	16	1	13
käytännön tietoturvatoimenpiteet.	0	3	1	2	6	8	6	22	0	10

Taulukossa 19 on käsitelty hallinnollisia tietoturvakriteerejä. Kokonaistuloksissa toipumissuunnitelman olemassaoloa käsittelevä kriteeri saa paljon (20 kpl) en osaa sanoa -vastauksia.

Taulukko 19. Hallinnolliset tietoturvakriteerit.

10. Minä pyrin työtehtävissäni huomioimaan, että yrityksellämme	**En ollenkaan**	**Melko harvoin**	**Melko usein**	**Lähes aina**	**En osaa sanoa**
on selkeä tavoite yrityksen liiketoiminnalle.	2	0	8	44	4
on selkeät tavoitteet, jotka tukevat yrityksen toiminnan tuloksen syntymistä.	2	0	8	44	4
on tietoturvaohjelma tietoturvajohtamisen ja turvallisuustyön tavoitteiden saavuttamiseksi.	2	2	14	27	13
on tietoturvapolitiikka, -ohjeistukset ja -dokumentaatio.	2	8	15	23	10
on menettely kriittisten tapahtumien johtamiselle.	3	5	18	19	13
on toipumissuunnitelmat.	3	8	16	11	20
on menettelyt sidosryhmien tietoturvan hallintaan.	3	7	16	16	16

Taulukossa 20 tuloksia tarkastellaan eriteltynä esimiesten ja työntekijöiden vastauksiin. Tällöin voidaan todeta, että toipumissuunnitelman olemassaoloa käsittelevän kriteerin tasoa laskee erityisesti työntekijöiden en osaa sanoa -vastausten suuri määrä. Kriteerille on työntekijöiltä tullut 17 en osaa sanoa -vastausta, joka on 38 % työntekijöiden vastauksista.

Taulukko 20. Hallinnolliset tietoturvakriteerit eriteltynä.

	En ollenkaan		**Melko harvoin**		**Melko usein**		**Lähes aina**		**En osaa sanoa**	
10. Minä pyrin työtehtävissäni huomioimaan, että yrityksellämme	**Esimies**	**Tt**	**Esimies**	**Tt**	**Esimies**	**Tt**	**Esimies**	**Tt**	**Esimies**	**Tt**
on selkeä tavoite yrityksen liiketoiminnalle.	0	2	0	0	1	7	12	32	0	4
on selkeät tavoitteet, jotka tukevat yrityksen toiminnan tuloksen syntymistä.	0	2	0	0	2	6	11	33	0	4
on tietoturvaohjelma tietoturvajohtamisen ja turvallisuustyön tavoitteiden saavuttamiseksi.	0	2	1	1	4	10	6	21	2	11
on tietoturvapolitiikka, -ohjeistukset ja -dokumentaatio.	0	2	3	5	4	11	5	18	1	9
on menettely kriittisten tapahtumien johtamiselle.	0	3	1	4	4	14	6	13	2	11
on toipumissuunnitelmat.	0	3	3	5	3	13	4	7	3	17
on menettelyt sidosryhmien tietoturvan hallintaan.	0	3	2	5	5	11	3	13	3	13

Taulukon 20 tuloksista voidaan todeta, että esimiesten osalta vastaukset osoittavat kokonaisuudessaan hyvää noudattamaan pyrkimisen tasoa. Kysymysryhmässä 11 esitetyillä hallinnollisilla toteuttamisen tietoturvakriteereillä on kaikkien kriteerien noudattamaan pyrkimisen taso kokonaisvastauksissa hyvää (liite 5). Taulukossa 21 on esitetty tulokset eriteltynä. Esimiesten noudattamaan pyrkimisen taso on myös näissä kriteereissä hyvä.

Taulukko 21. Hallinnolliset toteuttamisen tietoturvakriteerit eriteltynä.

11. Minä pyrin työtehtävissäni huomioimaan, että yrityksessämme	En ollen-kaan		Melko harvoin		Melko usein		Lähes aina		En osaa sanoa	
	Esimies	Tt	Esimies	Tt	Esimies	Tt	Esimies	Tt	Esimies	Tt
tietoturvan tavoitteita ja toteutumista seurataan ja arvioidaan.	0	0	2	5	5	8	4	15	2	17
työntekijälle kerrotaan tietoturvariskeistä.	0	4	2	8	6	12	5	12	0	9
varaudutaan tietoturvapoikkeamatilanteisiin.	0	1	3	5	2	11	7	14	1	14
tunnistetaan toiminnalle tärkeät ja siten suojattavat kohteet.	0	0	1	3	2	12	9	20	1	10
arvioidaan toiminnalle tärkeiden ja siten suojattavien kohteiden riskit.	0	0	1	7	2	10	8	16	2	12
suojataan tietoverkot ja tietojärjestelmät.	0	0	2	3	2	7	9	27	0	8
merkittäviä tietojenkäsittely-ympäristöjä muutetaan hallitusti.	0	0	1	7	4	6	7	19	1	13
pidetään yhteyttä asiakkaisiin ja sidosryhmiin tietoturvaa varten.	0	0	2	8	5	9	3	14	3	14

Taulukosta 21 nähdään, että työntekijöiden vastauksissa ”tietoturvan tavoitteita ja toteutumista seurataan ja arvioidaan” -kriteerillä on paljon (17 kpl) en osaa sanoa -vastauksia. Se on 38 % työntekijöiden vastauksista.

5.3.3 Yhteenveto: heikosti noudattamaan pyrityt tietoturvakriteerit

Kyselytutkimuksessa työntekijöitä pyydettiin arvioimaan omaa tietoturvakriteerien noudattamaan pyrkimyksen tasoa 81 tietoturvakriteerillä. Yhteenvetona todetaan, että kyselytutkimuksen tuloksissa on kohdassa 5.2 esiteltyjen mittarien perusteella heikosti noudattamaan pyrittyjä tietoturvakriteerejä yhteensä 22 kriteeriä eli 27 % tutkituista 81 kriteeristä. Näistä yleisiä tietoturvakriteerejä on 14 ja hallinnollisia 8. Heikosti noudattamaan pyrityt tietoturvakriteerit on esitelty taulukoissa 22 ja 23. Lisäksi kustakin tietoturvakriteeristä on harmaalla merkitty arvo, jonka takia kriteeri on määritelty heikosti noudattamaan pyrityksi.

Taulukko 22. Kyselyn tulosten yhteenveto: heikosti noudattamaan pyrityt yleiset tietoturvakriteerit.

Yleiset						
	Kaikki		**Esimiehet**		**Työntekijät**	
	En ollenkaan/ melko harvoin	**En osaa sanoa**	**En ollenkaan/ melko harvoin**	**En osaa sanoa**	**En ollenkaan/ melko harvoin**	**En osaa sanoa**
joku voi salakuunnella minua.	26	11	5	4	21	7
tietoturva on teknistä (20 %) ja hallinnollista (80 %) työtä.	8	15	1	5	7	10
tietoturva sisältyy perehdytykseen.	18	7	3	0	15	7
tiedolle laaditaan elinkaari.	19	10	3	2	16	8
tärkeä tieto salakirjoitetaan, jos siihen käsiksi pääseminen on mahdollista.	21	15	5	3	16	12
minä saan koulutusta yrityksen tietoturvakäytäntöihin.	17	3	5	1	22	2
minä saan tietoturvan sisältävää ohjausta ja ohjeita työhöni.	24	3	3	1	21	2
minun tietoturvaosaamistani kehitetään jatkuvasti.	28	5	4	1	24	4
minä tunnen yrityksen tietoturvatoimenpiteet.	20	4	4	0	16	4
tietoturvaa seurataan hallinnollisesti.	12	15	5	0	7	15
minä tiedän toimintatavat eri tietoturvatilanteissa.	17	8	5	1	12	7
vanhemmat kollegat toimivat hyvänä esimerkkinä tietoturvakäyttäytymisessä.	27	8	6	0	21	8
minä tiedän, mikä tieto on suojattavaa, missä se säilytetään ja kuka säilytystilaan pääsee.	15	10	5	0	10	10
minä tunnen yrityksen yleisen varmuuskopiointikäytännön.	23	6	4	0	19	6

Kyselyssä käsiteltiin yhteensä 52 yleistä tietoturvakriteeriä. Näistä 14 kriteerillä (27 %) ilmeni jomman kumman käytetyn mittarin mukaista heikkoa noudattamispyrkimystä, mikä on esitetty koostettuna taulukossa 22. Eniten heikon noudattamispyrkimyksen merkintöjä löytyy neljällä kriteerillä: ”joku voi salakuunnella minua” (3 merkintää), ”tärkeä tieto salakirjoitetaan, jos siihen käsiksi pääseminen on mahdollista” (4 merkintää), ”minä saan koulutusta yrityksen tietoturvakäytäntöihin” (3 merkintää) ja ”vanhemmat kollegat toimivat hyvänä esimerkkinä tietoturvakäyttäytymisessä” (3 merkintää). En osaa sanoa -heikon noudattamispyrkimyksen merkintöjä on vain kolmella kriteerillä, jotka ovat ”tietoturva on teknistä (20 %) ja hallinnollista (80 %) työtä”, ”tärkeä tieto salakirjoitetaan, jos siihen käsiksi pääseminen on mahdollista” ja ”tietoturvaa seurataan hallinnollisesti”. Näistä ”tietoturva on teknistä (20 %) ja hallinnollista (80 %) työtä” -kriteeri on ainut, jolla on pelkästään en osaa sanoa -merkintöjä. En ollenkaan/melko harvoin -heikon noudattamispyrkimyksen merkintöjä löytyy yhteensä 13 kriteerillä. Näistä kolmella tulos tulee pelkästään esimiesten vastauksista, kuudella pelkästään työntekijöiden vastauksista ja neljällä vastauksia oli tullut sekä esimiehiltä että työntekijöiltä.

Kyselyssä yhteensä 29 tietoturvakriteeriä luokiteltiin hallinnolliseksi tietoturvakriteeriksi. Näistä 8 kriteerin (28 %) kohdalla esiintyi asetetun mittariston perus-

teella heikkoa noudattamaan pyrkimystä, mikä on esitetty koostettuna taulukossa 23.

Taulukko 23. Kyselyn tulosten yhteenveto: heikosti noudattamaan pyrityt hallinnolliset tietoturvakriteerit.

Hallinnolliset						
	Kaikki		**Esimiehet**		**Työntekijät**	
	En ollenkaan/ melko harvoin	**En osaa sanoa**	**En ollenkaan/ melko harvoin**	**En osaa sanoa**	**En ollenkaan/ melko harvoin**	**En osaa sanoa**
osoitetaan selkeästi yrityksen johdon tuki tietoturvalle.	8	16	2	1	6	15
huomioidaan tietoturvajohtamisen laajuus.	7	17	2	2	5	15
huomioidaan tietoturvajohtamisen hyvä tietohallintotapa (IT Governance).	6	19	1	1	5	18
tietoturvan resursointi.	11	14	1	2	10	12
on toipumissuunnitelmat.	11	20	3	3	8	17
on menettelyt sidosryhmien tietoturvan hallintaan.	10	16	2	3	8	13
tietoturvan tavoitteita ja toteutumista seurataan ja arvioidaan.	7	19	2	2	5	17
pidetään yhteyttä asiakkaisiin ja sidosryhmiin tietoturvaa varten.	10	17	2	3	8	14

Taulukosta 23 voidaan aluksi todeta, että esimiesten osalta taulukko on puhdas ja kaikki heikon noudattamaan pyrkimisen merkinnät tulevat työntekijöiden vastauksista. Lisäksi taulukosta nähdään, että millään taulukossa esitetyllä kriteerillä ei ole en ollenkaan/melko harvoin -vastausten suuresta määrästä johtuvaa heikkoa noudattamaan pyrkimystä. Näin ollen kaikkien taulukossa esitettyjen kriteerien heikko noudattamaan pyrkimisen taso johtuu työntekijöiden en osaa sanoa -vastausten suuresta määrästä.

5.4 Ensimmäisen haastattelututkimuksen toteutus

Ensimmäisenä empiirisenä haastattelututkimuksena tehtiin Kahan työntekijöille sekä kvantitatiivinen että kvalitatiivinen haastattelututkimus. Haastattelun tavoitteena oli selvittää mitkä tekijät motivoivat työntekijöitä heidän pyrkiessä noudattamaan tietoturvakriteerejä. Haastattelu valittiin aineistonkeruumenetelmäksi, koska se mahdollisti motivaatiotekijöiden syvällisen käsittelyn. Samalla haluttiin pyrkiä ymmärtämään mitä ajatuksia kriteerit herättävät työntekijöissä sekä haluttiin täsmentää kyselytutkimuksessa epäselviksi jääneitä kohtia.

Haastattelun perustana oli helmikuussa 2013 Kahalla tehdyn kyselytutkimuksen tulosten 22 heikoimmin noudattamaan pyrittyä tietoturvakriteeriä**,** jotka on esitetty kohdassa 5.3.3. Näistä kriteereistä 14 oli yleisiä ja 8 hallinnollisia tietoturvakri-

teerejä. Motivaatiotekijöitä tarkasteltiin Decin ja Ryanin mittaamismenetelmällä toimintojen toteuttamisen motivaatiotekijöille, jotka ovat toisen henkilön tai tilanteen vaatimus, toteuttamisen tuottama mielihyvä tai oma kiinnostus, toteuttamatta jättämisestä aiheutuva häpeä, syyllisyys tai ahdistus sekä oma usko toteuttamisen tärkeydestä (esitetty kohdassa 2.1). Tämä menetelmä valittiin, koska sen muoto ja valmiit vastausvaihtoehdot sopivat arvioimaan yrityksen tietoturvakriteerien (eli tietoturvatoimenpiteiden) toteuttamisen motivaatiotekijöitä. 22 heikoimmin noudattamaan pyrityn tietoturvakriteerin ja Decin ja Ryanin mittaamismenetelmän pohjalta laadittiin haastattelurunko, joka on esitetty liitteessä 6. Haastattelun kysymyksillä pyrittiin tutkimaan tietoturvakriteereihin ja motivaatiotekijöihin liittyen työntekijöiden mielipiteitä ja asenteita. Haastattelussa käsiteltiin yhtä kriteeriä kerrallaan.

Haastateltavilta kysyttiin kuhunkin kriteeriin liittyen kaksi kysymystä. Ensimmäinen kysymys, *Millaisia ajatuksia kriteeri herättää sinussa?,* oli avoin kysymys, jolla pyrittiin selvittämään vastaajan mielipidettä. Kysymys valittiin, jotta pystyttiin ymmärtämään mitä ajatuksia kriteerit herättävät työntekijöissä sekä täsmentämään kyselytutkimuksessa epäselviksi jääneitä kohtia. Vastaajaa pyydettiin vastaamaan ensimmäiseen kysymykseen omin sanoin. Jälkimmäiselläkin kysymyksellä, *Mikä tai mitkä syyt motivoisivat sinua pyrkimyksessä noudattaa kriteeriä?*, selvitettiin mielipidettä ja asennetta. Kysymys valittiin, koska haluttiin selvittää mitkä tekijät motivoivat työntekijöitä heidän pyrkiessä noudattamaan tietoturvakriteerejä. Tämän kysymyksen vastaukset sidottiin Decin ja Ryanin mittaamismenetelmän mukaisiin vastausvaihtoehtoihin (toisen henkilön tai tilanteen vaatimus, toteuttamisen tuottama mielihyvä tai oma kiinnostus, toteuttamatta jättämisestä aiheutuva häpeä, syyllisyys tai ahdistus sekä oma usko toteuttamisen tärkeydestä). Kysymysten taustalla oli ajatus modernista motivaatioteoriasta, jossa tutkitaan motivaatiota ihmisen tavoitteiden näkökulmasta. Teorian mukaan ensin määritellään ihmisen tavoitteet ja pyrkimykset. Teorian yhtenä tavoitteena on selvittää millaisia tunteita ihmisellä herää tavoitteisiin ja pyrkimyksiin liittyen. Koska motivaatiotutkimusten yhteisenä tuloksena on löydetty runsaasti motivaatiotekijöitä, koettiin tutkimuksen suunnittelussa järkeväksi rajoittaa motivaatiotekijöiden määrää. Decin ja Ryanin mittaamismenetelmän mukaiset vastausvaihtoehdot tarjosivat sopivan vaihtoehdon. Haastattelun kysymysten ymmärrettävyys varmistettiin haastattelurungon laatimisen jälkeen yrityksen IT-päälliköllä, joka luki kysymykset läpi. Hän ei esittänyt vaatimuksia haastattelurungon muuttamiseksi.

Haastattelututkimus toteutettiin huhtikuussa 2013 yksilöhaastatteluna yrityksen tiloissa. Haastateltavat valittiin satunnaisesti numeron valitsevalla tietoteknisellä työkalulla kahdesta numeroidusta yrityksen henkilöstön nimilistasta, jotka oli järjestetty sukunimen mukaan aakkosjärjestykseen. Nimilistat muodostettiin ase-

man mukaan lajitellen, jolloin ensimmäisessä listassa olivat kaikki esimies-tason työntekijät (yhteensä 15 nimeä) ja toisessa kaikki nk. työntekijöihin kuuluvat työntekijät (104 nimeä). Haastattelussa oli alun perin varauduttu n. 15 haastattelun tekemiseen. Aluksi listoista valittiin haastatteluun kaksi esimiestä ja kolme työntekijää. Vain yhden esimiehen tai työntekijän haastattelua pidettiin liian suppeana. Viidennessä haastattelussa tulokset alkoivat toistua. Tämän jälkeen tehtiin vielä kolmen työntekijän haastattelu varmistamaan tuloksia. Tulosten toistuminen jatkui, jolloin voitiin varmistua saturaation saavuttamisesta ja haastattelut lopetettiin. Yhteensä haastatteluja tehtiin kahdeksan. Kenenkään haastatellun työntekijän toimenkuva ei liittynyt suoraan tietotekniikkaan. Kaikki haastattelut tehtiin yhden päivän aikana yhden ja saman henkilön toimesta. Haastateltavat saivat tiedon haastattelusta haastattelua edeltävänä päivänä. Haastateltavat eivät saaneet haastattelukysymyksiä tietoonsa etukäteen. Yhteen haastatteluun kulunut aika oli 20 minuutista reiluun puoleen tuntiin.

Käytännössä haastattelu eteni samalla tavoin kaikissa haastattelutilanteissa. Haastattelun teema ja näkökulma oli valittu etukäteen, minkä takia kaikille haastateltaville esitettiin samat kysymykset. Haastattelun alussa haastateltavalle annettiin haastattelun runko (liitteessä 6) myös paperilta seurattavaksi. Haastattelurungolla pyrittiin varmistamaan, että kaikkien haastateltavien kanssa käydään läpi samat asiat. Haastateltavalle kerrottiin liitteessä esitetty esipuhe myös suullisesti.

Haastatteluista kirjoitettiin heti haastattelun aikana muistiinpanot, kustakin haastattelusta oma muistiinpanonsa. Muistiinpanoihin kirjattiin huolellisesti kaikki haastateltavien vastaukset. Muistiinpanot kirjoitettiin puhtaaksi tekstinkäsittelyohjelmalla haastattelua seuraavana päivänä. Tutkimustulosten esittelyssä kerrotaan muistiinpanoihin kirjatut vastaukset, eikä omien asenteiden annettu millään tavoin vaikuttaa kerrottaviin tuloksiin. Kussakin haastattelussa tehdyt muistiinpanot käytiin läpi kaksi kertaa, jotta varmistuttiin siitä, että kaikki vastaukset ovat varmasti ja huolellisesti esitelty. Tulokset raportoitiin niin, ettei yksittäistä vastaajaa voida tunnistaa. Vastaajia käsiteltiin kahtena ryhmänä: esimies/johtoryhmä-asemassa olevia vastaajia käsiteltiin esimiehinä sekä muita työntekijöitä työntekijöinä.

Decin ja Ryanin menetelmän mukaiset neljä motivaatiotekijää on mahdollista lajitella ulkoisiin ja sisäisiin motivaatiotekijöihin. Ulkoisesti motivoiva on toisen henkilön tai tilanteen vaatimus -motivaatiotekijä sekä sisäisesti motivoivia loput kolme motivaatiotekijää eli toteuttamisen tuottama mielihyvä tai oma kiinnostus, toteuttamatta jättämisestä aiheutuva häpeä, syyllisyys tai ahdistus sekä oma usko toteuttamisen tärkeydestä. Tämä huomioidaan myöhemmin tulosten analysoinnissa.

5.5 Tulokset tietoturvakriteerien noudattamaan pyrkimisen motivaatiotekijöistä

Haastattelun ensimmäiseen kysymykseen, **millaisia ajatuksia kriteeri herättää** haastateltavassa, sai haastateltava vastata omin sanoin. Vastaukset olivat melko lyhyitä ja lähes kaikkien kriteerien kohdalla haastateltavat lähtivät miettimään toteutuuko kriteerin noudattaminen yrityksessä ja omassa työssä. Haastateltavat pohtivat vastauksissaan myös kriteerin noudattamisen tärkeyttä. Muutamien kriteerien kohdalla haastateltavat kysyivät ensireaktiona kriteerin ja sen termin merkitystä, jolloin haastattelija selitti merkityksen lyhyesti. Selitystä kaivattiin erityisesti termille hyvä tietohallintotapa (IT Governance), jonka kohdalla 6 haastateltavaa kysyi mitä se tarkoittaa. Toipumissuunnitelma-termin sekä teknisen ja hallinnollisen työn kohdalla kysyttiin 3 kertaa mitä niillä tarkoitetaan. Tietoturvan tavoitteiden ja toteutumisen seuraamiselle pyydettiin selitystä 2 kertaa. Lisäksi yhden kerran selitystä pyydettiin tiedon elinkaarelle, salakirjoittamiselle, yrityksen johdon tuen tietoturvan osoittamiselle, resursoinnille ja sidosryhmille.

Yleisistä tietoturvakriteereistä kysyttiin ensimmäisenä ajatuksia salakuuntelun mahdollisuudesta. Kaikki haastateltavat olivat yhtä mieltä siitä, että yrityksen toimistorakennuksessa ei tarvinnut lukittujen ulko-ovien takia pääasiallisesti miettiä salakuuntelun mahdollisuutta. Yksi haastateltava kuitenkin lisäsi, että rakennuksessakin mahdollisuus oli huomioitava jollain tavalla toteamalla ”*toki vieraita käy täälläkin*”. Sen sijaan rakennuksen ulkopuolella kaikki haastateltavat kertoivat ymmärryksensä arvioida liikesalaisuuksista puhuminen esimerkiksi puhelimessa aina tilanne- ja ympäristökohtaisesti.

”Tietoturva on teknistä (20 %) ja hallinnollista (80 %) työtä” -kriteerin kuultuaan lähes kaikki haastateltavat lähtivät pohtimaan, pitävätkö prosentit paikkansa ja totesivat, että on varmaan lähellä totuutta. Kriteerin sisällön merkityksen ymmärtämistä pidettiin myös tärkeänä.

Tietoturvan sisältymistä perehdytykseen pidettiin tärkeänä. Lähes kaikki haastateltavat totesivat, että kriteerin noudattaminen ei toteudu tai selkeästi näy yrityksen perehdytyksessä, mutta niin tulisi olla. Kaksi haastateltavaa näki yrityksen netti-etiketti-ohjeet jonkinlaisena perehdytyksenä. Yksi haastateltava totesi, että ehkä tietoturva ei sisälly perehdytykseen, koska ”*ihmisten oletetaan tietävän tietoturva-asiat jo ennestään*”.

Elinkaaren laatiminen tiedolle koettiin toteutuvan yrityksessä. Muutamassa vastauksessa elinkaaren laatimista pidettiin vaikeana. Tiedon elinkaaren laatiminen todettiin järkeväksi ja tärkeäksi. Yhdessä vastauksessa se yhdistettiin siihen, että

tiedot vanhenevat, jolloin niitä pitää päivittää tai uusia. Haastateltavien vastauksissa oli eriäviä mielipiteitä yhden haastateltavan todetessa, että ”*tietoa säilytetään liikaa”* ja toisen todetessa ”*historian tulisi säilyä”*.

Tärkeän tiedon salakirjoittamisen toteutumisen astetta omassa yrityksessä ei tiedetty selkeästi, mikä tuli esiin viidessä vastauksessa. Kahdessa vastauksessa asiaa pidettiin tärkeänä ja huomioonotettavana, yhdessä tarpeettomana. Lisäksi yhdessä vastauksessa todettiin, että yrityksen johdon tulisi kertoa, mikä tieto yritykselle on tärkeää.

”Minä saan koulutusta yrityksen tietoturvakäytäntöihin” -kriteeriin totesi puolet haastateltavista saavansa koulutusta ja puolet, että ei saa. Netti-etiketti-ohje ja teknisesti hoidetut rajoitukset nähtiin yhdessä vastauksessa jonkinlaisena tukena tietoturvakäytäntöjen oppimiselle. Seuraava kriteeri tietoturvan sisältävän ohjauksen ja ohjeiden saamisesta työhön samaistettiin yrityksen tietoturvakäytäntöjen koulutus -kriteeriin. Neljä haastateltavaa totesi saavan ohjausta ja ohjeita, joista kuitenkin yksi totesi myös, että ”*ohjeistusta ehkä puuttuu*”. Lisäksi yksi haastateltava vastasi, että ohjauksen ja ohjeiden saamisen taso on itse päätettävä ja ohjeiden saaminen on jollain ”*oman päättelyn tulosta”*.

Myös ajatukset tietoturvaosaamisen jatkuvasta kehittämisestä jakautuivat lähes puoliksi, kun viiden haastateltavan ensimmäisen ajatus kriteeristä oli, että ei toteudu, ja kolmen, että toteutuu. Yksi haastateltava pohti miten pitkää sykliä tarkoitetaan aikamääreellä jatkuvasti. Yhdessä vastauksessa toteutuminen koettiin tapahtuvan tietoturvaan liittyvillä tiedotteilla ja sähköposteilla, joita lähetetään työntekijöille.

”Minä tunnen yrityksen tietoturvatoimenpiteet” -kriteerin herättämät ajatukset olivat lyhyitä. Lähes kaikissa vastauksissa haastateltavat kertoivat tuntevansa yrityksen tietoturvatoimenpiteet osittain. Ainoastaan yhden haastateltavan ajatus oli, että hän ei tunne yrityksen tietoturvatoimenpiteitä. Lisäksi yksi haastateltava sanoi, että ”*tietoturvatoimenpiteitä ei tarvitse tietää, täytyy osata vain tietoturvakäyttäytyminen*”.

Tietoturvan seuraaminen hallinnollisesti nähtiin tietotekniikkaosastolla tapahtuvana toimenpiteenä kahdessa vastauksessa. Lisäksi viisi haastateltavaa uskoi kriteerin toteutumiseen yrityksessä ainakin osittain. Yksi haastateltava totesi, että ”*seuraamisessa havaituista virheistä mainitaan työntekijälle, jotta virhe ei toistuisi*”.

Tietotekniikkaosasto nähtiin kahdessa vastauksessa apuna myös eri tietoturvatilanteiden toimintatapoihin. Lisäksi viisi haastateltavaa vastasi tuntevansa toimin-

tatavat osittain. Näistä yksi haastateltava toi vastauksessaan esille, että ”*tiedän yrityksen toimintatavat osittain, mutta en tiedä mitä ovat yrityksen viralliset toimintatavat*”. Vain yksi haastateltava ei tiennyt toimintatapoja lainkaan.

Kriteeriin vanhempien kollegojen toimimisesta hyvänä esimerkkinä tietoturvakäyttäytymisessä kaksi haastateltavaa totesi kriteerin toteutuvan yrityksessä. Näistä toinen vastasi toteamalla ”*Opin heiltä, haluan tehdä asiat hyvin*”. Kolme haastateltavaa vastasi, että kriteeri ei toteudu. Näistä yksi totesi, että ”*eivät vanhemmat kollegat toimi myöskään huonona esimerkkinä*”. Yksi haastateltava toi esiin merkittävimpänä asiana konsernin roolin ja yksi pyrki itse olemaan hyvänä esimerkkinä myöhemmin rekrytoiduille työntekijöille. Lisäksi yksi haastateltava koki, että vanhempien kollegojen esimerkillä ei ole merkitystä tällä hetkellä, mutta piti kriteerin huomioimista tärkeänä.

Lähes kaikki haastateltavat uskoivat ”minä tiedän, mikä tieto on suojattavaa, missä se säilytetään ja kuka säilytystilaan pääsee” -kriteerin toteutuvan yrityksessä. Vain kaksi haastateltavaa vastasi kysymykseen ”ei toteudu”, mutta heidänkin vastauksensa kriteerin toteutumattomuudesta koski vain kriteerin loppuosaa tiedon säilytyspaikasta ja tilaan pääsevistä henkilöistä. Näistä toinen haastateltava totesi ”*tarvitseeko kaikkea tietää*”.

Viimeiseen yleiseen tietoturvakriteeriin yrityksen yleisen varmuuskopiointikäytännön tuntemisesta vain yksi haastateltava vastasi, että ei tunne käytäntöä. Loput seitsemän haastateltavan vastauksena oli ajatus, että tuntee käytännön vähintään osittain. Yksi haastateltava toi esille, että ”*varmuuskopiointikäytännöstä ei ole olemassa selkeää ohjetta*”.

Toisessa osassa esitetyt hallinnolliset tietoturvakriteerit aiheuttivat jonkin verran hämmennystä etenkin työntekijä-asemassa toimiville viidelle haastateltavalle. Heidän vastauksensa olivat erityisen lyhyitä ja osittain vastaukset esitettiin epävarmoina. Sen sijaan esimies-asemassa toimivien työntekijöiden vastauksissa ei näkynyt eroa yleisten tietoturvakriteerien vastaustyyliin.

Hallinnollisista tietoturvakriteereistä yksi työntekijä-asemassa ollut työntekijä toi toistuvasti jokaisen hallinnollisen kriteerin kohdalla esille, että hänellä ei ollut tietämystä mitä hallinnossa tapahtuu.

Ensimmäinen hallinnollinen tietoturvakriteeri käsitteli yrityksen johdon tuen osoittamista tietoturvalle selkeästi. Kuusi haastateltavaa totesi kriteerin toteutuvan yrityksessä. Näistä yksi piti tuen selkeää osoittamista tärkeänä vastaamalla ”*totta kai tulee tukea*”. Kaksi haastateltavaa ei osaa sanoa kriteerin näyttäytymisen tasoa yrityksessä.

”Huomioidaan tietoturvajohtamisen laajuus” -kriteeriin yhden haastateltavan ensimmäinen ajatus oli, että ”laajuus tulee tuntea, jotta ymmärtää mahdolliset ongelmat”. Lisäksi viisi haastateltavaa totesi, että tämä toteutuu yrityksessä ainakin jollakin tasolla. Kaksi haastateltavaa ei osannut sanoa toteutumisen tasoa.

Huomioidaan tietoturvajohtamisen hyvä tietohallintotapa (IT Governence) -kriteeri hämmensi eniten haastateltavia, joista kuusi haastateltavaa pyysi kriteerin kuultuaan selittämään mitä sillä tarkoitetaan. Selityksen jälkeen kuusi haastateltavaa totesi, että kriteeri toteutuu yrityksessä. Kaksi haastateltavaa ei osannut sanoa kriteerin toteutumisen tasoa.

Tietoturvan resurssien nähtiin kasvaneen useiden haastateltavien ajatuksissa, esimerkiksi ”*resursseja on parannettu viime aikoina*” totesi yksi haastateltava. Vain yhdessä vastauksessa ei osattu sanoa toteutumisen tasoa. Muut haastateltavat uskoivat tietoturvaresurssien määrittelyn toteutuvan yrityksessä. Kahdessa vastauksessa resurssien nähtiin jotenkin määräytyvän konsernin toimesta, yksi haastateltava uskoi tietotekniikkaosaston päättävän resursseista ja yksi talousosaston.

Toipumissuunnitelmien olemassaolon toteutumiseen uskoi 5 haastateltavaa. Näistä yksi uskoi konsernin hoitavan asian. Kaksi haastateltavaa sanoi vastauksessaan, että toipumissuunnitelmien olemassaolo ei näy työntekijälle. Lisäksi yksi vastaaja lisäsi, että ”*businekseen jatkuminen vaatii toipumissuunnitelmien olemassaoloa*”. Kolme haastateltavaa ei osannut sanoa kriteerin toteutumisen tasoa yrityksessä.

Myös sidosryhmien tietoturvan hallintaan tehtävien menettelyjen olemassaoloon nähtiin yhdessä vastauksessa busineksen vaatimus. Yksi haastateltava totesi kriteerin näkyvän yrityksessä ”*asiakkaiden auttamisena*” ja toinen ”*yhteisten palomuuri-ongelmien ratkaisemisena*”. Kriteerin toteuttaminen nähtiin myös konsernin tehtävänä. Yhdessä vastauksessa tämä uskottiin toteutettavan teknisesti. Vain yhdessä vastauksessa ei osattu arvioida toteutumisen tasoa.

Tietoturvan tavoitteiden ja toteutumisen seuraaminen ja arvioiminen nähtiin toteutuvan yhden haastateltavan vastauksessa ”*laatusertifikaatin vaatimuksesta*”. Yksi haastateltava kertoi seuraamista tehtävän kuukausittain ja päivittäin. Yksi haastateltava nosti esimerkkinä esiin salasanan vaihdon. Kaksi haastateltavaa ei osannut arvioida toteutumisen tasoa.

Viimeinen hallinnollinen tietoturvakriteeri käsitteli yhteyden pitämistä asiakkaisiin ja sidosryhmiin tietoturvaa varten. Kriteeri nähtiin kehittämisen lähtökohtana ja aukkojen löytämisen apuna. Yksi haastateltava kertoi esimerkkinä ”*salassa pidettävien asioiden sopimisen*”. Yhdessä vastauksessa kriteerin toteutuminen

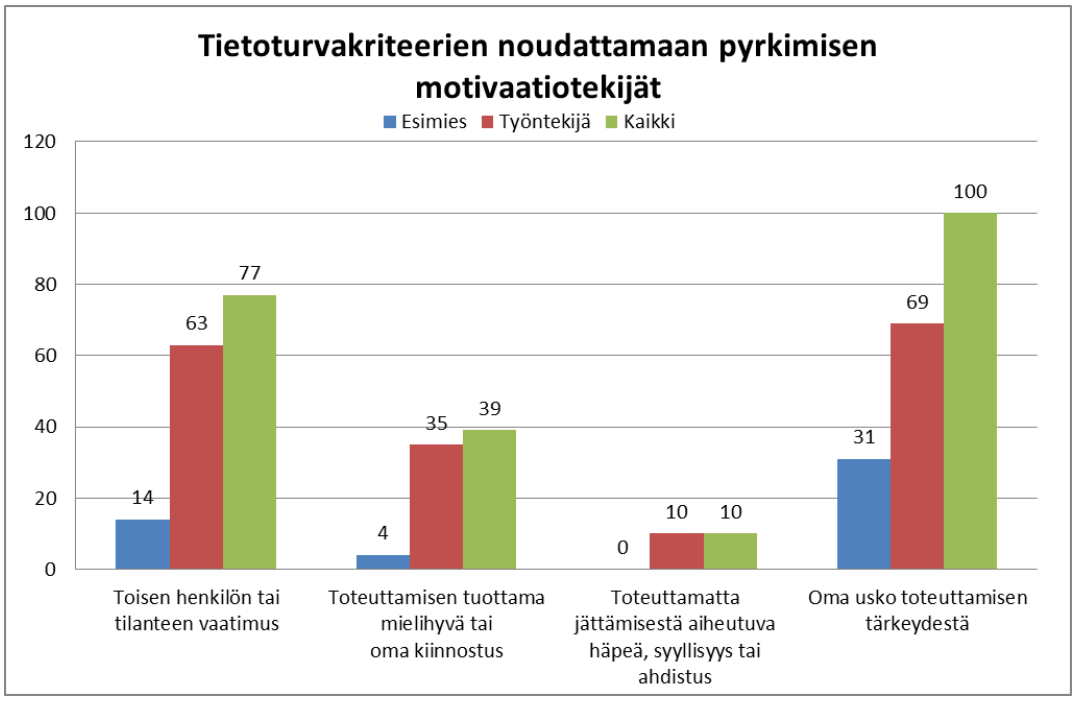
nähtiin tärkeänä ja toisessa haluttiin nostaa esille, että ”*tiedon annon tulee olla harkittua*”. Yksi haastateltava ei uskonut kriteerin toteutuvan yrityksessä.

Haastattelun toisessa kysymyksessä, **mikä tai mitkä syyt motivoisivat haastateltavaa pyrkimyksessä noudattaa kriteeriä**, pyydettiin vastaajia ensisijaisesti valitsemaan vastaus Decin ja Ryanin menetelmän neljän tekijän vaihtoehdoista, jotka ovat toisen henkilön tai tilanteen vaatimus, toteuttamisen tuottama mielihyvä tai oma kiinnostus, toteuttamatta jättämisestä aiheutuva häpeä, syyllisyys tai ahdistus sekä oma usko toteuttamisen tärkeydestä (esitetty kohdassa 2.1). Vastaajien oli kunkin kriteerin kohdalla mahdollista valita neljästä tekijästä 1-4 vaihtoehtoa. Lisäksi vastaajalle annettiin vastausvaihtoehdot ”Muu syy, mikä?” ja ”En osaa sanoa syytä”.

Tietoturvakriteerien motivaatiotekijöiden valitseminen Decin ja Ryanin menetelmän vaihtoehdoista oli kaikille haastateltaville helppoa, eikä kukaan haastateltava valinnut minkään kriteerin kohdalla, että ei osaisi sanoa tekijää, joka saisi hänet motivoitua pyrkimään yksittäisen kriteerin noudattamiseen. Haastateltavat eivät myöskään nimenneet annettujen vaihtoehtojen ohi mitään muuta motivaatiotekijää kriteerin noudattamiselle.

Haastateltavilla oli mahdollisuus valita 1-4 motivaatiotekijää. Pääsääntöisesti haastateltavat valitsivat annetuista motivaatiotekijöistä ainoastaan yhden vaihtoehdon, kun 22 kriteerin kohdalla kahdeksan haastateltavaa valitsi ainoastaan yhden motivaatiotekijän kaikkiaan 141 kertaa, eli keskimäärin noin 18 kriteerin kohdalla haastateltavaa kohden. Kaksi motivaatiotekijää valittiin yhteensä 23 kertaa eli keskimäärin noin kolme kertaa haastateltavaa kohden. Kolme motivaatiotekijää valittiin seitsemän kertaa ja neljä motivaatiotekijää viisi kertaa, joista yhtä kolmen motivaatiotekijän valintaa lukuun ottamatta kaikki loput kolmen ja neljän motivaatiotekijän valinnat tulivat kahdelta eri haastateltavalta.

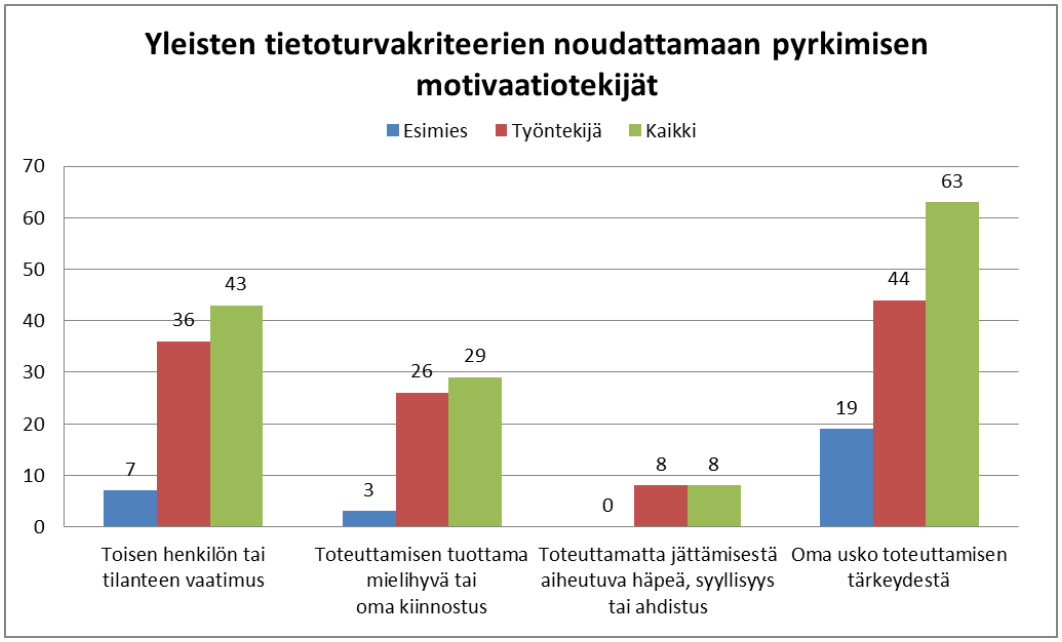
Kuviossa 4 on esitetty kaikkien haastattelussa käsiteltyjen tietoturvakriteerien noudattamaan pyrkimisen motivoivien tekijöiden mukaan jaoteltuna. Kahdeksan haastateltavaa valitsi 22 tietoturvakriteerille yhteensä 226 motivaatiotekijää. Selkeästi motivoivimmaksi tekijäksi on valittu oma usko toteuttamisen tärkeydestä 100 valinnalla, joka on 44 % kaikista motivaatiotekijöiden valinnoista. Toiseksi motivoivimmaksi on valittu toisen henkilön tai tilanteen vaatimus 77 valinnalla (34 %). Eroa on 10 %-yksikköä. Toteuttamisen tuottama mielihyvä tai oma kiinnostus on valittu 39 kertaa (17 %) ja toteuttamatta jättämisestä aiheutuva häpeä, syyllisyys tai ahdistus 10 kertaa (4 %).



Kuvio 4. Tietoturvakriteerien noudattamaan pyrkimisen motivaatiotekijät.

Kun kuvion 4 tuloksia tarkastellaan aseman mukaan, nähdään, että esimiehillä painottuu selkeästi oma usko toteuttamisen tärkeydestä -motivaatiotekijä 31 valinnalla, joka on 63 % esimiesten kaikista valinnoista. Toiseksi eniten (14 kertaa eli 29 %) esimiehet ovat valinneet motivaatiotekijäksi toisen henkilön tai tilanteen vaatimuksen. Muut vaihtoehtoina olleet motivaatiotekijät motivoivat esimiehiä vähän tai ei ollenkaan. Työntekijät ovat valinneet kaikkia neljää motivaatiotekijää. Myös työntekijöitä motivoi eniten oma usko toteuttamisen tärkeydestä, joka on valittu motivoivimmaksi tekijäksi 69 valinnalla (39 %), mutta ero toiseksi motivoivimpaan tekijään toisen henkilön tai tilanteen vaatimuksesta on vain kuusi valintaa 63 valinnalla (36 %). Myös toteuttamisen tuottama mielihyvä tai oma kiinnostus motivoi työntekijöitä, sillä se on valittu 35 kertaa, joka on 20 % työntekijöiden kaikista valinnoista. Toteuttamatta jättämisestä aiheutuva häpeä, syyllisyys tai ahdistus -motivaatiotekijäkin on tullut työntekijöillä valituksi yhteensä 10 kertaa.

Kuviossa 5 on esitetty yhteenveto haastatteluissa läpikäytyjen 14 yleisen tietoturvakriteerin noudattamaan pyrkimisen motivaatiotekijöiden jakautumisesta. Yhteensä näille 14 kriteerille haastatellut 8 työntekijää valitsivat 143 motivaatiotekijää. Kaikkien haastatelluiden vastauksissa oma usko toteuttamisen tärkeydestä on motivoivin 63 valinnalla (44 %) ennen toiseksi tullutta toisen henkilön tai tilanteen vaatimusta (43 valintaa eli 30 %). Kolmanneksi eniten motivoi toteuttamisen tuottama mielihyvä tai oma kiinnostus 29 valinnalla (20 %).



Kuvio 5. Yleisten tietoturvakriteerien noudattamaan pyrkimisen motivaatiotekijät.

Tarkasteltaessa tuloksia aseman mukaan, kuviosta 5 nähdään, että esimiehiä motivoi selkeästi eniten oma usko toteuttamisen tärkeydestä (19 valintaa eli 66 %). Seuraavaksi eniten esimiehiä motivoi toisen henkilön tai tilanteen vaatimus (7 valintaa eli 24 %). Toteuttamatta jättämisestä aiheutuvaa häpeää, syyllisyyttä tai ahdistusta esimiehet eivät valitse kertaakaan motivoivana tekijänä, ja toteuttamisen tuottaman mielihyvän tai oman kiinnostuksenkin vain kolme kertaa. Työntekijöillä motivaatiotekijöiden jakautuminen kolmen motivoivimman tekijän kesken on tasaisempaa. Oma usko toteuttamisen tärkeydestä motivoi myös työntekijöitä eniten 44 valinnalla, joka on 39 % työntekijöiden valinnoista, mutta työntekijät nimeävät vain kahdeksan valinnan erolla (36 valintaa eli 32 %) toiseksi eniten motivoivaksi tekijäksi toisen henkilön tai tilanteen vaatimuksen. Valintojen tasaisuudesta kertoo, että vielä kolmanneksikin eniten valittu toteuttamisen tuottama mielihyvä tai oma kiinnostus -motivaatiotekijä valitaan 26 kertaa (23 %). Toteuttamatta jättämisestä aiheutuvan häpeän, syyllisyyden tai ahdistuksen työntekijät valitsivat viiden eri kriteerin kohdalla yhteensä kahdeksan kertaa motivoivaksi tekijäksi pyrkiä kriteerin noudattamiseen. Haastattelujen tulokset yleisten tietoturvakriteerien noudattamaan pyrkimisen motivaatiotekijöistä kriteereittäin on esitetty taulukossa 24.

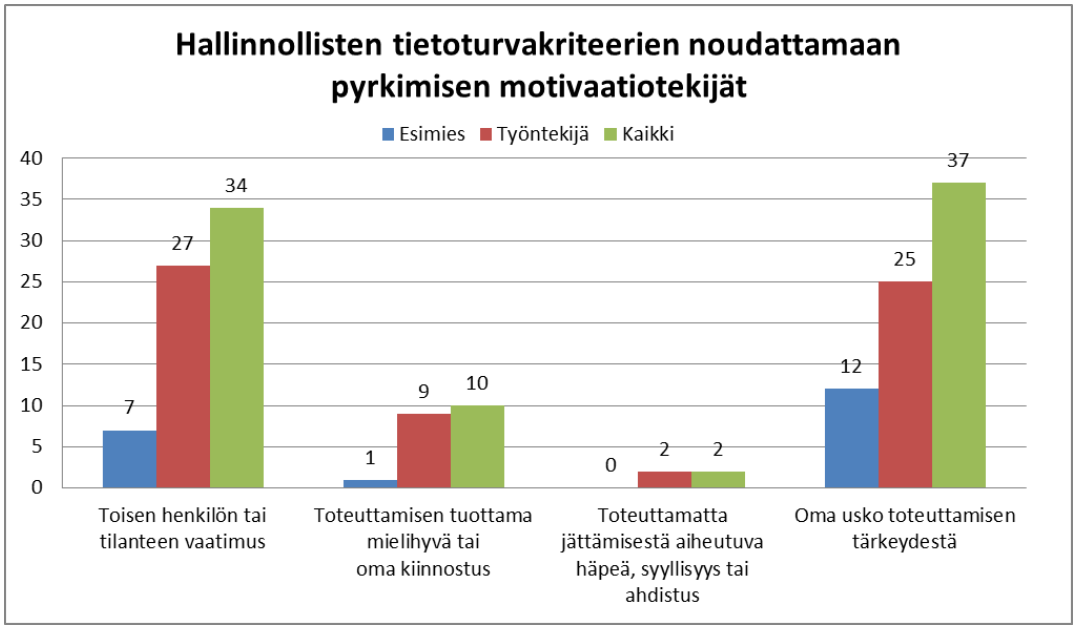
Taulukko 24. Yleisten tietoturvakriteerien noudattamaan pyrkimisen motivaatiotekijät.

	Decin ja Ryanin menetelmän motivointisyyt											
	Toisen henkilön tai tilanteen vaatimus			**Toteuttamisen tuottama mielihyvä tai oma kiinnostus**			**Toteuttamatta jättämisestä aiheutuva häpeä, syyllisyys tai ahdistus**			**Oma usko toteuttamisen tärkeydestä**		
Minä pyrin työtehtävissäni ymmärtämään/tukemaan, että	**Esimies**	**Työntekijä**	**Yhteensä**	**Esimies**	**Työntekijä**	**Yhteensä**	**Esimies**	**Työntekijä**	**Yhteensä**	**Esimies**	**Työntekijä**	**Yhteensä**
joku voi salakuunnella minua.	1	1	2		2	2		2	2	1	4	5
tietoturva on teknistä (20 %) ja hallinnollista (80 %) työtä.	2		2			0			0		5	5
tietoturva sisältyy perehdytykseen.		3	3	1	2	3		2	2	1	3	4
tiedolle laaditaan elinkaari.		3	3	1	2	3			0	1	3	4
tärkeä tieto salakirjoitetaan, jos siihen käsiksi pääseminen on mahdollista.	1	4	5		1	1			0	1	2	3
minä saan koulutusta yrityksen tietoturvakäytäntöihin.	1	3	4		2	2		1	1	2	5	7
minä saan tietoturvan sisältävää ohjausta ja ohjeita työhöni.		4	4		2	2		2	2	2	4	6
minun tietoturvaosaamistani kehitetään jatkuvasti.		3	3	1	4	5			0	1	2	3
minä tunnen yrityksen tietoturvatoimenpiteet.	1	2	3		3	3			0	1	2	3
tietoturvaa seurataan hallinnollisesti.		3	3			0		1	1	2	2	4
minä tiedän toimintatavat eri tietoturvatilanteissa.		4	4			0			0	2	4	6
vanhemmat kollegat toimivat hyvänä esimerkkinä tietoturvakäyttäytymisessä.		2	2		3	3			0	2	3	5
minä tiedän, mikä tieto on suojattavaa, missä se säilytetään ja kuka säilytystilaan pääsee.	1	2	3		3	3			0	1	3	4
minä tunnen yrityksen yleisen varmuuskopiointikäytännön.		2	2		2	2			0	2	2	4
Yhteensä	**7**	**36**	**43**	**3**	**26**	**29**	**0**	**8**	**8**	**19**	**44**	**63**

Taulukosta nähdään, että yhdenkään yleisen tietoturvakriteerin kohdalla ei ole valittu ainoastaan yhtä motivaatiotekijää. Kahdeksalle kriteerille on valittu kolme neljästä annetusta motivaatiotekijästä. Näistä vain yhdessä valitsematta jätetty motivaatiotekijä ei ole toteuttamatta jättämisestä aiheutuva häpeä, syyllisyys tai ahdistus. Kaikki motivaatiotekijät on valittu 4 kriteerille, jotka ovat ”joku voi salakuunnella minua”, ”tietoturva sisältyy perehdytykseen”, ”minä saan koulutusta yrityksen tietoturvakäytäntöihin” ja ”minä saan tietoturvan sisältävää ohjausta

ja ohjeita työhöni”. Kriteerien ”tietoturva on teknistä (20 %) ja hallinnollista (80 %) työtä” ja ”minä tiedän toimintatavat eri tietoturvatilanteissa” kohdalla on valittu kaksi motivaatiotekijää.

Kuviossa 6 on esitetty haastattelussa läpikäytyjen 8 hallinnollisen tietoturvakriteerin noudattamaan pyrkimisen motivaatiotekijöiden jakautuminen kokonaisuutena sekä jaoteltuna aseman mukaan esimiesten ja työntekijöiden motivaatiotekijöihin. Yhteensä motivaatiotekijöiden valintoja tehtiin 83 kappaletta. Kun tarkastellaan kaikkien haastateltujen vastauksia, kuviosta nähdään, että hallinnollisten tietoturvakriteerien noudattamaan pyrkimistä motivoivat keskenään lähes yhtä paljon oma usko toteuttamisen tärkeydestä (37 valintaa) sekä toisen henkilön tai tilanteen vaatimus (34 valintaa). Toteuttamisen tuottama mielihyvä tai oma kiinnostus motivoivat vain vähän (10 valintaa) ja toteuttamatta jättämisestä aiheutuva häpeä, syyllisyys tai ahdistus motivoi ainoastaan kahden kriteerin kohdalla.



Kuvio 6. Hallinnollisten tietoturvakriteerien noudattamaan pyrkimisen motivaatiotekijät.

Kun kuvion 6 tuloksia tarkastellaan aseman mukaan, huomataan, että esimiehillä oma usko toteuttamisen tärkeydestä on selkeästi painottunut (12 valintaa eli 60 %). Toiseksi eniten esimiehiä motivoi toisen henkilön tai tilanteen vaatimus, joka valittiin 7 kertaa (35 %). Muita motivaatiotekijöitä esimiehet pitävät vain vähän tai ei ollenkaan motivoivina. Työntekijöiden motivaatiotekijöinä korostuvat tasavertaisina kaksi tekijää: toisen henkilön tai tilanteen vaatimus valittiin 27 kertaa (43 %) ja oma usko toteuttamisen tärkeydestä 25 kertaa (40 %). Myös muut motivaatiotekijät saivat työntekijöiltä jonkin verran ääniä: toteuttamisen tuottama mie-

lihyvä tai oma kiinnostus 9 ääntä ja toteuttamatta jättämisestä aiheutuva häpeä, syyllisyys tai ahdistus 2 ääntä. Taulukossa 25 on esitetty hallinnollisten tietoturvakriteerien noudattamaan pyrkimisen motivaatiotekijät kriteereittäin.

Taulukko 25. Hallinnollisten tietoturvakriteerien noudattamaan pyrkimisen motivaatiotekijät.

	Decin ja Ryanin menetelmän motivointisyyt											
	Toisen henkilön tai tilanteen vaatimus			**Toteuttamisen tuottama mielihyvä tai oma kiinnostus**			**Toteuttamatta jättämisestä aiheutuva häpeä, syyllisyys tai ahdistus**			**Oma usko toteuttamisen tärkeydestä**		
Minä pyrin työtehtävissäni huomioimaan, että yrityksemme hallinnossa	**Esimies**	**Työntekijä**	**Yhteensä**	**Esimies**	**Työntekijä**	**Yhteensä**	**Esimies**	**Työntekijä**	**Yhteensä**	**Esimies**	**Työntekijä**	**Yhteensä**
osoitetaan selkeästi yrityksen johdon tuki tietoturvalle.	1	3	4		1	1			0	2	4	6
huomioidaan tietoturvajohtamisen laajuus.		4	4	1	1	2			0	1	3	4
huomioidaan tietoturvajohtamisen hyvä tietohallintotapa (IT Governance).	2	3	5		1	1			0	1	3	4
määritellään tietoturvan resursointi.		5	5			0			0	2	1	3
on toipumissuunnitelmat.		3	3		1	1			0	2	2	4
on menettelyt sidosryhmien tietoturvan hallintaan.	1	3	4		2	2			0	1	2	3
tietoturvan tavoitteita ja toteutumista seurataan ja arvioidaan.	2	3	5		2	2		1	1	1	5	6
pidetään yhteyttä asiakkaisiin ja sidosryhmiin tietoturvaa varten.	1	3	4		1	1		1	1	2	5	7
Yhteensä	**7**	**27**	**34**	**1**	**9**	**10**	**0**	**2**	**2**	**12**	**25**	**37**

Taulukosta nähdään, että viidelle kriteerille on valittu 3 motivaatiotekijää. Näissä kaikissa motivaatiotekijä toteuttamatta jättämisestä aiheutuvasta häpeästä, syyllisyydestä tai ahdistuksesta on ainoa valitsematta jätetty. Kaikki neljä motivaatiotekijää on valittu kahdelle kriteerille, jotka ovat ”tietoturvan tavoitteita ja toteutumista seurataan ja arvioidaan” ja ”pidetään yhteyttä asiakkaisiin ja sidosryhmiin tietoturvaa varten”. Yhdelläkään kriteerillä ei ole valittu vain yhtä motivaatiotekijää ja kaksi motivaatiotekijää on valittu vain kriteerille ”määritellään tietoturvan resursointi”.

5.6 Toisen haastattelututkimuksen toteutus

Viimeisenä empiirisenä tutkimuksena tehtiin Kahan työntekijöille toinen haastattelututkimus, joka oli kvalitatiivinen. Haastattelun tavoitteena oli selvittää mitkä tekijät vaikuttavat työntekijän motivaation syntymiseen ja muuttumiseen tietoturvakriteerien noudattamisessa. Haastattelu valittiin aineistonkeruumenetelmäksi, koska se mahdollisti motivaatiotekijöiden syntymisen ja muutosten syvällisen käsittelyn. Haastattelurungossa oli yhteensä 14 kysymystä (liite 7), joista kahdella ensimmäisellä kysymyksellä selvitettiin taustatietoina haastateltavan asema ja yritykseen töihintulovuosi. Lopuilla haastattelukysymyksillä 3–14 haettiin vastausta erityisesti tutkimuskysymyksiin mitkä tekijät vaikuttavat motivaation syntymiseen ja muuttumiseen tietoturvakriteerien noudattamisessa. Syntymiseen vaikuttavia tekijöitä etsittiin kolmella kysymyksellä, jotka olivat kysymys 3. Miksi tietoturvasta huolehtiminen on sinusta tärkeää?, kysymys 7. Mikä saa sinut kiinnostumaan tietoturvakriteerien noudattamisesta? Miksi? ja kysymys 11. Millaisissa tilanteissa pyrit erityisesti huomioimaan tietoturvan? Miksi?.

Motivaation muutosta ja muutokseen vaikuttavia tekijöitä selvitettiin kuudella kysymyksellä, jotka olivat kysymys 4. Miten motivaatiosi huomioida tietoturvaa on muuttunut sinulla siitä, kun tulit tähän yritykseen töihin? Mitkä tekijät ovat vaikuttaneet muutokseen?, kysymys 5. Onko motivaatiosi tietoturvan toteuttamiseen sinulla nyt heikompaa vai parempaa verrattuna aikaan ennen tässä yrityksessä työskentelyä? Miksi?, kysymys 6. Mitkä tekijät muuttavat sinun asennettasi tietoturvaa kohtaan? Miksi?, kysymys 8. Miten motivaatiosi tietoturvan huomioimiseen on muuttunut sinulla viimeisen 3 vuoden aikana? Mitkä tekijät ovat vaikuttaneet muutokseen? Miksi?, kysymys 9. Miten motivaatiosi tietoturvan huomioimiseen on muuttunut sinulla 1v sitten tehdyn tietoturvakyselyni jälkeen? Mitkä tekijät ovat vaikuttaneet muutokseen? ja kysymys 10. Onko motivaatiosi tietoturvan toteuttamiseen sinulla nyt heikompaa vai parempaa verrattuna tilanteeseen ennen kyselyäni? Mistä tämä johtuu?.

Motivaation muuttumiseen liittyen laadittiin lisäksi kolme kysymystä, joilla selvitettiin tarkemmin erityisesti motivaation paranemiseen tai heikkenemiseen vaikuttavia tekijöitä. Motivaation paranemiseen liittyen laadittiin kysymys 12. Mitkä tekijät lisäävät sinun motivaatiota tietoturvan toteuttamisessa? Mistä tämä johtuu? Motivaation heikkenemiseen liittyi kysymys 13. Mikä saisi sinut toimimaan tietoisesti tietoturvaohjeiden vastaisesti? Miksi? ja kysymys 14. Mitkä tekijät vähentävät sinun motivaatiota tietoturvan toteuttamisessa? Miksi?.

Kaikki kysymykset haluttiin pitää mahdollisimman avoimina, eikä niiden vastausmahdollisuutta rajattu millään tavoin. Tällä tavoin haluttiin pyrkiä mahdolli-

simman syvällistä tietoa etsivään tutkimukseen. Haastattelun kysymysten ymmärrettävyys varmistettiin haastattelurungon laatimisen jälkeen yhdellä yrityksestä satunnaisesti valitulla työntekijällä, joka luki kysymykset läpi. Hän ymmärsi kaikki kysymykset eikä hän esittänyt minkäänlaisia ehdotuksia haastattelurungon muuttamiseksi. Työntekijä ei ollut myöhemmin haastateltavien joukossa.

Haastattelututkimus toteutettiin huhtikuussa 2014 yksilöhaastatteluna yrityksen tiloissa. Haastateltavat valittiin satunnaisesti numeron valitsevalla tietoteknisellä työkalulla yhdestä numeroidusta yrityksen kaikki vakinaiset työntekijät (esimiehet ja työntekijät, yhteensä 123 nimeä) sisältävästä nimilistasta, joka oli järjestetty sukunimen mukaan aakkosjärjestykseen. Haastattelussa oli alun perin varauduttu 10–15 haastattelun tekemiseen. Aluksi listoista valittiin viisi työntekijää. Tulokset olivat keskenään hyvin samankaltaisia. Haastatteluja tehtiin vielä kaksi lisää. Näidenkin haastattelujen tulokset jatkoivat tulosten toistoa, jolloin todettiin saturaation saavuttaminen ja haastattelut lopetettiin. Yhteensä haastatteluja tehtiin seitsemän. Kenenkään haastatellun työntekijän toimenkuva ei liittynyt suoraan tietotekniikkaan. Kaikki haastattelut tehtiin yhden päivän aikana yhden ja saman henkilön toimesta. Haastateltavat saivat tiedon haastattelusta haastattelua edeltävällä viikolla. Haastateltavat eivät saaneet haastattelukysymyksiä tietoonsa etukäteen. Haastattelutilanteessa kysymykset esitettiin ainoastaan suullisesti. Yhteen haastatteluun kulunut aika vaihteli 20 ja 35 minuutin välillä.

Käytännössä haastattelu eteni samalla tavoin kaikissa haastattelutilanteissa. Haastattelun teema ja näkökulma oli valittu etukäteen, minkä takia kaikille haastateltaville esitettiin samat kysymykset. Haastattelurungolla pyrittiin varmistamaan, että kaikkien haastateltavien kanssa käydään läpi samat asiat. Haastattelun alussa haastateltavalle kerrottiin liitteen 7 alussa esitetty esipuhe suullisesti.

Haastatteluista kirjoitettiin haastattelun aikana muistiinpanot, kustakin haastattelusta oma muistiinpanonsa. Muistiinpanoihin kirjattiin huolellisesti kaikki haastateltavien vastaukset. Muistiinpanot kirjoitettiin puhtaaksi tekstinkäsittelyohjelmalla haastattelua seuraavana päivänä. Tutkimustulosten esittelyssä kerrotaan muistiinpanoihin kirjatut vastaukset. Omien asenteiden ei annettu millään tavoin vaikuttaa kerrottaviin tuloksiin. Kussakin haastattelussa tehdyt muistiinpanot käytiin huolellisesti läpi kaksi kertaa, jotta varmistuttiin siitä, että kaikki vastaukset ovat varmasti esitelty. Tulokset raportoitiin niin, ettei yksittäistä vastaajaa voida tunnistaa.

5.7 Tulokset motivaation syntymiseen ja muuttumiseen vaikuttavista tekijöistä tietoturvakriteerien noudattamisessa

Kaikki seitsemän haastateltua henkilöä olivat työntekijä-tason työntekijöitä. He olivat tulleet yritykseen töihin vuosien 2003 ja 2008 välillä. Kysymykset 3–14 olivat motivaation syntymiseen ja muuttumiseen vaikuttavia tekijöitä selvittäviä kysymyksiä.

Kysymyksessä kolme haluttiin tietää, miksi vastaaja kokee tietoturvasta huolehtimisen tärkeäksi. Kuusi vastaajaa mainitsi vastauksessaan sanan tieto. Esiin nousivat asiakas- ja tuotetietojen suojaamisen tärkeys. Kolmessa vastauksessa tieto nähtiin arvokkaana omaisuutena. Asiakastiedoissa kaksi vastaajaa halusi huolehtia yksityisyyden suojasta. Asiakas- ja tuotetietoja haluttiin suojata myös kilpailijoilta (3 vastaajaa). Lisäksi kahdessa vastauksessa tietoturvan huolehtiminen koettiin tärkeäksi virusten uhkan takia.

Kysymyksessä neljä kysyttiin, miten vastaajan motivaatio huomioida tietoturvaa on muuttunut siitä, kun hän on tullut kyseiseen yritykseen töihin, ja mitkä tekijät ovat vaikuttaneet muutokseen. Kuusi vastaajaa ilmoitti, että motivaatio huomioida tietoturvaa ei ole muuttunut mitenkään. Näistä neljä vastaajaa totesi, että tietoturvasta huolehtiminen on ollut aina hyvällä tasolla ja kaksi vastaajaa lisäsi, että tietoturva on ollut aina tärkeänä osana työtehtäviä. Kaksi vastaajaa totesi myös, että tietokoneella työskentely tarkoittaa automaattisesti velvollisuutta huolehtia tietoturva-asioista. Näistä toinen vastaaja toi syynä esille, että kaikesta tietokoneella tehdystä jää jälki. Vain yksi vastaaja kertoi, että motivaatio huomioida tietoturvaa on muuttunut kyseiseen yritykseen tulon jälkeen. Ennen yritykseen tuloa hän oli työskennellyt ulkomailla, missä tietoturvasta huolehtiminen oli erilaista. Vastaaja koki, että tietoturvasta huolehtiminen on Suomessa kaikkien työntekijöiden velvollisuus. Lisäksi hänen mielestään Suomessa myös puhutaan tietoturvasta enemmän.

Viidennessä kysymyksessä vastaajan haluttiin kertovan, onko motivaatio tietoturvan toteuttamiseen hänellä nyt heikompaa vai parempaa verrattuna aikaan ennen kyseisessä yrityksessä työskentelyä. Lisäksi vastaajaa pyydettiin pohtimaan mistä muutos johtuu. Kukaan vastaajista ei sanonut, että motivaatio tietoturvan toteuttamiseen olisi nyt heikompaa. Kaksi vastaajaa totesi, että motivaatio ei ole muuttunut heikompaan eikä parempaan suuntaan, vaan on pysynyt samana. Molemmat vastaajat lisäsivät, että yrityksen tietotekniikkaosasto huolehtii tietoturvaan liittyvistä isoista asioista ja heidän vastuullensa jää huolehtia tietoturvan perusteiden toteuttaminen omissa työtehtävissä. Viisi vastaajaa kertoi, että motivaatio tieto-

turvan toteuttamiseen on nyt parempaa. Näistä neljä toi perusteluna esille, että tietoturva on aiheena yleisesti enemmän esillä kuin aiemmin. Esimerkiksi eräs vastaaja totesi, että ”*tietoturvasta puhutaan yleisesti nyt enemmän*”. Kaksi perusteli motivaation muutosta tietokoneiden kehittymisellä, kolme toi esille jäljen jäämisen tiedon sähköisestä käsittelystä ja yksi perusteli parempaa tietoturvan toteuttamisen motivaatiota hakkeroinnin uhkalla. Viidestä vastaajasta, joiden mielestä tietoturvan toteuttamisen motivaatio on nyt parempaa, kolme toi tärkeänä esille tietotekniikkaosaston merkityksen tietoturvan toteuttamisen motivoivana tekijänä.

Kysymyksessä kuusi kysyttiin mitkä tekijät muuttavat vastaajan asennetta tietoturvaa kohtaan ja miksi. Viisi vastaajaa ilmoitti, että asenteeseen vaikuttavat tieto uhkista ja tietoturvariskeistä. Näistä kaksi vastaajaa lisäsi saavansa tietoa mediasta. Neljä vastaajaa toi esille, että luottaa siihen, että yritys huolehtii ja tiedottaa tietoturva-asioista. Esimerkiksi yhdessä vastauksessa todetaan: ”*Kun lukee tietoturvariskeistä, muuttuu kotona oman tietokoneen käyttö varovaisemmaksi, mutta töissä luotan suojauksiin ja työkaluihin.*” Yksi vastaaja toi esille, että esimerkiksi sähköpostissa on oltava varovaisempi, että millaisella tietosisällöllä sähköpostiin vastaa tai sen laittaa eteenpäin ja, että kenelle sähköpostin lähettää. Yksi vastaaja toi lisäksi esille, että mahdollinen epätietoisuus tietoturva-asioissa on epämiellyttävää.

Kysymyksessä seitsemän selvitettiin mikä saa vastaajan kiinnostumaan tietoturvakriteerien noudattamisesta ja miksi. Vastaukset jakautuvat kolmeen osaan. Kolme vastaajaa ilmoitti, että tietoturvasta huolehditaan jatkuvasti riittävällä tasolla, eikä mikään erityisesti saa siitä kiinnostumaan. Näistä kuitenkin kaksi vastaajaa toi esille, että jos yritys tiedottaa jostakin tietoturvauhkasta, huomioi hän luonnollisesti asian, mutta se ei varsinaisesti lisää hänen kiinnostustaan asiaan. Kaksi vastaajaa ilmoitti, että tietoturvakriteerien noudattamisesta saa kiinnostumaan halu suojata tietoja. Kaksi vastaajaa ilmoitti, että kiinnostumaan saa tarve tehdä jokin työtehtävä mihin tietoturvasuojaukset eivät anna lupaa. Näistä toinen vastaajaa toi esille, että tällöin on pakko selvittää, että mitä tulee tehdä, jotta kyseisen työtehtävän saa tehtyä. Hän myös jatkoi, että onneksi tietotekniikkaosasto on näissä tilanteissa aina halukas auttamaan työntekijää.

Kahdeksannessa kysymyksessä selvitettiin miten motivaatio tietoturvan huomioimiseen on muuttunut vastaajalla viimeisen kolmen vuoden aikana, mitkä tekijät ovat vaikuttaneet muutokseen ja miksi. Kaikki seitsemän haastateltavaa olivat jo tuolloin kyseisessä yrityksessä töissä. Kolme vastaajaa kertoi, että tietoturvan huomioimisen motivaatio ei ole muuttunut mitenkään, vaan on pysynyt samana. Näistä yksi vastaajaa lisäsi, että motivaatio tietoturvan huomioimiseen on hänellä

ollut aina hyvällä tasolla. Neljä vastaajaa toi esille, että laitteiden muutos on vaikuttanut tietoturvan huomioimisen motivaatioon. Näistä yhdessä vastauksessa todetaan: ”*Eri laitteet, kaikissa pitää tietoturvasta huolehtia*” ja kaksi vastaajaa mainitsi älypuhelimen, joka oli jaettu yrityksen työntekijöille. Jälkimmäisistä yksi vastaaja kertoi, että ”*Täytyy olla tarkka, että puhelin ei jää tai katoa minnekään etenkään ilman näppäinlukkoa, kun sillä pystyy lukemaan esimerkiksi työsähköpostin*”. Yhdessä vastauksessa todettiin, että ”*Salasanasuojaus on ollut ikuisesti*”. Yksi vastaaja kertoi, että nykyään hän lukee paremmin ohjelmalatausten kysymykset ja miettii aidosti, mitä niihin pitää vastata. Yksi vastaaja toi syynä esille yrityksessä tapahtuneen ison muutoksen tuotetarjonnassa, minkä takia tuotetietojen kanssa täytyi olla erityisen huolellinen.

Kysymys yhdeksän liittyi tätä tutkimusta varten yrityksessä vuotta aiemmin (helmikuussa 2013) tehtyyn kyselytutkimukseen. Kysymyksessä haluttiin tietää miten vastaajan motivaatio tietoturvan huomioimiseen on muuttunut vuosi sitten tehdyn tietoturvakyselyn jälkeen ja mitkä tekijät ovat vaikuttaneet muutokseen. Tähän kysymykseen vastasi vain kuusi haastateltavaa, sillä yksi haastateltava oli ollut kyselytutkimuksen aikaan hetkellisesti poissa yrityksen palveluksesta eikä hänelle esitetty kysymystä yhdeksän lainkaan. Kuudesta vastaajasta viisi ilmoitti, että motivaatio tietoturvan huomioimiseen ei ole muuttunut mitenkään. Myös kuudes vastaaja ilmoitti, että motivaatio tietoturvan huomioimiseen ei ole varsinaisesti muuttunut mitenkään, mutta kyselyn jälkeen hän oli keskustellut kyselyn asioista joidenkin kollegojensa kanssa, joten hän koki tulleensa jonkin verran kiinnostuneemmaksi tietoturva-asioista kyselyn jälkeen. Kollegoiden kanssa keskustelun aiheina olivat olleet yrityksen tietoturvatiedotuksen ja yleisen tietoturvasta keskustelun vähäisyys sekä työtietokoneen kotikäytön tietoturvariskit. Keskusteluissa oli tullut myös esille, että kyselyssä oli jonkin verran vaikeita kysymyksiä ja työntekijät olivat pohtineet, tulisiko heidän tietää kyseisistä asioista enemmän.

Myös kysymys 10 liittyi aiempaan kyselytutkimukseen. Kysymyksessä haluttiin tietää onko vastaajan motivaatio tietoturvan toteuttamiseen nyt heikompaa vai parempaa verrattuna tilanteeseen ennen kyselyä ja mistä se johtuu. Tähänkin kysymykseen tuli vain kuusi vastausta, koska kysymystä ei esitetty yhdelle haastateltavalle lainkaan, koska hän ei ollut osallistunut aiempaan kyselytutkimukseen. Kaikki kuusi haastateltavaa totesivat, että tietoturvan toteuttamisen motivaatiotaso ei ole muuttunut mitenkään, vaan on säilynyt samana. Kolme vastaajaa lisäsi, että tietoturvan toteuttaminen oli jo ennestään hyvällä tasolla. Yksi vastaajista totesi, että ”*Esimerkiksi yrityksen laatuvastaavat kävivät kyselyn tulokset läpi, eikä siitä seurannut yrityksessä mitään isompia muutoksia tietoturvan huomioimiseen, vaan työ on jatkunut samanlaisena*”.

Kysymyksessä 11 kysyttiin millaisissa tilanteissa vastaaja pyrkii erityisesti huomioimaan tietoturvan ja miksi. Seitsemästä vastaajasta yksi ei keksinyt mitään sellaista tilannetta, jossa hän huomioisi tietoturvan jotenkin erityisemmin. Kuudesta vastaajasta viisi mainitsi huomioimisen syynä tietojen suojaamisen. Esimerkiksi eräässä vastauksessa todettiin, että ”*tieto on arvokasta omaisuutta, arkaluontoista*”. Sähköposti tuli esiin kolmen haastateltavan vastauksessa, joista kaksi mainitsi sähköpostin ketjutuksen (ts. takaisin- ja edelleenlähetyksen) ja yksi sähköpostin tietosisällön (esimerkiksi oikea tilausnumero) vaativan aina tietoturvan tarkkaa huomioimista. Kaksi vastaajaa mainitsi henkilöstöasioiden vaativan tietoturvan tarkkaa huomioimista. Yksi vastaaja kertoi, että, jos hänellä on yrityksessä vieraita, hän huomioi aina, että pöydillä ei ole esillä mitään arkaluontoista materiaalia.

Kysymyksessä 12 vastaajaa pyydettiin kertomaan mitkä tekijät lisäävät motivaatiota tietoturvan toteuttamisessa ja mistä se johtuu. Kaksi haastateltavaa ei osannut nimetä mitään tietoturvan toteuttamisen motivaatiota lisäävää tekijää. Neljä haastateltavaa nosti esiin tietoturvasta puhumisen tai tiedottamisen lisäävän tietoturvan toteuttamisen motivaatiota. Näistä kaksi totesi syyksi, että, jos yritykseltä tulee tietoturvaan liittyvä tiedote, tarkoittaa se käytännössä todellista uhkaa, johon tulee reagoida. Yksi haastateltava totesi, että ”*motivaation luo se fakta, että tietoturvaa pitää noudattaa*”. Lisäksi yksi vastaaja ilmoitti, että ”*motivaatiota lisää se, että työ pitää saada tehtyä tehokkaast*i”.

Kysymykseen 13, jossa kysyttiin mikä saisi vastaajan toimimaan tietoisesti tietoturvaohjeiden vastaisesti ja miksi, tuli hyvin yksipuoleiset vastaukset. Kaikki haastateltavat sanoivat, että ei ole mitään sellaista asiaa, joka saisi hänet toimimaan tietoisesti tietoturvaohjeiden vastaisesti. Näistä yksi haastateltava esitti vastauksen muodossa, että hän ”*ei uskalla toimia tietoturvaohjeiden vastaisesti*”. Yksi haastateltava lisäsi vastauksessaan, että ”*haluan noudattaa ohjeita, koska taustalla on aina syy, eikä niitä ole tehty kiusalla*”. Kaksi vastaajaa lisäsivät vastauksessaan, että he toimisivat tietoturvaohjeiden vastaisesti, jos ylemmät esimiehet määräisivät toimimaan niin. Lisäksi yksi vastaaja totesi pitkän pohdinnan jälkeen, että ”*ehkä jokin työtehtäviin liittyvä pakollinen juttu, esimerkiksi luvattoman ohjelman lataus työtehtäviä varten, voisi olla sellainen, mutta senkin tekemistä pyrkisin ensin varmistamaan tietotekniikkaosastolta*”. Kaksi vastaajaa sanoi, että hän ei toimisi missään tilanteessa tietoisesti tietoturvaohjeiden vastaisesti, koska pelkää seuraamuksia. Näistä toinen pohti, että ”*siitä tulisi varmaan potkut*”.

Viimeisessä kysymyksessä 14 kysyttiin mitkä tekijät vähentävät vastaajan motivaatiota tietoturvan toteuttamisessa ja miksi. Seitsemästä haastatellusta neljä vas-

taajaa totesi, että ei ole olemassa mitään tietoturvan toteuttamisen motivaatiota vähentävää tekijää. Näistä neljästä vastaajasta kaksi täsmensi syyksi tietoturvatietojen päivittämisen, esimerkiksi toinen vastasi, että ”*tietoturva-asioissa on pysyttävä ajan tasalla*”. Kolme vastaajaa vastasi, että tietoturvan toteuttamisen motivaatiota vähentää, jos tietoturva estää, vaikeuttaa tai hidastaa varsinaisen työn tekoa. Esimerkkinä mainittiin tilanne, jossa ei ole oikeuksia tehdä jotakin päivitystä tai muuta työtehtävän vaatimaa asiaa. Lisäksi esimerkkinä mainittiin tilanne, jossa ei ole oikeuksia päästä johonkin hakemistoon tai näkemään jotakin tietoa. Yksi vastaaja totesi, että ”*tietotekniikkaosasto huolehtii tietoturva-asioista hyvin*”.

6 KESKUSTELUA

Tämän tutkimuksen peruskäsitteitä ovat olleet *tietoturva*, *tietoturvakriteeri* ja *motivaatio*. Niitä täsmennettiin tutkimuksen luvuissa 2 ja 3. Tietoturvan käsittelyssä keskityttiin erityisesti hallinnollisen tietoturvan kuvaamiseen. Motivaatiota tarkasteltiin teorioiden ja työssä oppimisen näkökulmista.

Tutkimusote oli sekä kvantitatiivinen että kvalitatiivinen. Tutkimuksessa etsittiin vastauksia seuraaviin tutkimuskysymyksiin: mitä tietoturvakriteerejä Suomessa julkaistut ohjeet sisältävät, millä tasolla työntekijät pyrkivät noudattamaan tietoturvakriteerejä, mitkä tekijät motivoivat työntekijöitä heidän pyrkiessä noudattamaan tietoturvakriteerejä, mitkä tekijät vaikuttavat motivaation syntymiseen tietoturvakriteerien noudattamisessa ja mitkä tekijät vaikuttavat motivaation muuttumiseen tietoturvakriteerien noudattamisessa. Tutkimuksen empiirisessä osassa tutkimuskysymyksiin etsittiin vastauksia dokumenttiaineistosta, kyselyllä ja haastatteluilla.

Seuraavassa pohditaan tämän väitöskirjatutkimuksen tulosten merkitystä tieteen ja käytännön kannalta, sekä esitetään käytännön suosituksia. Keskustelun kohteena ovat myös tutkimuksen rajoitukset. Lopuksi esitetään jatkotutkimusaiheita.

6.1 Tulosten tieteellinen merkitys

Tässä luvussa tarkastellaan tulosten tieteellistä merkitystä tutkimuskysymyksittäin.

1. tutkimuskysymys: Mitä tietoturvakriteerejä Suomessa julkaistut ohjeet sisältävät?

Tutkimuksessa vastattiin ensin tutkimuskysymykseen *mitä tietoturvakriteerejä Suomessa julkaistut ohjeet sisältävät.* Tällaisen analyysin tekeminen nähtiin tärkeäksi ja hyödylliseksi yrityksille, koska yrityksillä ei ole välttämättä aikaa käydä läpi laajoja dokumentteja. Tutkijoille ja tietoturvan kehittäjille analyysillä halutaan osoittaa viranomaisten ohjeistusten nykytila. Tutkimuskysymykseen vastattiin laajasti luvussa 4. Yhteenvetona ja vastauksena tutkimuskysymykseen muodostettiin 81 tietoturvakriteeriä kohdassa 5.1 (liite 2).

Tutkimuksen tuloksena todetaan, että suomalaisia pk-yrityksiä ohjeistavia tahoja ja ohjeistuksia on paljon, ja niiden kaikkien huomioiminen ja toteuttaminen yrityksissä on käytännössä vähintäänkin haastavaa. Laaksonen ja muut (2006: 21) ovat aiemmin todenneet, että yritykset kaipaavat viranomaisilta ohjeistuksia ja

selviä suosituksia mitä toimenpiteitä yrityksessä tulisi ja saisi tehdä, jotta tietoturvan ylläpitäminen ja parantaminen toteutuisi. Yritykset haluavat olla myös varmoja, että yrityksen toimenpiteet ovat lainmukaisia ja tehokkaita heidän pyrkiessä tavoitteisiin. Suomalaisten viranomaisten yrityksille tarjoamia tietoturvaohjeistuksia ei ole tutkittu tieteellisesti lainkaan. Kull (2012) tutki 29 Euroopan maan tietotekniikka-alalle asettamia sääntövaatimuksia. Tietoturvaan liittyen ainoastaan sääntövaatimukset tietoturvapolitiikalle oli määritelty tutkituissa maissa kohtalaisesti: 14 maassa perusteellisesti ja kahdessa maassa jotenkuten. Seitsemässä maassa ei tietoturvapolitiikkaa mainittu säännöissä lainkaan.

Suomalaisia pk-yrityksiä ohjeistavia tahoja on lukuisia ja huomioon otettavia ohjeistuksia on paljon. Tutkimuksessa esiteltiin 16 ohjeistavaa tahoa ja heiltä 8 julkaistua ohjeistusta. Näistä neljä oli sellaisia, että niiden läpikäynti perusteellisesti oli mahdollista. Ohjeistuksista keskeisimpiä voidaan lakien ja asetusten lisäksi nimetä esimerkiksi vuoden 2009 lopussa voimaan tullut Kansallinen turvallisuusauditointikriteeristö (KATAKRI) sekä elinkeinoelämän hyödynnettäväksi tarkoitettu VAHTI-ohjeistus, joka käsittää 46 voimassa olevaa ohjeistusta vuosilta 2000–2012.

Höne ja Eloff (2002a) ovat tutkimuksessaan esittäneet, että ohjeistukset sisältävät usein termejä, jotka ovat vaikeasti ymmärrettäviä. Ohjeet usein myös kirjoitetaan liian teknisestä näkökulmasta. Tämän tutkimuksen tulokset vahvistavat jossain määrin näitä näkemyksiä. Haastattelussa 22 läpikäydystä kriteeristä yhdeksän kriteerin kohdalla vähintään yksi haastateltava kysyi ensireaktiona kriteerin tai sen termin merkitystä. Selitystä kaivattiin eniten termille hyvä tietohallintotapa (IT Governance) (6 haastateltavaa). Toipumissuunnitelma-termin sekä teknisen ja hallinnollisen työn kohdalla 3 haastateltavaa kysyi mitä ilmaisulla tarkoitetaan. ”Tietoturvan tavoitteita ja toteutumista seurataan ja arvioidaan” -kriteerille pyydettiin selitystä 2 kertaa. Lisäksi tarkentavaa termiselitystä pyydettiin yhden kerran viiden kriteerin kohdalla. Laaditut tietoturvakriteerit ovat kuitenkin pääosin työntekijöille tuttuja ja ymmärrettäviä. Työntekijät myös tuntevat tietoturvakriteerien termit. Suurin osa esiin tulleista ilmaisujen tuntemattomuudesta voi johtua siitä, että termejä käyttävät pääasiassa esimiehet. Kuitenkin esimerkiksi toipumissuunnitelma-termi tulisi olla kaikkien työntekijöiden tiedossa. IT Governance -termin laaja tuntemattomuus johtunee siitä, että termi on pääasiassa esimiesten käytössä. Termille ei myöskään ole olemassa vielä virallista vakiintunutta suomennosta. *Johtopäätöksenä* todetaan, että tietoturvakriteerin noudattamattomuuden ei voida katsoa johtuvan työntekijöille vieraasta käsitteistöstä aiheutuvista ongelmista. Huomioitavaa kuitenkin on, että ohjeissa käytettävä termistö on erittäin kirjava.

2. tutkimuskysymys: Millä tasolla työntekijät pyrkivät noudattamaan tietoturvakriteerejä?

Seuraavaksi tutkimuksessa vastattiin tutkimuskysymykseen *millä tasolla työntekijät pyrkivät noudattamaan tietoturvakriteerejä?* Tutkimuskysymyksen asettelussa huomioitiin Ajzenin (1985) suunnitellun toiminnan teoriaa, jonka mukaan aikomuksen määrä on suhteessa tehtävästä suoriutumisen todennäköisyyteen. Vastauksen saamiseksi toteutettiin kvantitatiivinen kyselytutkimus, joka tuki Nurmen ja Salmela-Aron (2005: 23) mukaista modernin motivaatioteorian ajatusta motivaation tutkimisesta tavoitteiden näkökulmasta. Kyselytutkimuksen pohjana käytettiin luotuja tietoturvakriteerejä, jotka kirjoitettiin tavoitteen muotoon. Kyselyssä keskityttiin hakemaan vastausta erityisesti tavoitteiden toteuttamispyrkimyksen eli motivaation tasolle sen sijaan, että olisi selvitetty käytännön toteuttamisen tasoa.

Cox ja muut (2001) totesivat tutkimuksessaan, että ihmisen käyttäytyminen on keskeinen ja kriittinen tekijä tietoturvalle. Tämän tutkimuksen tuloksista on nähtävissä, että työntekijät ymmärtävät olevansa uhka tietoturvalle. 46 kyselyyn vastanneesta 58 työntekijästä (79 %) kertoi pyrkivänsä melko usein tai lähes aina huomioimaan, että työntekijä ja inhimillinen toiminta ymmärretään tietoturvan suurimpana uhkana.

Useat aikaisemmat tutkimukset ovat osoittaneet, että suomalaisten yritysten tietoturvan taso ei ole kovinkaan hyvä (mm. Partanen 2005). Yritysten yksi keskeinen ongelma on, että työntekijät laiminlyövät yrityksen tietoturvakäytäntöjä (Karjalainen 2011). Yrityksissä ei ymmärretä työntekijän tietoturvatietoisuuden merkitystä (Puhakainen 2006). Myös yritysten tietoturvaohjeita noudatetaan heikosti. Työntekijöiden heikko tietoturvatietoisuus on merkittävin syy tietoturvaväärinkäytöksille. (Siponen ym. 2007; D'Arcy ym. 2009.) Keskeisimpänä vastauksena tutkimuskysymykseen voidaan todeta, että tutkimuksen kohteena olleessa yrityksessä työntekijöiden tietoturvatietoisuus oli hyvä. Työntekijät pyrkivät pääsääntöisesti noudattamaan tietoturvakriteerejä ja pyrkivät hyvään tietoturvan tasoon. Kaikki yrityksen työntekijät kattaneella kyselyllä kerätty aineisto ja sen pohjalta laaditut tulokset osoittavat, että tutkitussa yrityksessä *työntekijät pyrkivät noudattamaan tietoturvakriteerejä varsin laajasti ja tasokkaasti* omassa työssään. Kyselytutkimuksessa tutkituista 81 tietoturvakriteeristä 59 kriteerissä noudattamaan pyrkiminen oli kaikilla käytetyillä mittareilla mitattuna vähintäänkin melko hyvää. Tieteellisesti nämä tutkimustulokset poikkeavat aiempien tutkimusten tuloksista. Merkittävää on huomata, että yrityksen työntekijöiden tietoturvatietoisuus oli hyvä. Työntekijät ymmärsivät tietoturvakriteerien merkityksen ja tunsivat termistön. Työntekijät myös huomioivat työntekijän ja inhimillisen toiminnan tieto-

turvan suurimpana uhkana. Näillä seikoilla on varmasti tietoturvan tasoa parantava vaikutus. Laajemmin pohdittuna yrityksen hyvään tietoturvatasoon on varmasti vaikuttanut yleisesti parantunut hallinnollisen tietoturvan merkityksen näkyvyys ja huomioiminen sekä yrityksille suunnattujen tietoturvaohjeiden lisääntyminen.

Partasen (2005) tutkimuksessa todetaan, että hallinnollinen turvallisuus tulisi huomioida yrityksissä paremmin. Kyselytutkimuksessa tutkituista 81 tietoturvakriteeristä 22 kriteerin tuloksissa oli nähtävissä jonkinlaisia heikkoja noudattamisen piirteitä. Näistä yleisiä tietoturvakriteerejä oli 14 ja hallinnollisia 8. Yleisistä tietoturvakriteereistä oli 13 kriteerillä vähintään yhtenä heikon noudattamisen piirteenä en ollenkaan/melko harvoin -vastausten suuri määrä. Vain yksi kriteeri tuli valituksi heikosti noudattamaan pyrityksi pelkästään en osaa sanoa -vastausten suuren määrän takia. Heikosti noudattamaan pyrittynä piirteenä oli kaikilla hallinnollisilla tietoturvakriteereillä työntekijöiltä tulleiden en osaa sanoa -vastausten suuri määrä. Tutkimuksen kohteena olleessa yrityksessä hallinnollisten tietoturvan tason voidaan katsoa olevan kokonaisuutena hyvä. Kuitenkin en ollenkaan/melko harvoin -vastaajiin pystyttäisiin oletettavasti vaikuttamaan motivoimalla työntekijöitä tehokkaammin. Tällöin hallinnollisen tietoturvan taso voisi olla vieläkin parempi. Yrityksen hyvään hallinnollisen tietoturvan tasoon on varmasti vaikuttanut yleisesti lisääntynyt hallinnollisen tietoturvan merkityksen näkyvyys.

Aikaisemmissa tutkimuksissa on osoitettu, että työntekijän kulttuurilla, iällä ja sukupuolella on merkitystä tietoturvakäyttäytymiseen (Hovav & D'Arcy 2012). Kun tämän tutkimuksen keskeisiä tuloksia tarkastellaan aseman mukaan, voidaan todeta, että yleisten tietoturvakriteerien osalta työntekijän asemalla ei tutkimuksen mukaan ole merkittävää vaikutusta tietoturvakriteerien noudattamispyrkimyksen tasoon. Sen sijaan hallinnollisissa tietoturvakriteereissä asemasta johtuvaa vaikutusta on nähtävissä: esimiesten noudattamaan pyrkimisen taso on hallinnollisissa tietoturvakriteereissä huomattavasti parempaa kuin työntekijöillä, sillä tuloksissa kaikki hallinnollisten tietoturvakriteerien heikon noudattamaan pyrkimisen vastaukset tulivat työntekijöiltä. Tätä voidaan selittää hallinnollisten tietoturvakriteerien suuremmalla merkityksellä esimiehille kuin työntekijöille.

3. tutkimuskysymys: Mitkä tekijät motivoivat työntekijöitä heidän pyrkiessä noudattamaan tietoturvakriteerejä?

Seuraavaksi tutkimuksessa vastattiin tutkimuskysymykseen *mitkä tekijät motivoivat työntekijöitä heidän pyrkiessä noudattamaan tietoturvakriteerejä?* Motivaatiotekijöitä tutkittiin, jotta työntekijöille pystyttäisiin löytämään tehokkaammin motivoivia tekijöitä tietoturvan parantamiseksi. Vastauksen saamiseksi kerättiin aineisto sekä kvantitatiivisella että kvalitatiivisella haastattelulla. Haastattelussa

selvitettiin tietoturvakirjallisuudessa ja suomalaisille pk-yrityksille suunnatuissa tietoturvaohjeistuksissa esitettyjen tietoturvakriteerien noudattamiseen motivoivia tekijöitä Decin ja Ryanin teorian mukaan. Haastattelu tukee Nurmen ja Salmela-Aron (2005: 23) mukaista modernin motivaatioteorian ajatusta, jossa motivaatiota tutkitaan ihmisen tavoitteiden näkökulmasta määrittelemällä tavoitteet sekä arvioimalla niiden toteuttamismahdollisuuksia ja toteuttamisen tärkeyttä sekä selvittämällä millaisia tunteita tavoite herättää. Haastattelun rungoksi määriteltiin luotuihin tietoturvakriteereihin pohjautuvat tavoitteet ja tuloksissa keskityttiin tuomaan esille vastaajissa heränneet tunteet ja tavoitteiden tärkeys.

Motivaatiotekijöiden valinta Decin ja Ryanin menetelmän vaihtoehdoista oli kaikille haastateltaville helppoa jokaisen tarkastellun 22 tietoturvakriteerin kohdalla. Yksittäinen haastateltava nimesi pääsääntöisesti (keskimäärin 18 kriteerin kohdalla) vain yhden motivaatiotekijän. Kuitenkaan yhdellekään tietoturvakriteerille ei valittu kaikkien haastateltavien vastauksissa pelkästään yhtä noudattamaan pyrkimiseen motivoivaa tekijää.

Tietoturvakriteerien noudattamaan pyrkimisessä kaikkia työntekijöitä motivoi eniten *oma usko toteuttamisen tärkeydestä* sekä *toisen henkilön tai tilanteen vaatimus*. Aseman mukaan tarkasteltuna esimiehillä *oma usko toteuttamisen tärkeyteen* on selkein motivaatiotekijä noin 63 % osuudella. Työntekijä-asemassa olevia työntekijöitä motivoi vajaan 40 % osuudella sekä *oma usko toteuttamisen tärkeydestä* että *toisen henkilön tai tilanteen vaatimus*. Työntekijöitä motivoi vahvasti myös *toteuttamisen tuottama mielihyvä tai oma kiinnostus* 20 % osuudella. Toteuttamatta jättämisestä aiheutuva häpeä, syyllisyys tai ahdistus motivoi työntekijöitä vain vähän ja esimiehet eivät valitse sitä ollenkaan motivoivaksi tekijäksi.

Yleisten ja hallinnolliset tietoturvakriteerien välisessä motivaatiotekijöiden vertailussa sekä esimiehillä että työntekijöillä on havaittavissa, että toisen henkilön tai tilanteen vaatimus koetaan hallinnollisissa tietoturvakriteereissä enemmän motivoivana kuin yleisissä tietoturvakriteereissä.

Useissa tutkimuksissa on myös osoitettu, että parantamalla työntekijöiden tietoturvatietoisuutta voidaan vaikuttaa työntekijän motivaatioon ja sitä kautta tietoturvakäyttäytymiseen (mm. Aytes & Connolly 2003; Puhakainen 2006; Siponen ym. 2007). Motivaatio on järjestelmä, joka virittää ja ohjaa ihmisen käyttäytymistä. Mikään yksittäinen motivaatioteoria ei yleisesti hyväksytysti kuvaa yksiselitteisesti ihmisen toimintaa. Myöskään ei ole olemassa yhtä suurta yleisesti hyväksyttyä integroivaa motivaatioteoriaa. (Vartiainen & Nurmela 2005: 189; Ruohotie 1998: 50.) Tieteellisen psykologisen tutkimuksen tuloksena on osoitettu, että ihmisen toimintaan vaikuttaa tunneperäinen ja tietoperäinen motivaatio. Aiempien motivaatiotutkimusten yhteisenä tuloksena voidaan todeta, että motivaatiotekijöi-

tä on runsaasti ja niiden merkitys on erilainen eri ihmisille. Motivaatio voi syntyä ulkoisesti tai sisäisesti. Sisäinen motivaatio on yksilön aitoa kiinnostusta opittavana olevasta kohteesta, minkä takia se on tehokkaampaa. Ulkoinen motivaatio luodaan ärsykkeillä, joihin reagoimisen jälkeen tekijä palkitaan. Tämän takia ulkoinen motivaatio on melko lyhytkestoista. (Ruohotie 1998: 35–37; Kolb 1984: 77–78; Niitamo 2005: 40–41; Rasila & Pitkonen 2010: 12.)

Aikaisemmissa tutkimuksissa on osoitettu, että sisäisesti motivoivilla tekijöillä on huomattavasti edistävämpi vaikutus työntekijän tietoturvaohjeiden noudattamiseen kuin ulkoisesti motivoivilla tekijöillä (Son 2011). Tämän tutkimuksen tuloksena todetaan, että hyvään tietoturvakäyttäytymiseen motivoivat sekä sisäisen että ulkoisen motivaation tekijät tasavertaisesti. Kaikkien haastattelussa käsiteltyjen tietoturvakriteerien noudattamaan pyrkimisessä eniten valittu motivaatiotekijä oli *oma usko toteuttamisen tärkeydestä*, jonka osuus kaikista motivaatiotekijöiden valinnoista oli 44 %. *Oma usko toteuttamisen tärkeyteen* on selkeästi *sisäisesti motivoiva* tekijä, joka perustuu tunteisiin ja kuvastaa yksilön aitoa kiinnostusta opittavana olevasta kohteesta. Toiseksi eniten valittu motivaatiotekijä oli *toisen henkilön tai tilanteen vaatimus* (34 %). Tämän motivaatiotekijän voidaan katsoa olevan *ulkoisesti motivoiva* tekijä ja se pohjautuu pelkästään tietoon.

Motivaatiolla on suuri merkitys työtehtävistä suoriutumiseen (Lämsä & Hautala 2008: 90). Puhakaisen (2006) tutkimuksen mukaan tietoturvatietoinen ja tietoturvan toteuttamiseen motivoitunut työntekijä huomaa yrityksen toimintaa uhkaavat epäkohdat tietoturvassa sekä haluaa kehittää ja parantaa omaa työskentelyänsä ja tietoturvakäyttäytymistänsä. Ruohotie (1991: 87–89) pitää motivaatiota keskeisenä tekijänä oppimisen tapahtumiseksi. Motivaatio suuntaa oppijan aktiivisuutta oppimiseen sekä tukee oppimisen päämäärän ja tavoitteen saavuttamista. Motivaatioprosessissa merkityksellisiä ovat oppijan odotukset, uskomukset ja arvot. (Ruohotie 1998: 70–71.) Motivoituminen vaatii tavoitteita, joihin pääsemisestä kunkin työntekijän tulisi päättää henkilökohtaisesti. Asetettavien tavoitteiden tulisi täyttää viisi vaatimusta, jotka ovat realistisuus, haastavuus, houkuttelevuus, mitattavuus ja henkilökohtainen merkitys. Työntekijän tulisi itse tehdä päätös tavoitteeseen pääsemisestä, mutta johtohenkilöstön on motivoitava työntekijöitä. (Niermeyer & Seyffert 2004: 38, 42, 61–62; Rasila & Pitkonen 2010: 5–6.) Tämän tutkimuksen tulokset vahvistavat näitä näkemyksiä. Tutkitussa yrityksessä työntekijät ovat tietoisia tietoturvasta ja heillä on selkeät tietoturvan toteuttamiseen motivoivat tekijät: *oma usko toteuttamisen tärkeydestä* ja *toisen henkilön tai tilanteen vaatimus*.

Laaksosen ja muiden (2006: 249, 255) mukaan työntekijöille on tärkeää kertoa suositeltavien toimintatapojen perimmäiset syyt. Tutkimuksen tuloksissa tämä on

vahvasti nähtävissä, koska *oma usko toteuttamisen tärkeydestä* on eniten valittu motivaatiotekijä. Kun ja muiden (2009) tutkimuksen tuloksena esitettiin, että tietoturvan hallintajärjestelmän käyttöönotossa tärkeitä motivaatiotekijöitä olivat aiemmat onnistuneet kokemukset, dokumenttien saatavuus, kustannusten rajaaminen, organisaation oppiminen ja organisaatiokulttuuri. Merkittävää on huomata, että tässä tutkimuksessa tuloksissa korostuvat erityisesti *oma usko toteuttamisen tärkeydestä* sekä *toisen henkilön tai tilanteen vaatimus*, joita ei Kun ja muiden (2009) motivaatiotekijöistä löydy lainkaan. Tältä osin tämän tutkimuksen tulokset laajentavat aiempaa ymmärrystä tietoturvan toteuttamisen motivaatiotekijöistä. Tulokset poikkeavat myös jonkin verran Bulgurcun, Cavusoglun ja Benbasatin (2010) aiemmista tuloksista, joiden mukaan työntekijän pyrkimykseen tietoturvaohjeiden noudattamiseen vaikuttavat asenne, normatiiviset uskomukset ja oma mahdollisuus vaikuttaa asiaan, sillä viimeisin näistä ei nouse tämän tutkimuksen tuloksissa esille lainkaan. Selittävänä tekijänä voidaan jossain määrin nähdä strukturoitu tutkimusasettelu, jonka pohjana käytettiin Decin ja Ryanin motivaatiotekijäluokittelua, vaikkakin haastattelu antoi mahdollisuuden laajempaan vastaamiseen.

Työntekijän tulee omaksua tietoturvaohjeet työpaikalla, jolloin niiden opettelu on työpaikalla tapahtuvaa oppimista. Tällainen oppimisprosessi alkaa toimintaan sitoutumisesta ja tavoitteen määrittelystä. (Ruohotie 1998: 77, 131–133.) Työssä oppiminen on työyhteisön käytäntöjen sisäistämistä ja niihin osallistumista (Lave & Wenger 1991; Brown & Duguid 1991). Tutkimuksen tuloksissa kävi ilmi, että vastaajat toivovat perehdytystä tietoturvakäytäntöihin. Eräs haastateltava totesi, että ihmisten oletetaan tietävän tietoturva-asiat jo ennestään, mikä ei välttämättä pidä paikkaansa. Vanhempien kollegojen toimimista esimerkkinä pidettiin kriteerinä hyvänä, koska heiltä kysytään ja opitaan muitakin oman toimenkuvan asioita. Aiemmin tutkimuksissa on todettu, että tietoturva noudattamisen motivaatioon voidaan vaikuttaa kouluttamalla tietoturva-asioita ja saamalla henkilöt ymmärtämään tilanteen vakavuus (Cheolho ym. 2012).

Puhakainen (2006) esitti tutkimuksessaan, että työntekijät mieltävät tietoturvan yhä teknisenä asiana. Tämän tutkimuksen tuloksista käy ilmi, että tutkitussa yrityksessä työntekijät ovat ymmärtäneet hallinnollisen tietoturvan merkityksen melko hyvin. Tutkimuksessa muodostettiin kirjallisuuden ja viranomaistahojen ohjeistusten pohjalta kriteeri ”tietoturva on teknistä (20 %) ja hallinnollista (80 %) työtä”. Tutkimukseen osallistuneista 58 vastaajasta 35 vastaajaa piti kriteeriin pyrkimisen tasoaan vähintään melko hyvänä. Ainoastaan 8 vastaajaa ei pyrkinyt kriteerin noudattamiseen lainkaan tai pyrki noudattamaan sitä melko harvoin. 15 vastaajaa ei osannut määritellä omaa kriteerin noudattamaan pyrkimisen tasoaan. Haastattelussa kriteerin syvällisemmässä pohdinnassa lähes kaikki haastateltavat

totesivat, että prosenttiosuudet pitävät todennäköisesti melko hyvin paikkansa. Haastateltavat pitivät kriteerin merkityksen ymmärtämistä tärkeänä. Kriteerin motivoivin tekijä oli *oma usko toteuttamisen tärkeydestä*, joka valittiin 5 kertaa. Myös toisen henkilön tai tilanteen vaatimus -motivaatiotekijä tuli valituksi (2 kertaa). Aikaisemmista tutkimuksista poikkeavan tuloksen selittävänä tekijänä voidaan nähdä hallinnollisen tietoturvan merkityksen yleisesti parantunut ymmärrys.

Aikaisemmissa tutkimuksissa on todettu, että yrityksen tietokoneita käytetään työhön liittymättömään omaan henkilökohtaiseen tarpeeseen, mikä aiheuttaa haittaa yrityksen toiminnalle (mm. Anandarajan 2002; Tian, Shen & Wang 2010). On myös todettu, että työhön liittymätön Internetin käyttö häiritsee merkittävästi työntekijän keskittymistä ja työntekoa (mm. Lim, Teo & Loo 2002; D'Arcy & Hovav 2007). Tämän tutkimuksen tuloksissa ei ole löydettävissä saman suuntaisia tuloksia. Tutkimuksessa kyselyyn vastanneista 58 työntekijästä 57 vastasi pyrkivänsä noudattamaan melko usein tai lähes aina kriteeriä ”työtietokoneellani on tietyt käyttötarkoitukset ja -oikeudet”. Kaikki 58 vastaajaa pyrkivät noudattamaan ”minulla on vastuu käyttäjätunnuksillani tehdyistä asioista” -kriteeriä melko usein tai lähes aina. Lisäksi 50 vastaajaa ilmoitti pyrkivänsä huomioimaan melko usein tai lähes aina tietoturvan osana päivittäistä toimintaansa. Selittävänä tekijänä voidaan nähdä yrityksen työntekijöiden hyvä tietoturvatietoisuuden taso.

Aiemmissa tutkimuksissa on esitetty, että työntekijä saadaan noudattamaan tietoturvaohjeita, kun tietoturvaohjeet vastaavat työntekijän työtehtäviä. Lisäksi työntekijän on ymmärrettävä tietoturvaohjeiden sisältö ja merkitys suhteessa omiin työtehtäviinsä. (Puhakainen 2006; Pahnila ym. 2007; Siponen ym. 2007; Puhakainen & Siponen 2010; Siponen & Vance 2010; Vance 2010.) Tämän tutkimuksen tulokset vahvistavat näitä ajatuksia. Kyselyn tuloksissa vastaajat pyrkivät melko usein tai lähes aina ymmärtämään tietoturvan osana yrityksen liiketoimintaa (83 % vastaajista) ja kiinteänä ja keskeisenä osana koko yrityksen toimintaa (90 %). Saman verran vastaajia (86 %) pyrki melko usein tai lähes aina huomioimaan tietoturvan osana päivittäistä toimintaansa. Tutkimuksessa havaittiin, että työntekijöille tietoturvakriteerit ovat käytännönläheinen ja jokapäiväinen osa omaa toimenkuvaa. Tämä näkyy välittömänä pyrkimyksenä arvioida tietoturvakriteerien toteuttamisen tasoa kriteereistä keskusteltaessa silloinkin, vaikka heiltä ei sitä pyydetä.

Herath ja Rao (2009a) ovat aiemmin todenneet, että tietoturvakäyttäytymiseen voidaan vaikuttaa sekä sisäisen että ulkoisen motivoinnin keinoin vaatimalla noudattamaan sääntöjä ja seuraamalla toimintaa. Tämän tutkimuksen tulokset vahvistavat näkemystä, sillä myös tämän tutkimuksen tuloksena todetaan, että työntekijää motivoivat sekä sisäiset että ulkoiset tekijät.

Tutkimuskysymyksen *mitkä tekijät motivoivat työntekijöitä heidän pyrkiessä noudattamaan tietoturvakriteerejä* vastausten keskeisinä *johtopäätöksinä* voidaan todeta, että työntekijät on helppo motivoida noudattamaan tietoturvakriteereitä. Motivointiin voidaan käyttää erilaisia sekä sisäisen että ulkoisen motivoinnin keinoja. Työntekijät saadaan sisäisesti motivoitumaan tietoturvakriteerien noudattamiseen, kun heidät saadaan ymmärtämään tietoturvakriteerin toteuttamisen tärkeys. Tutkimuksen mukaan työntekijät hyväksyvät myös ulkoisen motivoinnin keinot, jos esimerkiksi toinen henkilö tai tilanne vaatii kriteerin noudattamista. Tämän takia, vaikka sisäisten motivointikeinojen käyttäminen on tehokkaampaa, tulisi yrityksissä käyttää myös ulkoisen motivoinnin keinoja tietoturvakriteerien noudattamisvaatimuksissa.

4. ja 5. tutkimuskysymys: Mitkä tekijät vaikuttavat motivaation syntymiseen tietoturvakriteerien noudattamisessa ja mitkä tekijät vaikuttavat motivaation muuttumiseen tietoturvakriteerien noudattamisessa?

Lopulta tutkimuksessa vastattiin tutkimuskysymyksiin *mitkä tekijät vaikuttavat motivaation syntymiseen tietoturvakriteerien noudattamisessa* sekä *mitkä tekijät vaikuttavat motivaation muuttumiseen tietoturvakriteerien noudattamisessa?* Motivaatioon vaikuttavia tekijöitä tutkittiin syvällisemmin, jotta ymmärrettäisiin työntekijän tietoturvakäyttäytymistä ja työntekijän motivaation syntymiseen ja muuttumiseen vaikuttavia tekijöitä ja pystyttäisiin siten käyttämään yrityksen tietoturvan parantamiseen työntekijöitä tehokkaimmin motivoivia keinoja. Vastausten saamiseksi kerättiin aineisto kvalitatiivisella haastattelulla. Haastattelun rungoksi laadittiin kysymykset, joilla uskottiin saatavan vastaukset haluttuihin tutkimuskysymyksiin. Kaikille motivaation syntymistä ja muuttumista selvittäville kysymyksille oli yhteistä, että niissä pyrittiin syvälliseen vastaukseen pyytämällä myös vastauksen taustalla oleva perusteleva syy.

Haastattelun kysymysten yhteisenä vastauksena voidaan todeta, että työntekijät kokevat tietoturvan toteuttamisen motivaation pääosin pysyneen samana, mutta jonkin verran myös parantuneen. Työntekijät kokevat, että motivaatio tietoturvan toteuttamiseen oli ollut hyvällä tasolla jo ennen tuloa kyseiseen yritykseen töihin. Yrityksessä tehty koko henkilöstöä koskenut tietoturvakysely ei ollut tulosten mukaan muuttanut työntekijöiden motivaatiota tietoturvaohjeiden noudattamiseen mitenkään. Tuloksista käy kuitenkin ilmi, että tietoturvan toteuttamisen motivaatio paranee, kun tietoturva on aiheena yleisesti enemmän esillä. Tietoturvasta puhumisen lisäksi motivaatiota lisää yleinen tieto tietoturvariskeistä ja erityisesti yrityksen tiedotteet tietoturvauhkista. Näin ollen tutkimuksen tulokset tukevat sekä Huigangin ja Yajiongin (2010) tutkimuksen tuloksia, joiden mukaan tietoturvakäyttäytymisen motivaatioon vaikuttaa ymmärrys uhkasta, että Herathin ja

Raon (2009b) tutkimuksen tuloksia, joiden mukaan työntekijöiden asenteisiin tietoturvaohjeita kohtaan vaikuttaa heidän havaintonsa riskeistä.

Haastattelun tuloksista käy ilmi, että myös halu suojata yrityksen tietopääomaa lisää motivaatiota noudattaa tietoturvaohjeita. Työntekijät kokevat yrityksen tietopääoman, erityisesti tuote-, henkilö- ja asiakastietojen suojaamisen merkittävänä tietoturvaohjeiden noudattamiseen motivoivana tekijänä. Nämä tulokset vahvistavat Da Veigan ja Eloffin (2010) aiempaa tutkimustulosta, että positiivisella yrityksen tietoturvakulttuurilla pystytään vähentämään yrityksen tietopääomaan liittyviä riskejä. Tutkimuksen tuloksissa on myös nähtävissä, että viimeisen kolmen vuoden aikana tietoturvan toteuttamisen motivaatioon on työntekijöiden mukaan vaikuttanut tietoteknisten laitteiden muutos, esimerkiksi älypuhelinten käyttöönotto. Myös tietotekniikkaosaston merkitys, sähköisestä tietojen käsittelystä jäävä jälki ja tietokoneiden kehittyminen nimettiin tekijöiksi motivaation parantumiselle. Työntekijät huomioivat tietoturvan tällä hetkellä erityisesti sähköpostin ja henkilötietojen käsittelyssä sekä tietopääoman suojaamisessa. Tulokset tukevat Albrechtsenin (2007) aiempaa tulosta, jonka mukaan työntekijät ovat yleisesti motivoituneita toimimaan yrityksessä tietoturvallisesti. Kun nämä tulokset rinnastetaan Decin ja Ryanin teoriaan, voidaan todeta, että *oma usko toteuttamisen tärkeydestä* nousee esiin syynä tietoturvakriteerien noudattamisen motivaatioon.

Yhtenä haastattelun keskeisenä tuloksena nostetaan esille, että tutkimuksessa mukana olleista työntekijöistä kukaan ei ollut tietoisesti valmis toimimaan yrityksen tietoturvaohjeiden vastaisesti. Aiemmissa tieteellisissä tutkimuksissa on todettu, että työntekijät käyttäytyvät tietoisesti tietoturvaa uhkaavasti ja toimivat tietoisesti tietoturvaohjeiden vastaisesti (Guo ym. 2011). Lisäksi aiemmin on todettu, että tietoturvaohjelmat innostavat työntekijöitä heikosti eikä niillä ole työntekijöiden tietoturvakäyttäytymiseen parantavaa vaikutusta (Leach 2003). Tämän tutkimuksen tulokset ovat päinvastaisia näille tuloksille. Syynä tähän voidaan nähdä, että yrityksen työntekijät ymmärsivät tietoturvan merkityksen erityisesti tietojen suojaamisessa. Haastattelun tuloksissa työntekijät kuitenkin nimesivät joitakin tilanteita, joissa he voisivat kuvitella toimivansa tietoisesti yrityksen tietoturvaohjeiden vastaisesti. Tällainen on esimerkiksi, jos esimies tai ylempi johtaja määräisi toimimaan yrityksen tietoturvaohjeiden vastaisesti. Työntekijät myös totesivat, että voisivat kuvitella toimivansa tietoisesti tietoturvaohjeiden vastaisesti, esimerkiksi lataavansa luvattoman ohjelman omalle työtietokoneelle, jos työtehtävien hoitaminen ehdottomasti sitä vaatisi. Tämä tulos tukee Albrechtsenin (2007) tutkimuksen tuloksia, jonka mukaan liiallinen tietoturvasta aiheutuva työmäärä aiheuttaa ristiriitoja työtehtävien toteuttamisen ja tietoturvaohjeiden noudattamisen välille. Kun nämä tutkimustulokset rinnastetaan Decin ja Ryanin teoriaan, voi-

daan todeta, että myös *toisen henkilön tai tilanteen vaatimus* nousee esiin syynä tietoturvakriteerien noudattamisen motivaatioon.

Toisen haastattelun tulokset tukevat ja syventävät ensimmäisen haastattelun tuloksia, joiden mukaan oma usko toteuttamisen tärkeydestä motivoi vahvasti tietoturvan noudattamiseen. Ensimmäisessä haastattelussa myös toisen henkilön tai tilanteen vaatimus nousi esiin tietoturvan noudattamiseen motivoivana tekijänä. Myös tämä tulos sai vahvistusta toisen haastattelun tuloksissa.

Tutkimuskysymysten *mitkä tekijät vaikuttavat motivaation syntymiseen tietoturvakriteerien noudattamisessa* ja *mitkä tekijät vaikuttavat motivaation muuttumiseen tietoturvakriteerien noudattamisessa* vastausten keskeisinä *johtopäätöksinä* voidaan todeta, että työntekijät eivät ole valmiita tietoisesti toimimaan yrityksen tietoturvaohjeiden vastaisesti. Pääsääntöisesti tietoturvaohjeiden noudattamisen motivaation koetaan pysyvän samana tai paranevan. Tietopääoman suojaaminen ja yleinen keskustelu tietoturvasta ja siihen kohdistuvista uhkista ovat merkittävimpiä yksittäisiä motivaatioon parantavasti vaikuttavia tekijöitä. Oma usko toteuttamisen tärkeydestä on merkittävin tekijä, joka vaikuttaa työntekijöiden tietoturvakriteerien noudattamiseen. Myös toisen henkilön tai tilanteen vaatimus voi vaikuttaa motivaatioon tietoturvakriteerien noudattamisessa. Työntekijöiden motivaatio tietoturvaohjeiden noudattamiseen syntyy jo varhaisessa vaiheessa ja muutos motivaatiossa tapahtuu hitaasti. Motivaatio tietoturvaohjeiden noudattamiseen ei ole yrityskohtaista. Yksittäisellä yrityksellä on tietoturvaohjeiden noudattamisen motivaation syntymiseen vain vähän vaikutusta. Tietoturvaohjeiden noudattamisen motivaatioon on vahva negatiivinen vaikutus, jos tietoturva vaikeuttaa työntekijän työtehtävien tekemistä.

Tämä tutkimus tukee jossain määrin muiden tutkijoiden (mm. Karjalainen 2011: 27; Puhakainen & Siponen: 2010) päätelmiä siitä, että tietoturvatutkimuksen haasteena on sopivien teoreettisten viitekehysten ja yleisten lähestymisteorioiden puuttuminen. Tämän tutkimuksen tieteellisenä teoreettisena viitekehyksenä käytettiin motivaatioteoriaa, johon liittyen käsiteltiin oppimista. Decin ja Ryanin teorian onnistunut yhdistäminen tietoturvaan kannustaa toivottavasti tutkijoita yhä uusien erilaisten teorioiden yhdistämiseen tietoturvatutkimuksessa.

Tässä motivaation teoriaan pohjautuvassa tutkimuksessa vastattiin tutkimuskysymyksiin mitä tietoturvakriteerejä Suomessa julkaistut ohjeet sisältävät, millä tasolla työntekijät pyrkivät noudattamaan tietoturvakriteerejä, mitkä tekijät motivoivat työntekijöitä heidän pyrkiessä noudattamaan tietoturvakriteerejä sekä mitkä tekijät vaikuttavat motivaation syntymiseen ja muuttumiseen tietoturvakriteerien noudattamisessa. Tutkimuksen kaikkien tutkimuskysymysten vastaamisessa onnistuttiin.

6.2 Käytännön suositukset

Viranomaistahojen tulee ymmärtää, että tällä hetkellä tarjolla olevien tietoturvaohjeistajien ja -ohjeistusten määrä on runsas. Viranomaistahojen tulee pyrkiä *vähentämään sekä ohjeistajia että ohjeistuksia.* Ohjeistuksissa käytettävä termistö on kirjava, mikä hankaloittaa kokonaiskuvan muodostamista ohjeistuksista. Viranomaistahojen tulee pyrkiä *selkiyttämään ja vakinaistamaan tietoturvaa koskeva termistö*. Lisäksi viranomaistahojen tulee huomioida, että Internetissä julkaistavat ohjeistukset ovat nyt useissa osissa ja osittain erittäin pieninä paloina, minkä takia niiden lukeminen ja kokonaisvaltainen hahmottaminen on työlästä. *Ohjeistukset tulee muuttaa muotoon, jossa ne ovat helpommin saatavilla kokonaisuuksina ja hahmotettavista kokonaisvaltaisesti*.

Tutkimuksen perusteella suositellaan, että yrityksen hallinnossa tulee keskustella ja päättää selkeästi mihin viranomaistahojen tietoturvaohjeistuksiin yrityksessä keskitytään ja mitä niistä pyritään noudattamaan. Yritysten tulee selkeämmin tuoda kaikkien työntekijöiden tietoisuuteen mitä tietoturvakäytänteitä yrityksessä noudatetaan. Yritysten tulee pyrkiä noudattamaan yhteisesti hyväksyttyjä tietoturvastandardeja ja -käytänteitä, jolloin työntekijöiden siirtyminen yrityksestä toiseen tukee tehokkaammin hyvien tietoturvakäytänteiden toteutumisen.

Yrityksen *työntekijät tulisi saada ymmärtämään* erikseen kunkin tietoturvakriteerin kohdalla *miksi kyseisen kriteerin noudattaminen on yrityksessä tärkeää*. Tavoitteena tulee olla, että työntekijälle muodostuu *oma ymmärrys kunkin tietoturvakriteerin toteuttamisen tärkeydestä*. Käytännön suosituksena esitetään, että jokaisen ohjeen sisältö tulee kuvata ja kertoa niin selkeästi ja perusteellisesti, että työntekijä ymmärtää sen. Perusteet tulee kertoa työntekijälle noudattamatta jättämisestä aiheutuvana konkreettisena vaikutuksena käytännön toimintaan. Näin toimimalla työntekijä saadaan motivoituneemmaksi noudattamaan annettuja ohjeita. Noudattamisen syitä tulee perustella sisäisesti motivoivilla tekijöillä, kuten valinnan mahdollisuuden tunteella, tunteella omasta osaamisesta, tunteella noudattamisen merkityksellisyydestä ja tunteella tietoturvan toteutumisen edistymisestä. Lisäksi tietoturvan toteutumisesta tulee antaa palautetta.

Työntekijät ovat valmiita noudattamaan kriteerejä myös ulkoisesti motivoivista syistä, kuten toisen henkilön tai tilanteen vaatimuksesta. Siksi suositellaan, että yritysjohdon tulee selkeästi *vaatia tietoturvakriteerien noudattamista* tilanteissa, jossa se on aiheellista. Tällöinkin *vaade tulee perustella niin selkeästi ja perusteellisesti, että työntekijä ymmärtää sen*. Työntekijän tulee ymmärtää noudattamatta jättämisestä aiheutuva konkreettinen vaikutus käytännön toimintaan.

Tutkimuksen perusteella suositellaan, että yrityksen tietoturvakäytänteet tulee sisällyttää työhöntuloperehdytyksen osaksi. Tietoturvakulttuurin luomiseen ja vanhempien kollegojen antamaan hyvään tietoturvakäyttäytymisen esimerkkiin tulee panostaa yrityksissä. Uusista käyttöönotettavista tietoturvakäytänteistä tulee tiedottaa työntekijöille tehokkaasti. Tietoturvatiedotteiden määrä tulee kuitenkin pitää rajallisena, jotta tiedotteiden teho ei katoa määrän mukana. Jokaisen noudatettavaksi otettavan tietoturvakriteerin kohdalla työntekijä pitää saada ymmärtämään, miksi kriteerin noudattaminen yrityksessä on tärkeää ja miksi noudattamista vaaditaan. Työntekijöille tulee tarjota koulutusta tietoturvan käytäntöihin. Tietoturvan kehittäminen ja ohjaus tulee olla jatkuvaa ja kokonaisvaltaista. Yritysten tulee myös *huolehtia, että tietoturvan tekniset toteutukset eivät estä työntekijöiden päivittäistä työskentelyä*.

6.3 Rajoitukset

Tässä tutkimuksessa tarkasteltiin hallinnollista tietoturvaa. Tutkimus rajattiin tarkastelemaan yhtä suomalaista pk-yritystä ja sen työntekijöitä. Tarkastelu tehtiin esimiesten ja työntekijöiden näkökulmista.

Tutkimuksessa tarkasteltiin teoreettisena viitekehyksenä motivaatiota ja tietoturvaa. Tavoitteeseen pääsemiseksi käytettiin Decin ja Ryanin menetelmää mitata motivaatiotekijöitä, jossa motivaatiotekijöitä nimetään neljä. Osaltaan tämä rajoittaa haastateltavien vastauksia, mutta haastattelussa tarjottiin myös muu motivointisyy -vaihtoehto. Haastateltavat eivät kuitenkaan valinneet sitä kertaakaan. Kuitenkin, tulee huomioida, että jos nimettyjä motivaatiotekijöitä olisi ollut enemmän kuin Decin ja Ryanin menetelmän neljä vaihtoehtoa, olisivatko muut vaihtoehdot tulleet valituksi. Decin ja Ryanin menetelmä motivaatiotekijöiden mittaamiseksi soveltui erinomaisesti tietoturvakriteerien motivaatiotekijöiden määrittelemiseen.

Tietoturvadokumenttien sisällön kuvaaminen oli yksi tutkimuksen tavoitteista. Tietoturvaa ja tietoturvaohjeistuksia käsittelevissä luvuissa 3 ja 4 käytettiin mahdollisimman tarkasti alkuperäisten lähteiden mukaista termistöä, jotta lukijalle tulisi mahdollisimman totuudenmukainen kuva dokumenteissa käytössä olevasta termistöstä.

Tutkimuksen rajoitteissa täytyy huomioida jatkuvasti päivitettävät tietoturvaohjeistukset. Myös uusia tietoturvaohjeistuksia julkaistaan koko ajan. Tästä johtuen tutkimuksen toteuttaminen erityisesti ohjeistusten sisällön osalta oli haastavaa. Myös Internet ohjeistusten julkaisupohjana aiheutti tutkimustyölle haasteita. Internet-lähteiden linkit on pyritty päivittämään, jos niissä on havaittu muutoksia,

mutta siitä huolimatta tutkijalla on pelko, että linkkejä on päivitetty senkin jälkeen.

Kyselyssä tutkittiin millä tasolla työntekijät *pyrkivät* noudattamaan tietoturvakriteerejä, jolloin tulee huomata, että tutkimuksessa keskityttiin tietoturvaan pyrkimisen tasoon, eli motivaatioon ja haluun pyrkiä toimimaan tietoturvaohjeiden mukaisesti, ei käytännön toteutumisen tasoon.

Ensimmäisessä haastattelussa tarkasteltiin kyselytutkimuksen tuloksista poimittujen 22 heikoimmin noudattamaan pyrityn tietoturvakriteerin noudattamaan pyrkimisen motivaatiotekijöitä. Tästä johtuen voidaan pohtia, olisivatko eniten motivoivien ja vähiten motivoivien tietoturvakriteerien motivaatiotekijät samoja. Jos haastattelussa tarkastellut kriteerit olisivat olleet kyselytulosten eniten motivoineet kriteerit, olisiko ulkoisesti motivoiva tekijä toisen henkilön tai tilanteen vaatimuksesta ollut yhtä merkittävänä motivaatiotekijänä vai olisivatko sisäisesti motivoivat tekijät tulleet useammin valituiksi.

Kyselyn ja ensimmäisen haastattelun kysymykset valmisteltiin suoraan luotujen tietoturvakriteerien pohjalta, mikä saattoi aiheuttaa virheitä tutkimuksen tuloksissa. Kyselyn ja ensimmäisen haastattelun vastauksia voitaisiin katsoa olevan ohjatun tai rajoitetun. Tämän arvioimiseksi kyselyn ja haastattelun kysymysten laadinta on kuvattu kohdissa 5.2 ja 5.4.

Tutkimuksessa jollain tavalla rajoituksena nähdään ensimmäisen haastatteluaineiston rajoittuminen kahdeksaan työntekijään sekä kyselytutkimuksen vastausprosentin oltua 48,7 %. Haastattelun tulokset alkoivat kuitenkin toistua jo viidennen haastattelun jälkeen. Kyselyn osalta oli odotettavaakin, että kaikilta, joille kysely lähetetään, ei saataisi vastausta. Kun tutkija ei ollut paikalla, ei hän omalla toiminnallaan vaikuttanut lopputuloksiin, mutta ilman kyselyyn vastaajan ja tutkijan vuoropuhelua kyselyn vastausprosentti jää pienemmäksi. Vastaamatta jättäneiden osuuteen saattoi vaikuttaa myös tietoturva tutkimuksen aiheena sekä vastaamisen vapaaehtoisuus.

Toisen haastattelun ja sen vastausten arvioimiseksi toisen haastattelun kysymysten laadinta ja toteutus on kuvattu kohdassa 5.6. Tutkimuksessa jollain tavalla rajoituksena voidaan nähdä myös toisen haastatteluaineiston rajoittuminen seitsemään työntekijään. Haastattelun tulokset alkoivat kuitenkin toistua jo kolmannen haastattelun jälkeen.

Tutkimuksen *luotettavuuden arviointiin* liittyen tutkimuksen tavoitteisiin pääsemiseksi käytettiin kvantitatiivista kyselyä ja haastatteluja, joissa tehtiin sekä kvantitatiivista että kvalitatiivista tutkimusta. Kvantitatiivisen tutkimuksen arviointiin

käytetään yleisesti tutkimuksen validiteetin ja reliabiliteetin tarkastelua. Kvalitatiivisen tutkimuksen arviointiin voidaan käyttää yleisiä luotettavuuden arviointikriteerejä luotettavuus, vastaavuus, siirrettävyys ja vahvistettavuus (Guba & Lincoln 1989: 241–242; Kylmä & Juvakka 2007, 127). Seuraavassa kerrotaan näiden luotettavuuden arviointikriteerien määritelmät sekä miten tutkimuksessa on huomioitu tutkimuksen luotettavuuden arviointi näillä kriteereillä.

Kvantitatiivisen tutkimuksen validiteetit arvioinnissa tarkastellaan miten perusteellisesti tutkimus on tehty. Lisäksi arvioidaan ovatko saadut tulokset ja tehdyt päätelmät oikeita. Reliabiliteetin arvioinnissa tarkastellaan tutkimuksen mittaustulosten toistettavuutta ja analyysin johdonmukaisuutta. Kvantitatiivisessa tutkimuksessa luotettavuuden tarkastelu kohdistuu erityisesti mittarin tai tutkimusmenetelmän luotettavuuteen.

Kvalitatiivisessa tutkimuksessa Eskolan ja Suorannan (2005, 209–213) mukaan luotettavuuden arviointi kohdistuu koko tutkimusprosessiin. Kvalitatiiviselle tutkimukselle on ominaista, että tulosten analysointi sisältää tutkijan omaa pohdintaa, minkä takia luotettavuuden osalta tulee erityisesti pohtia tutkijan omaa vaikutusta tuloksiin. Luotettavuuden osalta tutkijaa itseään voidaan kuitenkin pitää tärkeimpänä ja parhaana arvioijana. Myös Kylmä ja Juvakka (2007, 129) pitävät tutkijaa ja hänen lähtökohtiaan keskeisenä kvalitatiivisen tutkimuksen luotettavuuden arvioinnissa, minkä takia tutkijan tulee tiedostaa omat lähtökohdat tutkimuksen tekijänä sekä kuvata ne tutkimusraportissa. Refleksiivisyys edellyttää, että tutkija itse arvioi omaa vaikutustaan aineistoon ja koko tutkimusprosessiin.

Vastaavuudella tarkoitetaan miten tutkimuksen tuottamat tulokset vastaavat alkuperäistä konstruktiota. Vastaavuus liitetään aineiston analyysiin ja tulosten tulkintaan. Keskeistä vastaavuuden arvioimisessa on, miten hyvin tutkija pystyy tavoittamaan tutkittavan todellisuuden. (Lincoln & Guba 1985.)

Siirrettävyydellä tarkoitetaan tulosten siirrettävyyttä toiseen kontekstiin. Jotta voitaisiin arvioida kvalitatiivisen tutkimuksen tutkimustulosten siirrettävyyttä vastaavanlaisiin tilanteisiin, tulee tutkijan kuvata riittävän tarkasti tutkimustilanne. Siirrettävyyden arvioimiseksi tutkijan on kuvattava myös tutkimukseen osallistuneita ja ympäristöä sekä tutkimusprosessi. (Kylmä & Juvakka 2007, 129; Tuomi & Sarajärvi 2009, 138–141.) Tuomi ja Sarajärvi (2009, 138–141) lisäävät, että kvalitatiivisessa tutkimuksessa on huomioitava, että tutkimustulokset liittyvät siihen paikkaan ja aikaan, jossa tutkimus on tehty, eivätkä kaikki tutkimustulokset ole toistettavissa. Hirsjärven, Remeksen ja Sajavaaran (2004, 216) mukaan siirrettävyys on todettavissa, jos esimerkiksi kaksi tutkijaa päätyy tutkimuksissaan samanlaiseen tutkimustulokseen.

Kvalitatiivisessa tutkimuksessa vahvistettavuus kohdistetaan koskemaan koko tutkimusprosessia. Vahvistettavuuden arvioimisen edellytyksenä on, että koko tutkimusprosessi on raportoitu riittävällä tarkkuudella, jotta toinen tutkija pystyy seuraamaan prosessin kulkua. Vahvistettavuuden arviointi kvalitatiivisessa tutkimuksessa voi olla melko haastavaa, koska eri tutkijoiden tekemät tulkinnat täsmälleen samasta aineistosta voivat olla hyvinkin erilaisia. Käytännössä tämä tarkoittaa tulosten todellisuuksien moninaisuutta, ei yksittäisen tutkimuksen epäluotettavuutta. Tämä lisää ymmärrystä tutkimuskohteesta ja siihen liitettävästä ilmiöstä. (Kylmä & Juvakka 2007, 128.) Eskola ja Suoranta (2005, 141–143) huomauttavat, että alkuperäistä totuutta ei ole mahdollista saavuttaa, kun analysoidaan kvalitatiivista aineistoa. Tulokset ovat vain yksi versio asiasta, koska tutkijan tekemät päätelmät ovat dokumentteihin kirjattujen aineistojen tulkintoja.

Kvantitatiivisen tutkimuksen validiteetin ja reliabiliteetin arvioimiseksi on pyritty kuvaamalla tutkimuksen konteksti sekä tutkimuksen toteutus aineiston keruineen ja analysointeineen mahdollisimman tarkasti. Tutkimuksessa on kuvattu avoimesti tutkimuksen teon vaiheet sekä tutkimuksessa käytetyt välineet ja menetelmät. Tällä tavoin lukijalle on haluttu antaa riittävästi tietoa tutkimuksen teosta, jotta tutkimuksen tuloksia on mahdollista arvioida.

Kvalitatiivisen tutkimuksen luotettavuuteen on pyritty kuvaamalla tutkimuksen toteutus aineiston keruineen ja analysointeineen mahdollisimman tarkasti. Tutkimuksessa on kuvattu avoimesti tutkimuksessa käytetyt välineet ja menetelmät. Tällä tavoin lukijalle on haluttu antaa riittävästi tietoa tutkimuksen teosta, jotta tutkimuksen tuloksia on mahdollista arvioida. Haastattelutilanteet olivat ennalta sovittuja ja niitä ei häiritty ulkoisilla tekijöillä. Haastattelututkimusten tulokset perustuivat pelkästään muistiinpanoissa oleviin merkintöihin, jotka tuotettiin vastuullisesti ja luotettavasti. Tutkimuksen heikkoutena voitaisiin pitää muistiinpanoissa olevan tiedon rajallisuutta. Muistiinpanoihin kirjattiin kuitenkin kaikki haastateltavien vastaukset. Tutkimustulosten esittely tehtiin rehellisesti, huolellisesti ja vastuullisesti ja niissä näkyy koko vastausten todellisuus, joten tulosten esittelyä voidaan pitää tyhjentävänä ja yksiselitteisenä. Haastattelujen vastauksista on esitetty suoria lainauksia, joilla halutaan vahvistaa havaintojen luotettavuutta ja osoittaa halu raportoida tulokset avoimesti ja rehellisesti. Luotettavuuden lisäämiseksi myös tutkimustulokset on esitetty selkeästi ja ymmärrettävästi, sekä täsmällisesti, yksityiskohtaisesti ja todellisesti.

Kyselyssä yrityksen työntekijöiden vastausprosentti oli korkea. Kyselyn toteuttaminen oli ennalta sovittu, ja sen vastaamisaika oli riittävä. Kyselyn vastaajia ei täsmällisesti tiedetä, koska kyselyyn vastattiin nimettömästi, mutta kyselyn tulokset on saatu vastaajilta, joka on rajattu ryhmä yrityksen todellisia työntekijöitä.

Vastaajien joukko koostuu sekä esimiehistä että työntekijöistä. Kyselyssä saatujen tulosten pohjalta pystyttiin tekemään ensimmäinen haastattelututkimus. Kyselytutkimuksessa käytetyt tutkimusmenetelmät, aineiston keruu ja analysointi sekä tutkijan oma toiminta ja vaikutus tutkimuksen tuloksiin on kuvattu kohdassa 5.2.

Ensimmäisessä haastattelututkimuksessa haastateltiin kahdeksaa ja toisessa seitsemää työntekijää. Tutkimuksen tulosten luotettavuutta siirrettävyyden osalta voitaisiin parantaa laajentamalla tutkimusten aineistopohjaa aineistonkeruuvaiheessa. Tutkimusten haastattelutulokset on kuitenkin saatu vastaajilta, joka on rajattu ryhmä yrityksen todellisia työntekijöitä. Vastaajat ovat ensimmäisessä haastattelututkimuksessa sekä esimiehiä että työntekijöitä, ja toisessa haastattelututkimuksessa sattumalta pelkästään työntekijöitä. Kenenkään haastatellun työntekijän toimenkuva ei liittynyt suoraan tietotekniikkaan. Haastattelun vastaajat ovat tiedossa, joten haastattelun vastaukset ovat ainakin periaatteessa todennettavissa jälkikäteen. Ensimmäisessä haastattelututkimuksessa käytetyt menetelmät, aineistojen keruu ja analysointi sekä tutkijan oma toiminta ja vaikutus tutkimuksen tuloksiin on kuvattu kohdassa 5.4, ja toisessa haastattelututkimuksessa käytetyt menetelmät, aineistojen keruu ja analysointi sekä tutkijan oma toiminta ja vaikutus tutkimuksen tuloksiin on kuvattu kohdassa 5.6.

Tutkimuksessa on huomioitu myös tutkimustoiminnan eettisyys huolehtimalla tutkittavien yksityisyydestä. Haastateltavista kerrottiin ainoastaan asema yrityksessä. Tarkemmat tiedot tutkittavista, esimerkiksi ikä- ja sukupuolijakauma, on jätetty mainitsematta ja kohderyhmää ei ole kuvattu tarkasti. Siirrettävyyden näkökulmasta tämä heikentää tutkimuksen luotettavuutta. Tutkimuksen kontekstina oli yksi suomalainen pk-yritys. Tutkimuksen tulosten siirrettävyyden arviointia varten on tutkimuksessa kuvattu kysely- ja haastattelututkimuksiin osallistunut suomalainen pk-yritys nimeltä. Tutkimuksessa on kerrottu yrityksen yleistiedot sekä kysely- ja haastattelututkimusten tekemiseen liittyneet tiedot mahdollisimman tarkasti. Tutkimuksen tulosten vahvistettavuuden arvioimiseksi on tutkimuksessa käytetyt menetelmät, aineistojen keruu ja analysointi sekä tutkijan oma toiminta ja vaikutus tutkimuksen tuloksiin esitetty täsmällisesti, yksityiskohtaisesti ja todellisesti. Haastattelujen vastauksista on esitetty suoria lainauksia, joilla halutaan osoittaa tulkintojen todellisuutta.

Tietoturvakriteerien sekä tietoturvaohjeistajien ja -ohjeistusten nimeämisessä oli haasteena aineiston jatkuva kehittyminen. Tietoturvakirjallisuuden ja -ohjeistusten sisällön tutkiminen ja esittely toteutettiin vuosina 2010–2011. VAHTI-ohjeistuksen osalta ohjeistuksia koskeva tieto päivitettiin vielä tutkimuksen lopussa vastaamaan VAHTI-ohjeistuksen tilannetta vuoden 2012 lopussa. Tietoturvakriteerejä etsittiin useista lähteistä, jotka olivat hyvin monitasoisia. Lisäksi

haasteena oli ohjeistuksissa käytetty kirjava termistö. Tietoturvakriteerien nimeäminen oli yksi tutkimuksen tavoite, jonka tulosta käytettiin toiseen tutkimuksen tavoitteeseen pääsemiseksi, ts. tietoturvakriteerien noudattamaan pyrkimisen motivaatiotekijöiden tutkimiseen yrityksen työntekijöillä. Tutkimukseen mukaan otettuja tietoturvaohjeita ja -dokumentteja ei voida pitää ainoana totuutena, vaikkakin ne ovat monipuolisia ja sisältävät erityisesti pk-yrityksille suunnattuja keskeisiä ohjeita pk-yritysten tietoturvan vaatimuksista. Kunkin ohjeen sisältöä analysoitaessa käytettiin siinä käytettyjä termejä, jolla haluttiin tuoda esille olemassa oleva totuus ohjeiden kirjavasta termikäytännöstä. Termien yhtenäistäminen ohjeiden kesken olisi vääristänyt tutkimuksen tulosta. Kriteerien löytämisessä käytettiin dokumenttianalyysiä. Koska tutkimuksessa esitellyt ohjeet ja dokumentit kehittyivät jatkuvasti jo tutkimuksen aikana, ei nimettyjä kriteerejä voida pitää ainoana totuutena. Myös ohjeistajien jatkuvaan päivittymiseen liittyen nimettyjä ohjeistajia ei voida pitää ainoana totuutena. Aineistonkeruun ajankohtana tietoturvaohjeistajia etsittiin useista lähteistä.

Kirjavat termit aiheuttivat jonkin verran ongelmia kyselyn ja haastattelujen toteutuksissa, kun kysymyksissä esiintyi vastaajille muutama outo termi. Tämä tapahtui siitäkin huolimatta, että kysymysten ymmärrettävyys pyrittiin etukäteen varmistamaan pyytämällä kysymyksiin kommentteja yhdeltä henkilöltä kyselyn ja haastattelujen kysymysten valmistuttua. Kommenttien pohjalta kysymyksiin tehtiin tarpeelliset muutokset. Haastattelujen tuloksiin oudot termit eivät vaikuttaneet mitenkään, koska oudot termit pystyttiin selittämään vastaajille heti haastattelun aikana. Sen sijaan kyselyn tuloksiin oudot termit saattoivat vaikuttaa jonkin verran. Outoja termejä esiintyi kuitenkin vain muutamassa kysymyksessä, joten niiden vaikutus tuloksiin on erittäin vähäinen.

6.4 Jatkotutkimusaiheet

Tässä tutkimuksessa tarkasteltiin hallinnollista tietoturvaa sekä esimiesten että työntekijöiden näkökulmat huomioiden suomalaisessa pk-yrityksessä. *Jatkotutkimusaiheena* tutkimusta voitaisiin syventää pelkästään hallinnossa työskentelevien työntekijöiden näkökulmaan tai pelkästään työntekijöiden näkökulmaan. Tarkastelu valtakunnallisesti laajemmin kaikki yritykset kattavasti tai tarkastelu yli maan rajojen olisi myös mielenkiintoista. Tässä tutkimuksessa tarkasteltiin erityisesti hallinnollisen tietoturvan kriteereitä. Samanlainen motivaatiotekijöiden tutkimus voitaisiin toteuttaa kullekin tietoturvan osa-alueelle erikseen.

Mielenkiintoista olisi tehdä tutkimus, jossa selvitettäisiin tietoturvakriteerien noudattamaan pyrkimisen motivaatiotaso sekä motivaatiotekijät ennen ja jälkeen

kunkin tietoturvakriteerin noudattamisen tärkeyden selittämistä työntekijöille. Tietoturvakriteerien motivoivuutta voitaisiin tarkastella myös tutkimuksessa läpikäytyjen ohjeistusten läpikäymisen jälkeen julkaistuista ohjeistuksista.

Tuloksissa todettiin ohjeistuksia löytyvän runsaasti ja lisäksi niiden todettiin sisältävän erittäin kirjavaa termistöä. Tietoturva-termin ja muut tietoturvaan liittyvät määritelmät, kuten riskiluokittelun määritelmä, voisivat olla tieteellisen tutkimuksen kohteita. Ohjeistuksiin ja sen termistöön kohdistuva tarkempi tutkimus ja analysointi sekä niiden selkiyttämiseen pyrkivä tutkimus esitetään jatkotutkimusaiheena, joissa nähdään myös poikkitieteellisiä lähestymismahdollisuuksia.

Suomalaisten viranomaisten yrityksille tarjoamia tietoturvaohjeistuksia ei ole tutkittu tämän tutkimuksen lisäksi tieteellisesti lainkaan. Mielenkiintoista olisikin selvittää laajemmin ovatko viranomaistahojen pk-yrityksille kirjoittamat tietoturvaohjeistukset konsulttikirjallisuutta vailla tieteellistä perustelua. Ohjeistusten sisältöjä voisi analysoida esimerkiksi soveltamalla Bungen (1967, 75) hyvän luokituksen kriteereitä kattavuus, pysyvyys, luokkien yhteispisteettömyys ja luonnollisuus.

Tässä tutkimuksessa motivaatiotekijöiden tarkastelu tehtiin 22 heikoiten motivoivasta kriteeristä. Tutkimus voitaisiin tehdä laajemmin koskemaan kaikkia kriteerejä. Tämän tutkimuksen tekemisessä käytettiin erityisesti Decin ja Ryanin motivaatiotekijöitä. Vastaavia tutkimuksia motivaatiotekijöistä voitaisiin tehdä avoimilla kysymyksillä, jolloin motivaatiotekijöitä voitaisiin tarkastella laajemmin.

LÄHTEET

Ajzen, I. (1985). From intentions to actions: a theory of planned behavior. SSSP Springer Series in Social Psychology. 11–39.

Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes. 50(2). 179–211.

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

Albrechtsen, E. & J. Hovden (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. Computers & Security. 29(4). 432–445.

Anandarajan, M. (2002). Profiling web usage in the workplace: A behavior-based artificial intelligence approach. Journal of Management Information Systems. 19(1). 243–266.

Anderson, C. & R. Agarwal (2010). Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions. MIS Quarterly. 34(3). 613–643.

Aytes, K. & T. Connolly (2003). A research model for investigating human behavior related to computer security. The proceedings of the 9th Americas conference on information systems. 2027–2031.

Bannert, M. (2002). Managing cognitive load – recent trends in cognitive load theory. Learning and Instruction. 12(1). 139–146.

Belth, M. (1965). Education as a Discipline. A Study of the Role of Models in Thinking. Boston: Allyn and Bacon.

Brown, J. & P. Duguid (1991). Organizational Learning and Communities of Practice: Toward a Unified View of Working, Learning and Innovation. Organization Science. 2(1). 40–57.

Bulgurcu, B., H. Cavusoglu & I. Benbasat (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quarterly. 34(3). 523–A7.

Bunge, M. (1967). Scientific research I. The search for system. Berlin: Springer-Verlag.

CERT-FI (2010a). CERT-FI:n www-sivuston etusivu. Päivitetty 3.2.2010. [viitattu 5.2.2010]. Saatavissa: http://www.cert.fi/.

CERT-FI (2010b). Ohjeet – Toimet tietoturvaloukkaustilanteessa. Päivitetty 29.1.2010. [viitattu 5.2.2010]. Saatavissa: http://www.cert.fi/ohjeet.html.

Cheolho, Y., H. Jae-Won & R. Kim (2012). Exploring factors that influence students' behaviors in information security. Journal of Information Systems Education. 23(4). 407–415.

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

Computer Security Institute (2009). 2009 CSI Computer Crime and Security Survey. Executive Summary. [viitattu 3.5.2011]. Saatavissa: www.pathmaker.biz/whitepapers/CSISurvey2009.pdf.

Cox, A., S. Connolly & J. Currall (2001). Raising information security awareness in the academic setting. VINE. 31(2). 11–16.

Culnan, M., E. Foxman & A. Ray (2008). Why it executives should help employees secure their home computers. MIS Quarterly. 7(1). 49–56.

Culnan, M. & C. Williams (2009). How ethics can enhance organizational privacy: lessons from the ChoisePoint and TJX Data Breaches. MIS Quarterly. 33(4). 673–687.

D'Arcy, J. & T. Herath (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. European Journal of Information Systems. 20(6). 643–658.

D'Arcy, J. & A. Hovav (2007). Deterring internal information systems misuse. Communications of the ACM. 50(10). 113–117.

D'Arcy, J., A. Hovav & D. Galletta (2009). User awareness of security countermeasures and its impact on information systems misuse. A deterrence approach. Information Systems Research. 20(1). 79–98.

D'Aubeterre, F., R. Singh & L. Iyer (2008). Secure activity resource coordination: Empirical evidence of enhanced security awareness in designing secure business processes. European Journal of Information Systems. 17(5). 528–542.

Da Veiga, A. & J. Eloff (2007). An information security governance framework. Information Systems Management. 24(4). 361–372.

Da Veiga, A. & J. Eloff (2010). A framework and assessment instrument for information security culture. Computers & Security. 29(2). 196–207.

De Corte, E., L. Verschaffel, N. Entwistle & J. Van Merriëboer (toim.) (2003). Unravelling basic components and dimensions of powerful learning environments. Elsevier.

Deci, E. (1971). Effects of externally mediated rewards on intrinsic motivation. Journal of Personality and Social Psychology. 18(1). 105–115.

Deci, E. & R. Ryan (2000). The "what" and "why" of goal pursuits: human needs and the self-determination of behavior. Psychological Inquiry. 11(4). 227–268.

Dey, D., A. Lahiri & G. Zhang (2012). Hacker behavior, network effects, and the security software market. Journal of Management Information Systems. 29(2). 77–108.

Dix, A., J. Finley, G. Abowd & R. Beale (2004). Human-computer interaction. Upper Saddle River: Prentice Hall.

Drevin, L., H. Kruger & T. Steyn (2007). Value-focused assessment of ICT security awareness in an academic environment. Computers & Security. 26(1). 36–43.

Elinkeinoelämän keskusliitto EK, Sisäasiainministeriö & Puolustusministeriö (2009). Kansallinen turvallisuusauditointikriteeristö (KATAKRI). Julkaistu 20.11.2009. [viitattu 12.5.2011]. Saatavissa: http://ek2.ek.fi/ytnk08/fi/STO/Katakri/KATAKRI_SET.pdf.

Engeström, Y. (1994). Teachers as collaborative thinkers: Activity-theoretical study of an innovative teacher team. In: Teachers' minds and actions: Research on teachers' thinking and practice. Eds I. Carlgren, G. Handal & S. Vaage. London: Falmer Press. 43–61.

Engeström, Y. (2001). Kehittävä siirtovaikutus: mitä ja miksi? Teoksessa: Tuomi-Gröhn, T. & Y. Engeström, (toim.). Koulun ja työn rajavyöhykkeellä: uusia työssä oppimisen mahdollisuuksia. Helsinki: Yliopistopaino. 19–27.

Ernst & Young (2008). Talouden taantumasta huolimatta tietoturvaan investoidaan yhä enemmän. Julkaistu 15.10.2008. [viitattu 1.3.2011]. Saatavissa: http://www.de.ey.com/FI/fi/Newsroom/News-releases/Tiedote_151008_GISS2008.

Ernst & Young (2009). Taantuma lisännyt yritysten tietoturvariskejä. Julkaistu 10.11.2009. [viitattu 1.3.2011]. Saatavissa: http://www.de.ey.com/FI/fi/Newsroom/News-releases/20091110_tiedote_GISS_2009.

Ernst & Young (2010). Yritykset eivät ole valmistautuneet uuden teknologian mukanaan tuomiin tietoturvariskeihin. Julkaistu 4.11.2010. [viitattu 1.3.2011].

Saatavissa: http://www.de.ey.com/FI/fi/Newsroom/News-releases/20101104_tiedote_GISS.

Eskola, J. & J. Suoranta (2005). Johdatus laadulliseen tutkimukseen. Tampere: Vastapaino.

Euroopan unioni (2007). Mikroyritysten sekä pienten ja keskisuurten yritysten määritelmä. Päivitetty 8.8.2007. [viitattu 1.2.2011]. Saatavissa: http://europa.eu/legislation_summaries/enterprise/business_environment/n26026_fi.htm.

Euroopan unioni (2010). Euroopan verkko- ja tietoturvavirasto (ENISA). Päivitetty 30.4.2010. [viitattu 15.2.2011]. Saatavissa: http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/l24153_fi.htm.

Guba, E. & Y. Lincoln (1989). Fourth Generation Evaluation. Newbury Park etc.: Sage Publications.

Guo, K., Y. Yuan, N. Archer & C. Connelly (2011). Understanding nonmalicious security violations in the workplace: a composite behavior model. Journal of Management Information Systems. 28(2). 203–236.

Hakala, M., M. Vainio & O. Vuorinen (2006). Tietoturvallisuuden käsikirja. Jyväskylä: Docendo Finland Oy.

Helenius, M. (2005). Tietoturvallisuuden tutkimus ja opetus. Nykytilanne ja kehittämismahdollisuudet. Tietoyhteiskuntainstituutin raportteja 2/2005. Tampere: Tampereen yliopisto.

Heljaste, J.-M., J. Korkiamäki, H. Laukkala, J. Mustonen, J. Peltonen & P. Vesterinen (2008). Yrityksen turvallisuusopas. Jyväskylä: Gummerus Kirjapaino Oy.

Helsingin Sanomat (2010). Valtiollisessa tietoturvassa on suuria puutteita. Julkaistu: 21.10.2010. [viitattu 15.2.2011]. Saatavissa: http://www.hs.fi/paakirjoitus/artikkeli/Valtiollisessa+tietoturvassa+on+suuria+puutteita/HS20101021SI1MA01stu.

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

Herath, T. & H. R. Rao (2009b). Protection motivation and deterrence: A framework for security policy compliance in organisations. European Journal of Information Systems. 18(2). 106–125.

Herzberg, F., B. Mausner & B. Snyderman (1959). The Motivation to work. 2. painos. New York: John Wiley & Sons.

Hirsjärvi, S. & H. Hurme (2008). Tutkimushaastattelu: teemahaastattelun teoria ja käytäntö. Helsinki: Gaudeamus Helsinki University Press.

Hirsjärvi, S., P. Remes, & P. Sajavaara (2009). Tutki ja kirjoita. Helsinki: Tammi.

Hovav, A. & J. D'Arcy (2012). Applying an extended model of deterrence across cultures: an investigation of information systems misuse in the U.S. and South Korea. Information & Management. 49(2). 99–110.

Hui, K-L., W. Hui & W. Yue (2012). Information security outsourcing with system interdependency and mandatory security requirement. Journal of Management Information Systems. 29(3). 117–156.

Huigang, L. & X. Yajiong (2010). Understanding security behaviors in personal computer usage: a threat avoidance perspective. Journal of the Association for Information Systems. 11(7). 394–413.

Höne, K. & J. Eloff (2002a). What makes an effective information security policy? Network Security. 2002(6). 14–16.

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

Illeris, K. (2002). The three dimensions of learning. Frederiksberg: Roskilde University Press.

International Organization for Standardization (2009). New ISO/IEC standard gives overview of information security management systems. Julkaistu: 12.5.2010. [viitattu 5.2.2010]. Saatavissa: http://www.iso.org/iso/pressrelease.htm?refid=Ref1223.

International Organization for Standardization (2011a). JTC 1/SC 27. IT Security techniques. [viitattu 21.9.2011]. Saatavissa: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45306&published=on.

International Organization for Standardization (2011b). JTC 1/SC 27. [viitattu 21.9.2011]. Saatavissa: http://www.iso.org/iso/iso_technical_committee?commid=45306.

Jonassen, D. (1995). Supporting communities of learners with technology: a vision for integrating technology with learning in schools. Educational Technology. 35(4). 60–63.

Johnston, A. & M. Warkentin (2010). Fear appeals and information security behaviors: an empirical study. MIS Quarterly. 34(3). 549–566.

Jordan, E. & L. Silcock (2006). Strateginen IT-riskien hallinta. Helsinki: Edita Publishing Oy.

Järvelä, S., P. Häkkinen & E. Lehtinen (toim.) (2006). Oppimisen teoria ja teknologian opetuskäyttö. Helsinki: WSOY.

Järvinen, A. (1999). Facilitating knowledge processing in a workplace setting. Teoksessa: Forrester, K., N. Frost, D. Taylor & K. Ward (toim.) 1st international conference on researching work and learning proceedings. University of Leeds. England. 10th–12th September 1999. 677–682.

Kaha (2013). Oy Kaha Ab. Yrityksen www-sivuston etusivu. [viitattu 21.1.2013]. Saatavissa: http://www.kaha.fi/default.php?id=2.

Kalyga, S. & P. Chandler & J. Sweller (1998). Levels of expertise and instructional design. Human Factors. 40(1). 1–17.

Karjalainen, M. (2011). Improving employees' information systems (IS) security behavior. [viitattu 13.3.2012]. Saatavissa: http://herkules.oulu.fi/isbn9789514295676/isbn9789514295676.pdf.

Karjalainen, M. & M. Siponen (2011). Toward a new meta-theory for designing information systems (IS) security training approaches. Journal of the Association for Information Systems. 12(8). 518–555.

Keskuskauppakamari & Helsingin seudun kauppakamari (2008). Yritysten rikosturvallisuus 2008: Riskit ja niiden hallinta. [viitattu 10.5.2011]. Saatavissa: http://www.keskuskauppakamari.fi/content/download/7766/155752/yritysturvallisuusselvitys+2008.pdf.

Kolb, D. (1984). Experiental learning: Experience as a source of learning and development. Engelwood Cliffs. NJ: Prentice-Hall.

Ku, C-Y., Y-W. Chang & D. Yen (2009). National information security policy and its implementation: A case study in Taiwan. Telecommunications Policy. 33(7). 371–384.

Kull, A. (2012). A Method for Continuous Information Technology Supervision: The Case of the Estonian Financial Sector. Tampere: Tampere University Press. [viitattu 19.11.2013]. Saatavissa: http://urn.fi/urn:isbn:978-951-44-8689-0.

Kylmä, J. & T. Juvakka (2007). Laadullinen terveystutkimus. Helsinki: Edita Prima.

Laaksonen, M., T. Nevasalo & K. Tomula (2006). Yrityksen tietoturvakäsikirja. Ohjeistus, toteutus ja lainsäädäntö. Helsinki: Edita Publishing Oy.

Laukkanen, R. (2000). Aikuinen oppii eri tavalla. Aikuiskasvatus. 2/20. 167.

Lave, J. & E. Wenger (1991). Situated Learning. Legitimate Peripheral Participation. Cambridge: Cambridge University Press.

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

Leontjev, A. (1977). Toiminta, tietoisuus, persoonallisuus. Helsinki: Kansankulttuuri.

Leppänen, J. (2006). Yritysturvallisuus käytännössä. Turvallisuusjohtamisen portfolio. Helsinki: Gummerus Kirjapaino Oy.

Liikenne- ja viestintäministeriö (2008). Valtioneuvoston periaatepäätös kansalliseksi tietoturvastrategiaksi. [viitattu 28.4.2010]. Saatavissa: http://www.lvm.fi/c/document_library/get_file?folderId=57092&name=DLFE-5405.pdf&title=Valtioneuvoston%20periaatepäätös%20kansalliseksi%20tietoturvastrategiaksi%20(su/ru/eng%20LVM62/2008).

Liikenne- ja viestintäministeriö (2010a). Tietoturva. [viitattu 5.2.2010]. Saatavissa: http://www.lvm.fi/web/fi/tietoturva.

Liikenne- ja viestintäministeriö (2010b). Kilpailukykyinen ja ihmisläheinen tietoyhteiskunta. Arjen tietoyhteiskunnan neuvottelukunnan www-sivusto. [viitattu 16.4.2010]. Saatavissa: http://www.arjentietoyhteiskunta.fi/index.phtml?s=2.

Liikenne- ja viestintäministeriö (2010c). Arjen tietoyhteiskunnan tietoturvallisuus -ryhmä. Arjen tietoyhteiskunnan neuvottelukunnan www-sivusto. [viitattu 16.4.2010, 18.11.2011]. Saatavissa: http://www.arjentietoyhteiskunta.fi/index.phtml?s=10.

Liikenne- ja viestintäministeriö (2011). Lindén: Julkishallinnon tietoturvallisuus keskitettävä Viestintävirastolle. Julkaistu: 8.2.2011. [viitattu 15.2.2011]. Saatavissa: http://www.lvm.fi/web/fi/tiedote/view/1228818.

Lim, V., T. Teo & G. Loo (2002). How do I loaf here? Let me count the ways. Communications of the ACM. 45(1). 66–70.

Lincoln, Y. & E. Cuba (1985). Naturalistic Inquiry. Beverly Hills: Sage Publications.

Little, B. (1983). Personal projects: A rationale and method for investigation. Environment and Behavior. 15(3). 273–309.

Liukkonen, J. (2002). Rahasta vai rakkaudesta työhön. Jyväskylä: Likes-työelämäpalvelut.

Lowry, P., G. Moody, D. Galletta & A. Vance (2013). The drivers in the use of online whistle-blowing reporting systems. Journal of Management Information Systems. 30(1). 153–190.

Lämsä, A-M. & T. Hautala (2008). Organisaatiokäyttäytymisen perusteet. 1.-4. painos. Helsinki: Edita Prima Oy.

Marton, F. & S. Booth (1997). Learning and awareness. New Jersey: Lawrence Erlbaum Associates.

Maslow, A. (1943). A theory of human motivation. Psychological Review. 50(4). 370–396.

Mason, P. & K. Cosh (2008). Managing complexity in ICT systems development. International Journal of Information Technology and Management. 7(3). 264–282.

McClelland, D. (1976). The achieving society. New York: Irvington Publishers.

McClelland, D. (1978). Managing motivation to expand human freedom. American Psychologist. 33(3). 201–210.

Mensch, S. & L. Wilkie (2011). Information security activities of college students: an exploratory study. Academy of Information and Management Sciences Journal. 14(2). 91–116.

Moody, G. (2011). A multi-theoretical perspective on IS security behaviors. Väitöstutkimus. Oulu: Oulun yliopisto.

Murray, H. (1938). Explorations in personality. Oxford: Oxford University Press.

Myyry, L., M. Siponen, S. Pahnila, T. Vartiainen & A. Vance (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. European Journal of Information Systems. 18(2). 126–139.

Ng, B-Y., A. Kankanhalli & Y. Xu (2009). Studying users' computer security behavior: a health belief perspective. Decision Support Systems. 46(4). 815–825.

Niermeyer, R. & M. Seyffert (2004). Motivaatio. Helsinki: Oy Rastor Ab.

Niitamo, P. (2005) Tunneperäinen ja tietoperäinen motivaatio. Teoksessa: Mikä meitä liikuttaa. Modernin motivaatiopsykologian perusteet. Keuruu: PS-kustannus. 40–52.

Nurmi, J-E. & K. Salmela-Aro (2005). Modernin motivaatiopsykologian perusta ja käsitteet. Teoksessa: Mikä meitä liikuttaa. Modernin motivaatiopsykologian perusteet. Keuruu: PS-kustannus. 10–27.

Nuttin, J. (1984). Motivation, planning, and action: A relational theory of behavior dynamics. Leuven: Leuven University Press.

Nykänen, K. (2011). Tietoturvakoulutuksen vaikuttavuuden arviointi yksilön ja organisaation tietoturvakäyttäytymiseen. Väitöstutkimus. Oulu: Oulun yliopisto.

Opetus- ja kulttuuriministeriö (2012). Aikuiskoulutus. [viitattu 25.4.2012]. Saatavissa:
http://www.minedu.fi/OPM/Koulutus/aikuiskoulutus_ja_vapaa_sivistystyoe/.

Pahnila, S., M. Siponen & A. Mahmood (2007). Employees' behavior towards IS security police compliance. Proceedings of the 40th Hawaii international conference on system science.

Partanen, K. (2005). Tietoturvan tila pohjoiskarjalaisissa yrityksissä. Diplomityö. Lappeenranta: Lappeenrannan teknillinen yliopisto. [viitattu 19.11.2013]. Saatavissa: https://oa.doria.fi/handle/10024/35290.

Pollock, E. & P. Chandler & J. Sweller (2002). Assimilating complex information. Learning and Instruction. 12(1). 61–86.

Puhakainen, P. (2006). A design theory for information security awareness. Väitöstutkimus. Oulu: Oulun yliopisto.

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

Puolimatka, T. (2002). Opetuksen teoria. Konstruktivismista realismiin. Helsinki: Tammi.

Rasila, M. & M. Pitkonen (2010). Motivaatio, työn ilo ja into. Helsinki: Yrityskirjat Oy.

Rhee, H-S., C. Kim & Y. Ryu (2009). Self-efficacy in information security: its influence on end users' information security practice behavior. Computers & Security. 28(8). 816–826.

Robbins, P. (2001). Organizational Behaviour. New Jersey: Prentice-Hall inc.

Rogers, R. (1975). A protection motivation theory of fear appeals and attitude change1. The Journal of Psychology. 91(1). 93–114.

Rotvold, G. (2008). How to create a security culture in your organization: a recent study reveals the importance of assessment, incident response procedures, and social engineering testing in improving security awareness programs. Information Management. 42(6). 32–38.

Ruohotie, P. (1991). Motivaatio ja oppimisstrategiat ammatillisissa opinnoissa. Teoksessa: Ammattikasvatuksen tutkimus Hämeenlinnan tutkimusyksikössä 1990–1991. No 4. Hämeenlinna: Tampereen yliopisto. 85–121.

Ruohotie, P. (1998). Motivaatio, tahto ja oppiminen. Helsinki: Oy Edita Ab.

Ruokamo, H. & S. Pohjolainen (1999). Etäopetus multimediaverkoissa (ETÄ-KAMU) -tavoitetutkimushanke. Digitaalisen median raportti 1/99.

Saarenpää, A., T. Pöysti, M. Sarja, V. Still & R. Balboa-Alcoreza (1997). Tietoturvallisuus ja laki. Näkökohtia tietoturvallisuuden oikeudellisesta sääntelystä. Helsinki: Edita Oy.

Salmela-Aro, K. (2005). Motivaation mittaaminen. Esimerkkinä Brian Littlen henkilökohtaisten projektien menetelmä. Teoksessa: Mikä meitä liikuttaa. Modernin motivaatiopsykologian perusteet. Keuruu: PS-kustannus. 28–39.

Sarkar, K. (2010). Assessing insider threats to information security using technical, behavioural and organizational measures. Information Security Technical Report. 15(3). 112–133.

Sawyer, R. (toim.) (2006). The Cambridge handbook of the learning sciences. Cambridge: Cambridge University Press.

Siponen, M., S. Pahnila & A. Mahmood (2007). Emplyees' adherence to information security policies: An empirical study. IFIP SEC 2007 Conference, 14–16 May. Sandton, Gauteng. South Africa.

Siponen, M. & A. Vance (2010). Neutralization: new insights into the problem of employee systems security policy violations. MIS Quarterly. 34(3). 487–502.

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

Spears, J. & H. Barki (2010). User participation in information systems security risk management. MIS Quarterly. 34(3). 503–522.

Suomen Ekonomiliitto (2005). Johtajuus!. Keuruu: Otavan Kirjapaino Oy.

Suomen Standardisoimisliitto (2006). Kansainväliset uudet tietoturvastandardit nyt suomeksi. Julkaistu 3.8.2006. [viitattu 5.2.2010]. Saatavissa: http://www.sfs.fi/ajankohtaista/tiedotteet/20060803150421.html.

Suomen Standardisoimisliitto (2007). ISO/IEC 17799 on nyt ISO/IEC 27002. Julkaistu 21.9.2007. [viitattu 15.3.2011]. Saatavissa: http://www.sfs.fi/ajankohtaista/tiedotteet/20070921152430.html.

Suomen Standardisoimisliitto (2011a). Mikä SFS on? [viitattu 28.2.2011]. Saatavissa: http://www.sfs.fi/sfs_lyhyesti/index.html.

Suomen Standardisoimisliitto (2011b). Tietoturvatekniikat. [viitattu 21.9.2011]. Saatavissa: http://www.sfs.fi/it/aihealueet/tietoturva/.

Suomen Standardisoimisliitto (2011c). Standardit. [viitattu 21.9.2011]. Saatavissa: http://www.sfs.fi/it/aihealueet/tietoturva/standardit/index.html.

Suomi.fi-portaali (2008). Laatua verkkoon – Tietoturva. Päivitetty 5.5.2008. [viitattu 5.2.2010]. Saatavissa: http://www.suomi.fi/suomifi/laatuaverkkoon/suositukset_ja_ohjeet/tietoturva/index.html

Tekniikan sanastokeskus (2002). Tietotekniikan termitalkoot -projektin sivusto. Tietoturva. Päivitetty 17.4.2002. [viitattu 30.1.2010]. Saatavissa: http://www.tsk.fi/tsk/termitalkoot/haku-266.html.

Temizkan, O., R. Kumar, S. Park & C. Subramaniam (2012). Patch release behaviors of software vendors in response to vulnerabilities: An empirical analysis. Journal of Management Information Systems. 28(4). 305–338.

Thomson, K-L. & R. von Solms (2005). Information security obedience: a definition. Computers & Security. (24)1. 69–75.

Tian, J., Z. Shen & K-L. Wang (2010). Investigation of officials' behaviors of Internet abuse under E-Government in China. Journal of US-China public administration. 7(2). 16–23.

TIEKE Tietoyhteiskunnan kehittämiskeskus ry (2004a). Tietoturvaopas. Etusivu. [viitattu 9.4.2010]. Saatavissa: http://www.tieke.fi/julkaisut/oppaat_yrityksille/tietoturvaopas/.

TIEKE Tietoyhteiskunnan kehittämiskeskus ry (2004b). Huoneentaulu. Tietoturvan huoneentaulu. [viitattu 9.4.2010]. Saatavissa: http://www.tieke.fi/julkaisut/oppaat_yrityksille/tietoturvaopas/huoneentaulu/.

TIEKE Tietoyhteiskunnan kehittämiskeskus ry (2004c). Perusteluja. Miksi tietoturvan takia kannattaa nähdä vaivaa? [viitattu 9.4.2010]. Saatavissa: http://www.tieke.fi/julkaisut/oppaat_yrityksille/tietoturvaopas/perusteluja/.

TIEKE Tietoyhteiskunnan kehittämiskeskus ry (2004d). Alkuperä. Selvitä tiedon ja tiedoston alkuperä ennen käyttöä. [viitattu 9.4.2010]. Saatavissa: http://www.tieke.fi/julkaisut/oppaat_yrityksille/tietoturvaopas/huoneentaulu/alkupera/.

TIEKE Tietoyhteiskunnan kehittämiskeskus ry (2004e). Korvat. Muista, että seinillä on korvat – useammat kuin arvaatkaan. [viitattu 9.4.2010]. Saatavissa: http://www.tieke.fi/julkaisut/oppaat_yrityksille/tietoturvaopas/huoneentaulu/korvat/.

TIEKE Tietoyhteiskunnan kehittämiskeskus ry (2004f). Lukitse. Lukitse ovesi ja tietokoneesi, kun lähdet muualle. [viitattu 9.4.2010]. Saatavissa: http://www.tieke.fi/julkaisut/oppaat_yrityksille/tietoturvaopas/huoneentaulu/lukitse/.

TIEKE Tietoyhteiskunnan kehittämiskeskus ry (2004g). Salasana. Käytä salasanoja, joissa on muitakin merkkejä kuin kirjaimia, ja pidä ne salassa. [viitattu 9.4.2010]. Saatavissa: http://www.tieke.fi/julkaisut/oppaat_yrityksille/tietoturvaopas/huoneentaulu/salasana/.

TIEKE Tietoyhteiskunnan kehittämiskeskus ry (2004h). Älä hätäile. Älä hätäile, äläkä varsinkaan toimi hätiköidysti. [viitattu 9.4.2010]. Saatavissa: http://www.tieke.fi/julkaisut/oppaat_yrityksille/tietoturvaopas/huoneentaulu/ala_hataile/.

TIEKE Tietoyhteiskunnan kehittämiskeskus ry (2004i). Varmenna. Ota talteen kaikki tarpeellinen, ennen kuin vahinko sattuu. [viitattu 16.4.2010]. Saatavissa: http://www.tieke.fi/julkaisut/oppaat_yrityksille/tietoturvaopas/huoneentaulu/varmenna/.

TIEKE Tietoyhteiskunnan kehittämiskeskus ry (2004j). Virukset. Käytä ajantasaisia viruksentorjuntaohjelmia ja muita turvajärjestelmiä. [viitattu 16.4.2010]. Saatavissa: http://www.tieke.fi/julkaisut/oppaat_yrityksille/tietoturvaopas/huoneentaulu/virukset/.

TIEKE Tietoyhteiskunnan kehittämiskeskus ry (2004k). Omat järjestelyt. Selvitä itsellesi oman organisaatiosi tietoturvajärjestelyt. [viitattu 16.4.2010]. Saatavissa: http://www.tieke.fi/julkaisut/oppaat_yrityksille/tietoturvaopas/huoneentaulu/omat_jarjestelyt/.

TIEKE Tietoyhteiskunnan kehittämiskeskus ry (2004l). Pohdintaa. Miksi viruksia ja muita tietoturvaongelmia on? [viitattu 8.4.2010]. Saatavissa: http://www.tieke.fi/julkaisut/oppaat_yrityksille/tietoturvaopas/pohdintaa/.

TIEKE Tietoyhteiskunnan kehittämiskeskus ry (2004m). Jälkipuhe. Yleistä taustaa. [viitattu 8.4.2010]. Saatavissa: http://www.tieke.fi/julkaisut/oppaat_yrityksille/tietoturvaopas/jalkipuhe/

TIEKE Tietoyhteiskunnan kehittämiskeskus ry (2005a). Tietoturvakartoitus. Etusivu. [viitattu 12.2.2010]. Saatavissa: http://tietoturvakartoitus.tieke.fi/testi2.php?pg=1.

TIEKE Tietoyhteiskunnan kehittämiskeskus ry (2005b). Tietoturvakartoitus. [viitattu 12.2.2010]. Saatavissa: http://tietoturvakartoitus.tieke.fi/testi2.php?pg=31.

TIEKE Tietoyhteiskunnan kehittämiskeskus ry (2010). Tietoturva. [viitattu 12.2.2010]. Saatavissa: http://www.tieke.fi/verkkokaveri/teemat/tietoturva/.

TIEKE Tietoyhteiskunnan kehittämiskeskus ry (2011). TIEKE. [viitattu 27.9.2011]. Saatavissa: http://www.tieke.fi/tieke/.

Tietokone (2005). Liikesalaisuudet unohtuvat taksin takapenkille. Päivitetty: 24.1.2005. [viitattu 8.4.2010]. Saatavissa: http://www.tietokone.fi/uutiset/2005/liikesalaisuudet_unohtuvat_taksin_takapenkille.

Tietotekniikan liitto (2008). ATK-sanakirja 1. Helsinki: Talentum Media Oy.

Tietoturva ry (2010). Miten pääsen tietoturva-alalle? [viitattu 12.2.2010]. Saatavissa: http://www.ttlry.fi/yhdistykset/tietoturva/koulutus_ja_sertifioinnit/alalle_kouluttautuminen/

Tiivis tietoturvasanasto (2004). Helsinki: Taloustieto Oy.

Tilastokeskus (2006). Tietoyhteiskuntatilasto 2006. Helsinki: Yliopistopaino.

Tilastokeskus (2011). Pk-yritys. [viitattu 1.2.2011]. Saatavissa: http://www.stat.fi/meta/kas/pk_yritys.html.

Tuomi, J. & A. Sarajärvi (2009). Laadullinen tutkimus ja sisällönanalyysi. 5. uudistettu laitos. Helsinki: Tammi.

Tynjälä, P. (2000). Oppiminen tiedon rakentamisena. Konstruktivistisen oppimiskäsityksen perusteita. Helsinki: Tammer-Paino Oy.

Vaherva, T. (2002). Henkilöstökoulutuksen rajat ja mahdollisuudet. Teoksessa: Oppiminen ja asiantuntijuus. Työelämän ja koulutuksen näkökulmia. Toim. A. Eteläpelto & P. Tynjälä. Helsinki: Werner Söderström Osakeyhtiö. 83–101.

Valtiovarainministeriö (2003). Valtionhallinnon tietoturvakäsitteistö. VAHTI 4/2003. Julkaistu 26.11.2003. [viitattu 5.2.2010]. Saatavissa: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/50903/50902_fi.pdf.

Valtiovarainministeriö (2006). Tietoturvallisuuden arviointi valtionhallinnossa. VAHTI 8/2006. Julkaistu 20.7.2006. [viitattu 10.5.2011]. Saatavissa: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20060802Tietot/A_vahti_08_netti.pdf.

Valtiovarainministeriö (2008). Valtionhallinnon tietoturvasanasto. VAHTI 8/2008. Julkaistu 14.11.2008. [viitattu 5.2.2010]. Saatavissa:

http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20081211Valtio/Vahti_8_NETTI%2b_KANNET.pdf.

Valtiovarainministeriö (2010a). Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI. [viitattu 5.2.2010]. Saatavissa: http://www.vm.fi/vm/fi/13_hallinnon_kehittaminen/09_Tietoturvallisuus/01_tietoturvaryhma_VAHTI/index.jsp.

Valtiovarainministeriö (2010b). Voimassa olevat tietoturvaohjeet ja -määräykset. [viitattu 5.2.2010]. Saatavissa: http://www.vm.fi/vm/fi/13_hallinnon_kehittaminen/09_Tietoturvallisuus/02_tietoturvaohjeet_ja_maaraykset/index.jsp.

Valtiovarainministeriö (2010c). Tietoturvallisuus. [viitattu 12.2.2010]. Saatavissa: http://www.vm.fi/vm/fi/13_hallinnon_kehittaminen/09_Tietoturvallisuus/index.jsp.

Valtiovarainministeriö (2011). Valtionhallinnon tietoturvallisuus. [viitattu 26.5.2011, 28.2.2012]. Saatavissa: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/index.jsp.

Valtiovarainministeriö (2013). Voimassa olevat tietoturvaohjeet ja -määräykset. [viitattu 4.1.2013]. Saatavissa: http://www.vm.fi/vm/fi/16_ict_toiminta/009_Tietoturvallisuus/02_tietoturvaohjeet_ja_maaraykset/index.jsp.

Vance, A. (2010). Why do employees violate IS security policies? Acta universitatis Ouluensis. [viitattu 21.11.2013]. Saatavissa: http://herkules.oulu.fi/isbn9789514262876/isbn9789514262876.pdf.

Vartiainen, M. & K. Nurmela (2005). Tavoitteet ja tulkinnat – motivaatio ja palkitseminen työelämässä. Teoksessa: Mikä meitä liikuttaa. Modernin motivaatiopsykologian perusteet. Keuruu: PS-kustannus. 188–212.

Viestintävirasto (2009a). Tietoturvalliseen yhteiskuntaan. Päivitetty 16.9.2009. [viitattu 5.3.2010]. Saatavissa: http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva.html.

Viestintävirasto (2009b). Liikkuvan työn tietoturvan suurin riski on ihminen. Päivitetty 4.2.2009. [viitattu 7.5.2010]. Saatavissa: http://www.ficora.fi/index/viestintavirasto/lehdistotiedotteet/2009/P_8.html.

Viestintävirasto (2010a). Yrityksen tietoturvaopas. [viitattu 5.3.2010]. Saatavissa: http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/index.html.

Viestintävirasto (2010b). Tietoturvaohjeet (malli). [viitattu 5.3.2010]. Saatavissa: http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/pdf/Tietoturvaohjeet.pdf.

Viestintävirasto (2010c). Tietoturvakartoitus-kysymyslista. [viitattu 5.3.2010]. Saatavissa: http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/pdf/Tietoturvakartoitus_kysymyslista.pdf.

Viestintävirasto (2010d). Tietoturvaohjelman avainkohdat. [viitattu 5.3.2010]. Saatavissa: http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/pdf/Tietoturvasuunnitelman_avainkohdat.pdf.

Viestintävirasto (2010e). Toimiva tietoturva (sivut 1/7–7/7). [viitattu 5.3.2010]. Saatavissa: http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/toimiva_tietoturva.html.

Viestintävirasto (2010f). Tilanteen kartoitus (sivut 1/7–7/7). [viitattu 5–12.3.2010]. Saatavissa: http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/tilanteen_kartoitus.html.

Viestintävirasto (2010g). Suunnittelu (sivut 1/13–13/13). [viitattu 12.3.2010]. Saatavissa: http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/suunnittelu.html.

Viestintävirasto (2010h). Internet-pelisäännöt. [viitattu 12.3.2010]. Saatavissa: http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/internetpelisaannot.html.

Viestintävirasto (2010i). Tietoturva tavaksi (sivut 1/6–6/6). [viitattu 12.3.2010]. Saatavissa: http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/tietoturva_tavaksi.html.

Viestintävirasto (2010j). Salassapitosopimuksen avainkohdat. [viitattu 12.3.2010]. Saatavissa: http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/pdf/Salassapitosopimuksen_avainkohdat.pdf.

Viestintävirasto (2010k). Liikkuva työ (sivut 1/7–7/7). [viitattu 8.4.2010]. Saatavissa: http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/liikkuva_tyo.html.

Viestintävirasto (2011). Kansallinen tietoturvaviranomainen NCSA-FI. Päivitetty 20.1.2011. [viitattu 15.2.2011]. Saatavissa: http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/ncsa-fi.html.

Vroom, V. (1964). Work and motivation. Oxford: Wiley.

VTT (2009a). Kärkiohjelmat ja suuret innovaatio-ohjelmat. [viitattu 23.4.2010]. Saatavissa: http://www.vtt.fi/research/spearhead_and_innovation_programmes.jsp.

VTT (2009b). Teknologia- ja innovaatiostrategia. [viitattu 23.4.2010]. Saatavissa: http://www.vtt.fi/research/technology_and_innovation_strategy.jsp.

VTT (2009c). Tietoturva. [viitattu 23.4.2010]. Saatavissa: http://www.vtt.fi/research/innovation_infsecurity.jsp.

VTT (2009d). Tietoturva. Tutkimusalueet. [viitattu 23.4.2010]. Saatavissa: http://www.vtt.fi/research/area/information_and_network_security.jsp.

VTT (2009e). Pk-yrityksen riskienhallinta. [viitattu 23.4.2010]. Saatavissa: http://www.pk-rh.fi/.

VTT (2009f). Startti riskienhallintaan. [viitattu 23.4.2010]. Saatavissa: http://www.pk-rh.fi/startti-riskienhallintaan.

VTT (2009g). Riskienhallinnan hyödyt. [viitattu 23.4.2010]. Saatavissa: http://www.pk-rh.fi/startti-riskienhallintaan/riskienhallinnan-hyodyt/.

VTT (2009h). Riskilajit. [viitattu 23.4.2010]. Saatavissa: http://www.pk-rh.fi/riskilajit.

VTT (2009i). Liikeriskit. [viitattu 23.4.2010]. Saatavissa: http://www.pk-rh.fi/riskilajit/liikeriskit/.

VTT (2009j). Henkilöriskit. [viitattu 23.4.2010]. Saatavissa: http://www.pk-rh.fi/riskilajit/henkiloriskit/henkiloriskit/.

VTT (2009k). Tietoriskit. [viitattu 23.4.2010]. Saatavissa: http://www.pk-rh.fi/riskilajit/tietoriskit/tietoriskit/.

VTT (2009l). Tietoriskien tunnistaminen ja hallinta. [viitattu 23.4.2010]. Saatavissa: http://www.pk-rh.fi/riskilajit/tietoriskit/tietoriskien-tunnistaminen-ja-hallinta.

VTT (2009m). Tuoteriskit. [viitattu 23.4.2010]. Saatavissa: http://www.pk-rh.fi/riskilajit/tuoteriskit/tuoteriskit/.

(VTT 2009n). Mitä ovat ympäristöriskit? [viitattu 23.4.2010]. Saatavissa: http://www.pk-rh.fi/riskilajit/ymparistoriskit/mita-ovat-ymparistoriskit/.

(VTT 2009o). Projektiriskit. [viitattu 23.4.2010]. Saatavissa: http://www.pk-rh.fi/riskilajit/projektiriskit/projektiriskit/.

VTT (2009p). Rikosriskit. [viitattu 23.4.2010]. Saatavissa: http://www.pk-rh.fi/riskilajit/rikosriskit/rikosriskit/.

VTT (2009q). Riskienhallinnan perusvaatimukset. [viitattu 23.4.2010]. Saatavissa: http://www.pk-rh.fi/perusvaatimukset/riskienhallinnan-perusvaatimukset/.

VTT (2009r). Riskienhallinnan perusvaatimukset. [viitattu 23.4.2010]. Saatavissa: http://www.pk-rh.fi/perusvaatimukset/riskienhallinnan-perusvaatimukset/riskienhallinnan-perusvaatimukset/.

VTT (2009s). Yrityksen riskien kartoittaminen. [viitattu 23.4.2010]. Saatavissa: http://www.pk-rh.fi/tyovalineet/yrityksen-riskien-kartoittaminen.

VTT (2009t). Mitä haavoittuvuusanalyysi on? [viitattu 23.4.2010]. Saatavissa: http://www.pk-rh.fi/tyovalineet/haavoittuvuusanalyysi-1/mita-haavoittuvuusanalyysi-on.

VTT (2009u). Riskien hallinta: kehittämistoimenpiteet. [viitattu 23.4.2010]. Saatavissa: http://www.pk-rh.fi/tyovalineet/haavoittuvuusanalyysi-1/riskien-hallinta-kehittamistoimenpiteet.

VTT (2010). VTT:n www-sivuston etusivu. Päivitetty 25.3.2010. [viitattu 23.4.2010]. Saatavissa: http://www.vtt.fi/.

Yleinen suomalainen asiasanasto - YSA (2011). Tietoturva. [viitattu 17.9.2011]. Saatavissa: http://www.yso.fi/onto/ysa/Y106522.

Yritysturvallisuus EK Oy (2001). Ovatko yrityksesi tietoriskit hallinnassa? Käytännön tietoturvallisuusopas pk-yrityksille. [viitattu 7.5.2010]. Saatavissa: http://ek2.ek.fi/ytnk08/fi/julkaisut_liitteet/Tietoturva.pdf.

Yritysturvallisuus EK Oy (2008). Tiedotteet. Pk-yritysten tietoturvaopas. Päivitetty 5.8.2010. [viitattu 7.5.2010, 20.9.2011]. Saatavissa: http://ek2.ek.fi/ytnk08/fi/tiedotteet.php.

Yritysturvallisuus EK Oy (2009a). Yritysturvallisuus. Päivitetty 17.8.2009. [viitattu 7.5.2010]. Saatavissa: http://ek2.ek.fi/ytnk08/fi/yritysturvallisuus.php.

Yritysturvallisuus EK Oy (2009b). Yritysturvallisuus EK. Päivitetty 17.8.2009. [viitattu 7.5.2010]. Saatavissa: http://ek2.ek.fi/ytnk08/fi/yleista.php.

Yritysturvallisuus EK Oy (2010). Yritysturvallisuus EK Oy:n www-sivuston kotisivu. Päivitetty 7.5.2010. [viitattu 7.5.2010]. Saatavissa: http://ek2.ek.fi/ytnk08/fi/index.php.

Zuboff, S. (1990). Viisaan koneen aikakausi. Uusi tietotekniikka ja yritystoiminta. Keuruu: Otava.

LIITTEET

Liite 1. Kansallinen turvallisuusauditointikriteeristö tietoturvalle.

Hallinnollisen tietoturvan kriteerit (Elinkeinoelämän keskusliitto EK ym. 2009: 62–68).

Kysymys	**Lähtötason suositukset**
Onko organisaation tietoturvallisuudella johdon tuki?	Organisaation tietoturvallisuudella on johdon tuki. Vaaditaan vähintään, että 1) tietoturvallisuus on vastuutettu (johdon vastuut, tietohallinnon/ järjestelmien ylläpidon vastuut, peruskäyttäjän vastuut, jne.); 2) organisaatiolla on johdon hyväksymät tietoturvaperiaatteet ja -käytänteet; 3) tietoturvaperiaatteet ja -käytänteet on saatettu koko yrityksen tietoon; 4) tietoturvaperiaatteet ja -käytänteet katselmoidaan aina, kun merkittäviä muutoksia tapahtuu; 5) johto edellyttää, että työntekijät, toimittajat ja ulkopuoliset tietojen käsittelijät toimivat organisaation tietoturvaperiaatteiden mukaisesti; 6) tietoturvallisuudelle on varattu tarvittavat resurssit.
Onko yrityksellä dokumentoitu ohjelma tietoturvallisuuden johtamiseksi ja turvallisuustyön tavoitteiden saavuttamiseksi?	Organisaatiolla on tietoturvasuunnitelma, toimintaohje, tai vastaava, ja siihen liittyvät ohjeet tarpeen mukaan. Vaaditaan, että 1) suunnitelma sisältää kuvaukset ainakin hallinnollisesta, fyysisestä ja tietoteknisestä tietoturvallisuudesta; 2) suunnitelma ottaa huomioon mahdollisen toimintaa säätelevän lainsäädännön (ml. tietosuoja); 3) suunnitelmaan liittyvät ohjeet ovat riittäviä suhteessa organisaatioon ja suojattavaan kohteeseen.
Pääkysymys:	1) Suojattavat kohteet (assets) on tunnistettu.

Onko toiminnalle tärkeät suojattavat kohteet (toiminnot, tiedot, järjestelmät) tunnistettu? Lisäkysymykset: Mitä uhkia niihin kohdistuu? Onko suojattaville kohteille määritetty vastuuhenkilöt?	2) Suojattaviin kohteisiin kohdistuvat uhat on tunnistettu. 3) Suojattaville kohteille on nimetty omistaja/vastuuhenkilö. 4) Suojattavien kohteiden suojausmenetelmät on suhteutettu kohteisiin sekä niihin kohdistuviin riskeihin.
Miten suojattaviin kohteisiin kohdistuvia riskejä arvioidaan?	1) Suojattaviin kohteisiin kohdistuvia riskejä arvioidaan jollain järjestelmällisellä menetelmällä. 2) Arviointi tapahtuu vähintään vuosittain ja lisäksi merkittävien muutosten yhteydessä. 3) Valitut suojausmenetelmät on asianmukaisesti suhteutettu kohteisiin sekä niihin kohdistuviin riskeihin. 4) Johto on hyväksynyt valitut suojausmenetelmät ja jäännösriskit.
Pääkysymys: Miten organisaation tietoturvallisuutta arvioidaan? Lisäkysymys: Kehitetäänkö toimintaa havaintojen perusteella?	Tietoturvallisuuden tasoa seurataan säännöllisesti.
Onko tietoturvallisuudesta huolehdittu alihankinta-, palveluhankinta- ja muissa vastaavissa yhteistyökuvioissa?	Tarjouspyyntöihin on liitetty tietoturvavaatimukset.
Miten organisaatiossa toimitaan tietoturvapoikkeamatilanteissa?	Tietoturvapoikkeamien hallinta on 1) suunniteltu, 2) ohjeistettu/koulutettu, ja erityisesti 3) viestintäkäytännöt ja -vastuut on sovittu.
Pääkysymys: Onko toiminnan lakisääteiset vaatimukset huomioitu? Lisäkysymys: Ovatko esimerkiksi henkilötietojen käsittelyn prosessit henkilötietolain edellyttämällä tasolla?	Toimintaa koskevat laki- ja sopimusperustaiset vaatimukset on tunnistettu ja täytetty.

Onko yrityksessä menettely, jonka avulla varmistetaan, että merkittävät tietojenkäsittely-ympäristön muutokset tapahtuvat hallitusti?	Tietojenkäsittelyyn liittyviin muutoksiin on käytössä muutoshallintamenettely.
Ovatko kaikki tietoverkot ja -järjestelmät yrityksen tietoturvaperiaatteiden mukaisesti suojattuja?	Kaikki tietoverkot ja -järjestelmät ovat organisaation tietoturvaperiaatteiden mukaisesti suojattuja.

Henkilöstöturvallisuuden kriteerit osana tietoturvaa (Elinkeinoelämän keskusliitto EK ym. 2009: 68–73).

Kysymys	**Lähtötason suositukset**
Hallitaanko kaikkien käyttäjien pääsy- ja käyttöoikeuksia hyvän tiedonhallintatavan mukaisesti?	1) Käyttöoikeuden myöntämisen yhteydessä tarkistetaan, että oikeuden saaja kuuluu henkilöstöön tai on muutoin oikeutettu. 2) On olemassa selkeä ja toimiva tapa muutosten ilmoittamiseen ja tarvittavien muutosten tekemisiin. 3) Käyttö- ja pääsyoikeuksien muutokset välittyvät sekä fyysiseen (kulunvalvonta jne.) että loogiseen pääsyyn ja käyttöön. 4) Järjestelmien käyttöoikeuksien hallintaan on nimetty vastuuhenkilö. 5) Käyttöoikeuksien käsittely ja myöntäminen ohjeistettu. 6) Käyttäjillä on vain ne oikeudet, joita he tarvitsevat tehtäviensä hoitamiseen. Pääsy on rajattu vain omiin työtehtäviin liittyviin verkkoihin, tietoihin ja järjestelmiin.
Onko salassapito- tai vaitiolositoumukset laadittu ja otettu käyttöön siten, että ne vastaavat organisaation tietojen suojaamistarpeita?	Salassapito- tai vaitiolositoumukset vastaavat organisaation tietojen suojaamistarpeita.
Pääkysymys:	Organisaation avainhenkilöt on tunnistettu ja

Onko avainhenkilöt sekä organisaation riippuvuus heistä tunnistettu? Lisäkysymys: Onko heidän varalleen suunniteltu varahenkilöt tai -menettelyt?	varahenkilöjärjestelmä on perustettu.
Onko organisaatiossa huolehdittu riittävästä ohjeistuksesta, koulutuksesta ja tiedotuksesta?	Organisaatiossa on huolehdittu riittävästä ohjeistuksesta ja koulutuksesta. Henkilöstö on saanut perehdytyksen yhteydessä ohjeet, kuinka toimia organisaation turvaperiaatteiden mukaisesti. Ohjeistuksen/koulutuksen tulee sisältää tärkeimmät toimintatilanteet (peruskäyttö, etäkäyttö, matkatyö, ylläpito, jne.) ja -tavat.
Onko tietoon ja tietojenkäsittelypalveluihin määritetty hyväksyttävän käytön säännöt ja onko niistä tiedotettu henkilöstölle?	1) Hyväksyttävän käytön säännöt on määritetty. 2) Dokumentoidut säännöt ovat henkilöstölle helposti saatavilla.
Valvotaanko organisaatiossa tietoturvaohjeiden noudattamista ja onko tietoturvarikkomusten käsittely ja seuraukset määritelty?	Tietoturvaohjeiden noudattamista valvotaan ja rikkeisiin puututaan.
Pääkysymys: Millaisia menettelytapoja organisaatiolla on tunnistaa ulkopuoliset työntekijät sekä vierailijat? Lisäkysymys: Onko henkilöstö ohjeistettu vieraiden isännöintiä varten?	Henkilöstö on ohjeistettu vierailijoiden isännöintiä varten.

Fyysisen turvallisuuden kriteerit osana tietoturvaa (Elinkeinoelämän keskusliitto EK ym. 2009: 73–75).

Kysymys	**Lähtötason suositukset**
Pääkysymys: Miten suojattavaa tietoa sisältävän tilan fyysisestä turvallisuudesta on huolehdittu? Lisäkysymys: Miten kulunvalvonta on järjestetty?	Toimistojen, tilojen ja laitteistojen fyysinen turvallisuus on suunniteltu ja toteutettu riskiarvion mukaisilla menetelmillä. Suojattavat tiedot, niitä käsittelevät laitteistot, oheislaitteet ja tietovälineet on sijoitettu ja suojattu niin, että niihin ei ole pääsyä ulkopuolisilla.
Tapahtuvatko laitetilan ja sen laitteistojen huolto-, asennus- ja siivoustoimet vain valvottuina?	Laitetilan ja sen laitteistojen huolto-, asennus- ja siivoustoimet tapahtuvat riskienarvioinnin mukaisesti. Riskienarvioinnissa voidaan päätyä hyväksymään toimet esim. vain oman henkilöstön valvomana, sähköisellä tallentavalla kulunvalvonnalla (esim. sähköinen kulkuavain ja koodi) järjestettynä, ja/tai sopimuksin suojattuna.
Miten on varauduttu salakuunteluun, hajasäteilyyn ja vastaaviin uhkiin?	Tilojen äänieristyksen täytyy olla riittävä, jottei normaali puheääni kuulu sellaisen tilan ulkopuolelle, jossa keskustellaan salassa pidettävistä asioista. Henkilöstölle on muistutettava, että taukopaikoilla (tupakkakopit jne.) ei saa keskustella salassa pidettävistä asioista.
Pääkysymys: Onko LVIS-järjestelyt varmistettu niin, että ne vastaavat organisaation toimintavaatimuksia? Lisäkysymys: Ovatko organisaation kriittiset laitteistot häiriöttömän sähkönsyötön (UPS) piirissä?	Kriittiset laitteistot ovat tunnistetut ja tarvittaviin toimenpiteisiin on ryhdytty.
Ovatko näyttöpäätteet asetetut siten, ettei salassa pidettävää tietoa paljastu ohikulkijoille tai muille asiattomille?	Näyttöpäätteet on asetettu harkiten siten, ettei tieto paljastu asiattomille.

Tietoliikenneturvallisuuden kriteerit (Elinkeinoelämän keskusliitto EK ym. 2009: 75–80).

Kysymys	**Lähtötason suositukset**
Onko tietoliikenneverkon rakenne turvallinen?	1) Ei-luotettuihin verkkoihin ei kytkeydytä ilman palomuuriratkaisua. Erityisesti Internet-verkon on oltava erotettu palomuurilla organisaation tietoverkoista ja -järjestelmistä. 2) Palomuuri- ja VPN-konfiguraatiot ovat organisaation tietoturvaperiaatteiden mukaisia ja dokumentoituja.
Pääkysymys: Ovatko palomuurien ja vastaavien liikennettä suodattavien laitteiden säännöstöt hyvien tietoturvaperiaatteiden mukaisia? Lisäkysymys: Onko varauduttu yleisimpiin nykyisiin verkkohyökkäyksiin?	1) Säännöstöt estävät oletuksena kaiken liikenteen, mitä ei ole erikseen sallittu (default-deny). 2) Määrittelemätön liikennöinti on estetty molempiin suuntiin. 3) Yleisiin verkkohyökkäyksiin on varauduttu konfiguroimalla palomuuri estämään verkkohyökkäykset.
Miten varmistutaan siitä, että liikennettä suodattavat tai valvovat järjestelmät toimivat halutulla tavalla?	1) Organisaatiossa on vastuutettu ja organisoitu palomuurien ja muiden suodatuslaitteiden sääntöjen lisääminen, muuttaminen ja poistaminen. 2) Suodatussäännöt on dokumentoitu
Onko hallintayhteydet suojattu asianmukaisesti?	Verkkojen ja tietojärjestelmien (ml. palvelimet, työasemat, verkkolaitteet ja vastaavat) hallintaliikenne on eriytettyä ja/tai salattua.
Ovatko verkon aktiivilaitteet kovennettuja (konfiguroituja organisaation omilla parametreilla tehdasparametrien sijasta)?	Verkon aktiivilaitteet on kovennettu organisaation yhtenäisen menettelytavan mukaisesti. Käytännössä vaaditaan ainakin, että 1) oletussalasanat on vaihdettu, 2) vain tarpeellisia verkkopalveluita on päällä, 3) verkkolaitteiden ohjelmistoihin on asennettu tarpeelliset turvapäivitykset.

Ovatko langattomien verkkojen perussuojaukset käytössä?	1) Organisaation hallinnoimien langattomien verkkojen käyttö sallitaan vain tunnistetuille ja valtuutetuille käyttäjille. 2) Liikenne salataan luotettavasti. 3) "Vierasverkoille", joista ei ole pääsyä organisaation sisäverkkoon, suositellaan, mutta ei vaadita salausta ja käyttäjien tunnistamista.
Onko sisäverkon rakenteen näkyminen Internetiin estetty?	Ei erityissuosituksia. Perustason vaatimukset: Tietoliikenne ei saa paljastaa organisaation sisäverkon rakennetta.
Pääkysymys: Miten verkkoa, järjestelmiä ja niiden käyttöä valvotaan? Lisäkysymys: Onko resurssit mitoitettu toimintavaatimusten mukaisiksi?	Ei erityissuosituksia. Perustason vaatimukset: Verkkoliikenteen normaali tila (baseline) on tiedossa. On vähintään oltava tiedossa normaalit liikennemäärät ja käytetyt protokollat verkon eri osissa.

Tietojärjestelmäturvallisuuden kriteerit (Elinkeinoelämän keskusliitto EK ym. 2009: 81–93).

Kysymys	**Lähtötason suositukset**
Tunnistetaanko ja todennetaanko käyttäjät ennen pääsyn sallimista organisaation tietoverkkoon ja -järjestelmiin?	Käyttäjät tunnistetaan ja todennetaan ennen pääsyn sallimista organisaation tietoverkkoon ja -järjestelmiin.
Onko organisaatiossa menettelytapa, jolla uudet järjestelmät (työasemat, kannettavat tietokoneet, palvelimet, verkkolaitteet, verkkotulostimet ja vastaavat) asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus?	Käytössä on menettelytapa, jolla uudet järjestelmät (työasemat, kannettavat tietokoneet, palvelimet, verkkolaitteet, ja vastaavat) asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus. Työasemilta ja kannettavilta tietokoneilta vaaditaan, että 1) alusta sisältää vain järjestelmän tarvitsemia ohjelmistokomponentteja; 2) tarjottavat (erityisesti verkko-)palve-

	lut minimoitu ja rajattu vain välttämättömiin; 3) käyttöjärjestelmään ja sovellusohjelmistoihin on asennettu tarpeelliset turvapäivitykset; 4) järjestelmiin asennuksen yhteydessä automaattisesti luoduille tileille (esim. "administrator" ja "guest") on oikeudet rajattu minimiin tai poistettu käytöstä; 5) oletussalasanat on vaihdettu; 6) työasemat lukittuvat automaattisesti, jos niitä ei käytetä vähään aikaan (minimivaatimus: salasanasuojattu näytönsäästäjä aktivoituu 10 minuutin käyttämättömyyden jälkeen); 7) käyttöoikeudet asetettu I 203.0:n mukaisesti; 8) lokimenettelyt asetettu. Palvelimilta vaaditaan LISÄKSI, että a) alustan komponenttien, prosessien (esim. palvelinprosessit), hakemistojen ja lisäohjelmien käyttöoikeudet on asetettu tarkoituksenmukaisiksi vähimpien oikeuksien periaatteen mukaisesti; b) palvelimet konfiguroitu valmistajien ja luotettujen tahojen ohjeiden mukaisesti. Verkkolaitteiden vaatimukset: I 405.0. Verkkotulostimet, puhelinjärjestelmät ja vastaavat: Soveltaen vastaavat vaatimukset kuin työasemilla ja palvelimilla: (verkko-)palvelut karsittava tarvittaviin, oletushallintatunnukset vaihdettava, tarpeelliset turvapäivitykset asennettava.
Miten on pienennetty haittaohjelmien aiheuttamia riskejä?	Haittaohjelmien havaitsemis- ja estotoimet sekä niistä toipumismekanismit ja asiaankuuluvat käyttäjien valppautta lisäävät ohjeet otettu käyttöön. Käytännössä vaaditaan, että ainakin 1) haittaohjelmantorjuntaohjelmistot

	on asennettu kaikkiin sellaisiin järjestelmiin, jotka ovat yleisesti alttiita haittaohjelmatartunnoille (erityisesti työasemat, kannettavat tietokoneet ja palvelimet); 2) torjuntaohjelmistot ovat toimintakykyisiä ja käynnissä; 3) torjuntaohjelmistot tuottavat havainnoistaan lokitietoja; 4) haittaohjelmatunnisteet päivittyvät säännöllisesti; 5) Käyttäjiä on ohjeistettu haittaohjelmauhkista ja organisaation tietoturvaperiaatteiden mukaisesta toiminnasta
Pääkysymys: Miten organisaation lokimenettelyt on toteutettu? Lisäkysymys: Kerätäänkö verkoista, laitteista ja järjestelmistä keskeiset lokitiedot ja käsitelläänkö niitä asianmukaisesti?	1) Tallenteiden kattavuus on riittävä tietomurtojen tai niiden yritysten jälkikäteiseen todentamiseen. 2) Keskeisiä tallenteita säilytetään 24 kk tai erillisessä sopimuksessa määrätty aika. 3) Luottamukselliset lokitiedot on suojattu asianmukaisesti (pääsynvalvonta, käsittely, poisto).
Miten salassa pidettävät tiedot säilytetään tietojärjestelmissä?	Tietojärjestelmissä sensitiivisten tietojen jakelu hoidetaan käyttöoikeusmäärittelyillä ja järjestelmän käsittelysäännöillä tai jollain vastaavalla menettelyllä.
Kuinka varmistutaan siitä, että luottamuksellista tietoa sisältävät liikuteltavat kiintolevyt, muistit, mediat, älypuhelimet, ja vastaavat ovat aina suojattuja luvatonta pääsyä vastaan?	1) Sensitiivistä tietoa sisältävät kannettavien tietokoneiden kiintolevyt, USB-muistit, tallennusmediat ja vastaavat ovat luotettavasti suojattuja. 2) Sensitiivistä tietoa sisältävät älypuhelimet suojataan riskiarvion mukaisesti.
Kuinka varmistutaan siitä, etteivät salassa pidettävät tiedot joudu kolmansille osapuolille huoltotoimenpiteiden tai käytöstä poiston yhteydessä?	1) Kaikki sensitiivistä tietoa sisältävät laitteistojen osat (kiintolevyt, muistit, muistikortit, jne.) tyhjennetään luotettavasti käytöstä poiston tai huoltoon lähetyksen yhteydessä. Mikäli luotetta-

	va tyhjennys ei ole mahdollista, sensitiivistä tietoa sisältävä osa on tuhottava mekaanisesti. 2) Kolmannen osapuolen suorittamia huoltotoimenpiteitä valvotaan, jos laitteen muistia tai vastaavaa ei voida luotettavasti tyhjentää ennen huoltotoimenpiteitä. 3) Suositellaan turvallisuussopimuksen tekemistä huoltoyhtiön kanssa.
Pääkysymys: Miten varmistutaan, ettei organisaation verkossa ole luvattomia laitteita tai järjestelmiä? Lisäkysymykset: Miten tiedetään mitä (tietojärjestelmiin liittyviä) laitteita organisaatiossa on käytössä? Miten hallitaan tietoa käytetyistä ohjelmistoista ja niiden versio- ja lisenssitilanteesta? Havaitaanko, jos laite viedään luvatta pois organisaation tiloista? Havaitaanko, jos järjestelmiin on asennettu luvattomia ohjelmistoja? Tarkistetaanko kaikki tilat, joista on mahdollista päästä organisaation verkkoon, säännöllisesti luvattomien laitteistojen ja ohjelmistojen havaitsemiseksi?	1) Laitteista pidetään laiterekisteriä, johon kirjataan myös hävitetyt/käytöstä poistetut laitteet. 2) Ohjelmistoista pidetään rekisteriä, johon kirjataan käytössä olevat ohjelmistot ja lisenssit.
Miten on varmistuttu siitä, että käytetyt salausratkaisut ovat riittävän turvallisia?	Käytetään tunnettuja ja yleisesti luotettavina pidettyjä salausratkaisuja, tai ratkaisun luotettavuudesta on varmistuttu jollain muulla luotettavalla menetelmällä.
Salausavainten hallinta. Pääkysymys: Ovatko salaiset avaimet vain valtuutettujen käyttäjien ja prosessien käytössä? Lisäkysymys:	Vaaditaan, että salaiset avaimet ovat vain valtuutettujen käyttäjien ja prosessien käytössä.

Ovatko salausavaintenhallinnan prosessit ja käytännöt dokumentoituja ja asianmukaisesti toteutettuja?	
Käytetäänkö istunnonhallinnassa tunnettua ja luotettavana pidettyä tekniikkaa?	Istunnonhallinnassa käytetään tunnettua ja luotettavana pidettyä tekniikkaa tai istunnon kaappaus ja kloonaus on muuten tehty huomattavan vaikeaksi. Mikäli ei käytetä tunnettua tekniikkaa, huolehdittava kuntoon ainakin 1) suljettujen istuntojen uudelleenaktivoinnin esto, 2) istuntoavainten eriytys niiden lähettämisessä käytetyistä avaimista, 3) istunnon sulkeminen mikäli ei käyttäjäaktiviteetteja tiettyyn aikaan, 4) istuntojen pituuksien rajoitukset.
Onko huolehdittu, että autentikaatiodataa ei säilytetä tietojärjestelmissä selväkielisinä?	Autentikaatiodataa (kuten salasanoja, sormenjälkiä, jne.) ei säilytetä tietojärjestelmissä selväkielisinä. Tietojärjestelmissä voidaan säilyttää vain yksisuuntaisella tiivistefunktiolla, tai vastaavalla luotettavana pidetyllä menetelmällä autentikaatiodatasta saatuja tiivisteitä.
Miten on varmistuttu ajettavan koodin turvallisuudesta?	Ohjelmistoja hankitaan ja asennetaan vain luotettavista ja luvallisista lähteistä.

Tietoaineistoturvallisuuden kriteerit (Elinkeinoelämän keskusliitto EK ym. 2009: 94–99).

Kysymys	**Lähtötason suositukset**
Millainen tiedon luokittelumenettely organisaatiolla on?	Tiedot on luokiteltu niiden merkittävyyden ja/tai lakisääteisten vaatimusten perusteella.
Onko huolehdittu siitä, että salassa pidettäviä tietoa sisältäviä aineistoja ja	Salassa pidettävälle aineistolle on työtiloissa lukitut kaapit, kassakaapit tai

tietovälineitä säilytetään turvallisesti?	vastaavat.
Hävitetäänkö luottamuksellisia tietoja sisältävät aineistot luotettavasti?	1) Luottamuksellisten sähköisten aineistojen hävittäminen tapahtuu luotettavasti (ylikirjoitus tai tallenteen fyysinen tuhoaminen). 2) Ei-sähköisten luottamuksellisten aineistojen tuhoaminen on järjestetty luotettavasti.
Onko salassa pidettävän aineiston kopiointi ja tulostus järjestetty turvallisesti?	Sensitiivisen aineiston kopiointi ja tulostus on järjestetty riskienarvioinnissa riittävän turvalliseksi katsotulla menettelyllä.
Pääkysymys: Onko salassa pidettävän aineiston sähköinen välitys järjestetty turvallisesti? Lisäkysymys: Onko tietoliikenne (ml. sähköinen viestintä) suojattu riskeihin nähden riittävillä mekanismeilla?	1) Organisaatiossa pystytään tunnistamaan sensitiiviset/salassa pidettävät tiedot ja huolehtimaan siitä, että ne välitetään asianmukaisesti suojaten. 2) Yhteys sähköpostipalvelimen ja -asiakasohjelman välillä on suojattu. 3) Mikäli sähköpostissa, pikaviestimissä, VoIPpuheluissa ja vastaavissa käsitellään sensitiivistä tietoa, on liikenne (tai viesti) suojattava riskienarvioinnin mukaisesti siten, että sensitiivistä tietoa ei pääse vuotamaan ulkopuolisille.
Onko salassa pidettävän aineiston välitys postilla ja/tai kuriirilla järjestetty turvallisesti?	Välitys on hoidettu riskienarvioinnin perusteella riittävän turvalliseksi katsotulla menettelyllä.
Pääkysymys: Pystytäänkö seuraamaan minne ja mistä salassa pidettävät aineistot on välitetty? Lisäkysymys: Kirjataanko turvaluokitellut aineistot?	Ei erityistä suositusta. Perustason vaatimukset: Ei auditointivaatimuksia. Korotetun tason vaatimukset: Suojaustason III tieto, riippumatta sen muodosta, rekisteröidään diaariin tai rekisteriin ennen välitystä ja vastaanotettaessa. Jos kyseessä on viestintä- ja tietojärjestelmä, kirjaamismenettelyt voidaan suorittaa sen omien prosessien avulla.

Käyttöturvallisuuden kriteerit (Elinkeinoelämän keskusliitto EK ym. 2009: 100–107).

Kysymys	**Lähtötason suositukset**
Pääkysymys: Onko huolehdittu, että organisaatiolla on toimintaansa nähden riittävät jatkuvuuden varmistavat suunnitelmat? Lisäkysymykset: Testataanko toipumisvalmiutta säännöllisesti? Suojataanko salassa pidettävät tiedot myös hätätilanteissa?	On varmistettu, että kriittisten verkkojen (ml. Internet-yhteys), verkkolaitteiden, tietojärjestelmien, palvelinten ja vastaavien vikaantumisesta pystytään toipumaan (liike)toimintavaatimuksiin nähden riittävässä ajassa. Käytännössä tämä vaatii usein 1) jatkuvuus- /toipumissuunnitelmaa, ja 2) suunnitelman säännöllistä testaamista. Vähintään tulee määritellä järjestelmien käytettävyysvaatimukset ja mitoittaa toipumismekanismit riskienarvioinnin mukaisesti niihin.
Pääkysymys: Mahdollistaako organisaatiossa saatavilla oleva dokumentaatio vioista, toimintahäiriöistä, hyökkäyksistä ja vastaavista toipumisen? Lisäkysymykset: Onnistuuko toipuminen jos järjestelmän tai verkon vastuuhenkilö ei ole käytettävissä? Miten nopeasti toipuminen onnistuu? Seurataanko säännöllisesti, että suojattavaa tietoa käsittelevän ympäristön dokumentaatio on ajan tasalla? Miten menetellään, mikäli tiedoissa on puutteita?	Verkot, järjestelmät ja niihin liittyvät asetukset on dokumentoitu siten, että viat ja toimintahäiriöt pystytään korjaamaan toimintavaatimusten mukaisesti.
Pääkysymys: Onko organisaatiossa selkeät periaatteet ja toimintatavat siitä, ketkä saavat asentaa ohjelmistoja, tietoliikenneyhteyksiä ja oheislaitteita? Lisäkysymykset: Käytetäänkö vain hyväksymisprosessin läpäisseitä verkkoja ja järjestelmiä?	1) Käytössä selkeät periaatteet ja toimintatavat siitä, ketkä saavat asentaa ohjelmistoja, tietoliikenneyhteyksiä ja oheislaitteita. 2) Periaatteiden noudattamista valvotaan ja varmistetaan teknisin keinoin (esimerkiksi rajoittamalla asennus- ja asetusten muokkausoikeus vain ylläpi-

Käytetäänkö salassa pidettävän tiedon käsittelyyn vain viranomaisen hyväksymiä tiloja, verkkoja ja järjestelmiä? Miten varmistutaan tietojärjestelmien eheydestä?	täjille). 3) Turva-asetusten ja -ohjelmien valtuuttamaton muokkaus on estetty peruskäyttäjiltä.
Onko organisaatiossa otettu käyttöön periaatteet ja turvamekanismit etä- ja matkatyön riskejä vastaan?	1) Organisaatiossa on käytössä periaatteet ja turvamekanismit etä- ja matkatyön riskejä vastaan. 2) Periaatteista ja vaadittavista mekanismeista on tiedotettu henkilöstölle.
Ovatko kehitys-/testaus- ja tuotantojärjestelmät erilliset?	1) Kehitys-/testaus- ja tuotantojärjestelmien on oltava erilliset. Tuotantojärjestelmän oltava erillinen, jotta kehitys- tai testaustoimet eivät aiheuta tuotantokatkoksia. 2) Ennen uuden järjestelmän käyttöönottoa testidatat, oletus- ja testikäyttäjätilit ja vastaavat poistetaan.
Pääkysymys: Miten varmistetaan, että verkossa ja sen palveluissa ei ole tunnettuja haavoittuvuuksia? Lisäkysymykset: Onko tietoturvatiedotteiden seuranta vastuutettu? Onko turvapäivitysten asentamiseen luotu menettelytavat? Valvotaanko niiden toteutumista?	Viranomaisten (esim. CERT), laite- ja ohjelmistovalmistajien sekä muiden vastaavien tahojen tietoturvatiedotteita seurataan ja tarpeelliset turvapäivitykset asennetaan hallitusti.
Miten varmistutaan siitä, että työskentelytauoilla tai työskentelyn jälkeen laitteet eivät jää ilman riittävää suojaa?	Käyttäjät velvoitetaan seuraavaan käytäntöön: 1) Työasema, pääte, kannettava tietokone tai vastaava lukitaan aina (esim. salasanasuojatulla näytönsäästäjällä tai muulla menettelyllä), kun laitteelta poistutaan. 2) Aktiiviset istunnot päätetään työn päättyessä ja tauoilla (esim. etäyhteydet ja palvelinistunnot puretaan). 3) Laitteesta/järjestelmästä kirjaudutaan ulos työn päättyessä.

Onko käytössä ns. puhtaan pöydän politiikka? Koskeeko sama periaate myös näyttöjä?	1) Papereita ja siirrettäviä tallennusvälineitä koskeva puhtaan pöydän politiikka sekä tietojenkäsittelypalveluja koskeva puhtaan näytön politiikka on käytössä. 2) Huolehditaan siitä, ettei neuvottelutiloihin jää asiakirjoja tai muita muistiinpanoja kokousten jälkeen.
Pääkysymys: Onko huolehdittu riittävästä työtehtävien eriyttämisestä niin, ettei synny ns. vaarallisia työyhdistelmiä? Lisäkysymys: Onko huolehdittu siitä, että kriittiset ylläpitotoimet vaativat kahden tai useamman henkilön hyväksynnän?	Tehtävät ja vastuualueet on mahdollisuuksien mukaan eriytetty, jotta vähennetään organisaation suojattavien kohteiden luvattoman tai tahattoman muuntelun tai väärinkäytön riskiä.
Onko riittävästä varmuuskopioinnista huolehdittu?	Riittävästä varmuuskopioinnista on huolehdittu. Huolehdittava, että: 1) Varmistusten taajuus on suhteessa varmistettavan tiedon kriittisyyteen. 2) Varmuuskopioinnin oikea toiminta ja palautusprosessi testataan säännöllisesti. 3) Varmuuskopiot säilytetään eri fyysisessä sijainnissa kuin varsinainen järjestelmä. 4) Varmuuskopioihin pääsy on estetty muilta kuin valtuutetuilta käyttäjiltä.

Liite 2. Kriteerien muodostaminen.

Tässä 3-sivuisessa liitteessä kuvataan kriteerien muodostaminen esitetyn kirjallisuuden ja ohjeiden perusteella.

	Kirjallisuus	Tieteelliset tutkimukset	Yrityksen tietoturvaopas (Viestintävirasto, CERT-FI ja NCSA-FI)	Kansallinen turvallisuusauditointikriteeristö (KATAKRI)	Käytännön tietoturvallisuus-opas pk-yrityksille (Yritysturvallisuus EK Oy)	Tietoturvaopas (TIEKE Tietoyhteiskunnan kehittämiskeskus ry)
2. Minä pyrin työtehtävissäni ymmärtämään, että						
tietoturvalle on olemassa pelisäännöt.	x	x	x	x	x	x
tietoturvaan liittyy yleisiä oikeuksia ja velvollisuuksia.	x		x	x	x	x
työtietokoneellani on tietyt käyttötarkoitukset ja -oikeudet.	x		x	x	x	x
minulla on vastuu käyttäjätunnuksillani tehdyistä asioista.	x		x	x	x	x
salasanalle on vaatimuksia.	x		x	x	x	x
työtietokoneen ohjelmiin liittyy vaatimuksia.	x		x	x	x	x
yrityksemme palomuuriin ja virustorjuntaohjelmistoon liittyy vaatimuksia.	x	x	x	x	x	x
työsähköpostiin ja roskapostiin liittyy vaatimuksia.	x	x	x	x	x	x
tietoturvatarkastuksia on tehtävä säännöllisesti.	x		x	x	x	x
tiedostojen tallentamiseen liittyy vaatimuksia.	x		x	x	x	x
tiedon ja tiedoston alkuperän selvittäminen on tärkeää.	x		x	x	x	x
joku voi salakuunnella minua.	x		x	x	x	x
3. Minä pyrin työtehtävissäni tukemaan yrityksemme yleistä toiminnallista tavoitetta, että						
tietoturva varmistaa yrityksen liiketoiminnan ja palveluiden jatkuvuuden.	x	x	x	x	x	x
tietoturvaa kehitetään tietoturvatoiminnan prosessikuvauksia hyödyntäen.	x	x	x	x	x	
tietoturva säästää aikaa ja rahaa.		x	x	x	x	x
tietoturva on teknistä (20 %) ja hallinnollista (80 %) työtä.	x	x	x		x	x
tietoturvatavoitteita ja -vaikutuksia mitataan.	x	x	x	x	x	x
tietoturvariskejä ennakoidaan ja niihin varaudutaan.	x	x	x	x	x	x
tietokoneiden ja verkkojen suojaukset ovat ajan tasalla.	x	x	x	x	x	x
tietoturvaa tuetaan yrityksen arvoilla.	x	x		x	x	
tietoturvaa varten luodaan tietoturvapolitiikka ja -ohjeet.	x	x	x	x	x	x
4. Minä pyrin työtehtävissäni tukemaan yrityksemme toiminnallista tavoitetta, että						
tietoturva on kiinteä ja keskeinen osa koko yrityksen toimintaa.	x	x	x	x	x	x
tietoturva on yrityksen liiketoiminnan osa.	x	x	x	x	x	x
tietoturva on suunniteltua ja seurattua toimintaa.	x	x	x	x	x	x
tietoturva sisältyy perehdytykseen.	x	x	x	x	x	x
tietoturvassa huomioidaan työntekijän maalaisjärki ja päätöksentekotaidot.	x	x			x	x
yrityksen johto määrittelee tietoturvaperiaatteet.	x	x	x	x	x	x
yrityksen johto tekee tietoturvapäätökset.	x	x	x	x	x	
työntekijä ja inhimillinen toiminta ymmärretään tietoturvan suurimpana uhkana.	x	x	x		x	x

	Kirjallisuus	Tieteelliset tutkimukset	Yrityksen tietoturvaopas (Viestintävirasto, CERT-FI ja NCSA-FI)	Kansallinen turvallisuusauditointikriteeristö (KATAKRI)	Käytännön tietoturvallisuus-opas pk-yrityksille (Yritysturvallisuus EK Oy)	Tietoturvaopas (TIEKE Tietoyhteiskunnan kehittämiskeskus ry)
5. Minä pyrin työtehtävissäni tukemaan yrityksemme tietoihin liittyvää tavoitetta, että						
tiedolle laaditaan elinkaari.	x		x	x	x	x
asiakastiedot varmistetaan.	x	x	x	x	x	x
taloudellisesti ja toiminnallisesti merkittävä tieto selvitetään tiedon luokittelulla.	x	x	x	x	x	x
suojattava tieto kartoitetaan riskianalyysillä.	x	x	x	x	x	x
keskeinen tieto suojataan.	x	x	x	x	x	x
tärkeä tieto salakirjoitetaan, jos siihen käsiksi pääseminen on mahdollista.	x		x	x	x	x
varmuuskopioinnille laaditaan suunnitelma.	x		x	x	x	x
6. Minä pyrin työtehtävissäni huomioimaan, että yrityksessämme						
minä saan koulutusta yrityksen tietoturvakäytäntöihin.	x	x	x	x	x	x
minä saan tietoturvan sisältävää ohjausta ja ohjeita työhöni.	x	x	x	x	x	x
minun tietoturvaosaamistani kehitetään jatkuvasti.	x	x	x	x	x	x
minä huomioin tietoturvan osana päivittäistä toimintaani.	x	x	x	x	x	x
minä tunnen yrityksen tietoturvatoimenpiteet.	x	x	x	x	x	x
tietoturvaa seurataan hallinnollisesti.	x	x	x	x	x	
minä tiedän toimintatavat eri tietoturvatilanteissa.	x	x	x	x	x	x
minä osaan toimia rauhallisesti tietoturvapoikkeustilanteessa.	x	x	x	x	x	x
vanhemmat kollegat toimivat hyvänä esimerkkinä tietoturvakäyttäytymisessä.	x	x	x	x	x	
7. Minä pyrin työtehtävissäni huomioimaan, että toiminnassani						
minä noudatan yrityksen tietoturvakäytäntöjä.	x	x	x	x	x	x
minä tiedän lähimmän tietoturvahenkilön.	x		x	x	x	x
minä tiedän, mikä tieto on suojattavaa, missä se säilytetään ja kuka säilytystilaan pääsee.	x	x	x	x	x	x
minä tunnen yrityksen yleisen varmuuskopiointikäytännön.	x		x	x	x	x
minä noudatan puhtaan pöydän periaatetta.	x			x	x	
minä lukitsen lukituiksi ohjeistetut ovet.	x		x	x	x	x
minä lukitsen tietokoneen, kun en ole käyttämässä sitä.	x		x	x	x	x
8. Minä pyrin työtehtävissäni huomioimaan, että yrityksemme hallinnossa						
varmistetaan yrityksen johdon tietoisuus tietoturvauhkista.	x	x		x	x	x
osoitetaan selkeästi yrityksen johdon tuki tietoturvalle.	x	x	x	x	x	
huomioidaan yrityksen toimintaan vaikuttavat lakisääteiset vaatimukset.	x		x	x	x	
huomioidaan henkilöstöturvallisuus.	x		x	x	x	x
huomioidaan toimitilaturvallisuus.	x		x	x	x	x
huomioidaan tietoturvajohtamisen laajuus.	x			x	x	
huomioidaan tietoturvajohtamisen hyvä tietohallintotapa (IT Governance).	x			x	x	

	Kirjallisuus	Tieteelliset tutkimukset	Yrityksen tietoturvaopas (Viestintävirasto, CERT-FI ja NCSA-FI)	Kansallinen turvallisuusauditointikriteeristö (KATAKRI)	Käytännön tietoturvallisuus-opas pk-yrityksille (Yritysturvallisuus EK Oy)	Tietoturvaopas (TIEKE Tietoyhteiskunnan kehittämiskeskus ry)
9. Minä pyrin työtehtävissäni huomioimaan, että yrityksemme hallinnossa määritellään						
selkeästi tahot, jotka johtavat tietoturvaa.	x		x	x	x	x
selkeästi tahot, jotka vastaavat tietoturvasta.	x		x	x	x	x
menettelyt, joilla tietoturvaa hallitaan.	x	x		x	x	x
tietoturvan resursointi.	x	x	x	x	x	x
tietoturvan yhteys yrityksen liiketoimintastrategiaan.	x	x	x	x	x	x
yrityksen toiminnan kehittämisen jatkotoimenpiteet.	x	x	x	x	x	
käytännön tietoturvatoimenpiteet.	x	x	x	x	x	x
10. Minä pyrin työtehtävissäni huomioimaan, että yrityksellämme						
on selkeä tavoite yrityksen liiketoiminnalle.	x	x	x	x	x	
on selkeät tavoitteet, jotka tukevat yrityksen toiminnan tuloksen syntymistä.	x	x	x	x	x	x
on tietoturvaohjelma tietoturvajohtamisen ja turvallisuustyön tavoitteiden saavuttamiseksi.	x	x	x	x	x	x
on tietoturvapolitiikka, -ohjeistukset ja -dokumentaatio.	x	x	x	x	x	x
on menettely kriittisten tapahtumien johtamiselle.	x	x	x	x	x	x
on toipumissuunnitelmat.	x	x		x	x	x
on menettelyt sidosryhmien tietoturvan hallintaan.	x	x	x	x	x	x
11. Minä pyrin työtehtävissäni huomioimaan, että yrityksessämme						
tietoturvan tavoitteita ja toteutumista seurataan ja arvioidaan.	x	x	x	x	x	x
työntekijälle kerrotaan tietoturvariskeistä.	x	x	x	x	x	x
varaudutaan tietoturvapoikkeamatilanteisiin.	x	x	x	x	x	x
tunnistetaan toiminnalle tärkeät ja siten suojattavat kohteet.	x	x	x	x	x	x
arvioidaan toiminnalle tärkeiden ja siten suojattavien kohteiden riskit.	x	x	x	x	x	x
suojataan tietoverkot ja tietojärjestelmät.	x	x	x	x	x	x
merkittäviä tietojenkäsittely-ympäristöjä muutetaan hallitusti.	x	x		x	x	
pidetään yhteyttä asiakkaisiin ja sidosryhmiin tietoturvaa varten.	x	x	x	x	x	x

Liite 3. Sähköposti kyselystä.

Niina Kinnunen Vaasan yliopistosta tekee väitöskirjatutkimusta aiheesta ”Viranomaisten tietoturvaohjeistusten motivoivuus”.

Kaha osallistuu Vaasan yliopistolle tehtävään väitöskirjatutkimukseen ”Viranomaisten tietoturvaohjeistusten motivoivuus”.

Tutkimus tehdään web-kyselynä, johon pääset vastaamaan alla olevasta linkistä:

http://www.webropolsurveys.com/S/2EB8F6FA6A276401.par

Vastaaminen vie n. 5-10 minuuttia. Vastata voit heti, mutta kuitenkin viimeistään ensi viikon pe 15.2.

Kaikkien vastanneiden ja kyselyn lopussa yhteystietonsa jättäneiden kesken arvotaan illalliskortteja.

Kaha saa tutkimuksen tulokset hyödynnettäväksi omaan toimintaansa sisäisesti sekä sidosryhmien kanssa.

Toivottavasti mahdollisimman moni vastaa kyselyyn, niin saamme kattavan tutkimuksen tulokset käyttöömme!

Lisätietoja tutkimuksesta antaa Sanna Kainulainen ja tutkija Niina Kinnunen.

t. Sanna

Liite 4. Sähköinen kyselylomake.

Väitöskirjatutkimus Kahan työntekijöille: Viranomaisten tietoturvaohjeistusten motivoivuus

Oheisella kyselyllä tutkitaan viranomaistahojen tietoturvaohjeistusten motivoivuutta. Arvioi omaa tavoitettasi pyrkiä toimimaan tietoturvakriteerien mukaisesti: arvioi pyrkimyksesi tasoa, ei käytännön toteuttamisen tasoa. Kaikki kysymykset ovat pakollisia.

1. Asema yrityksessä	**Valitse**
Johtoryhmä / esimies	
Työntekijä	

2. Minä pyrin työtehtävissäni ymmärtämään, että	**En ollenkaan**	**Melko harvoin**	**Melko usein**	**Lähes aina**	**En osaa sanoa**
tietoturvalle on olemassa pelisäännöt.					
tietoturvaan liittyy yleisiä oikeuksia ja velvollisuuksia.					
työtietokoneellani on tietyt käyttötarkoitukset ja -oikeudet.					
minulla on vastuu käyttäjätunnuksillani tehdyistä asioista.					
salasanalle on vaatimuksia.					
työtietokoneen ohjelmiin liittyy vaatimuksia.					
yrityksemme palomuuriin ja virustorjuntaohjelmistoon liittyy vaatimuksia.					
työsähköpostiin ja roskapostiin liittyy vaatimuksia.					
tietoturvatarkastuksia on tehtävä säännöllisesti.					
tiedostojen tallentamiseen liittyy vaatimuksia.					
tiedon ja tiedoston alkuperän selvittäminen on tärkeää.					
joku voi salakuunnella minua.					

3. Minä pyrin työtehtävissäni tukemaan yrityksemme yleistä toiminnallista tavoitetta, että	**En ollenkaan**	**Melko harvoin**	**Melko usein**	**Lähes aina**	**En osaa sanoa**
tietoturva varmistaa yrityksen liiketoiminnan ja palveluiden jatkuvuuden.					
tietoturvaa kehitetään tietoturvatoiminnan prosessikuvauksia hyödyntäen.					
tietoturva säästää aikaa ja rahaa.					
tietoturva on teknistä (20 %) ja hallinnollista (80 %) työtä.					
tietoturvatavoitteita ja -vaikutuksia mitataan.					
tietoturvariskejä ennakoidaan ja niihin varaudutaan.					
tietokoneiden ja verkkojen suojaukset ovat ajan tasalla.					
tietoturvaa tuetaan yrityksen arvoilla.					
tietoturvaa varten luodaan tietoturvapolitiikka ja -ohjeet.					

4. Minä pyrin työtehtävissäni tukemaan yrityksemme toiminnallista tavoitetta, että	**En ollenkaan**	**Melko harvoin**	**Melko usein**	**Lähes aina**	**En osaa sanoa**
tietoturva on kiinteä ja keskeinen osa koko yrityksen toimintaa.					
tietoturva on yrityksen liiketoiminnan osa.					
tietoturva on suunniteltua ja seurattua toimintaa.					
tietoturva sisältyy perehdytykseen.					
tietoturvassa huomioidaan työntekijän maalaisjärki ja päätöksentekotaidot.					
yrityksen johto määrittelee tietoturvaperiaatteet.					
yrityksen johto tekee tietoturvapäätökset.					
työntekijä ja inhimillinen toiminta ymmärretään tietoturvan suurimpana uhkana.					

5. Minä pyrin työtehtävissäni tukemaan yrityksemme tietoihin liittyvää tavoitetta, että	**En ollenkaan**	**Melko harvoin**	**Melko usein**	**Lähes aina**	**En osaa sanoa**
tiedolle laaditaan elinkaari.					
asiakastiedot varmistetaan.					
taloudellisesti ja toiminnallisesti merkittävä tieto selvitetään tiedon luokittelulla.					
suojattava tieto kartoitetaan riskianalyysillä.					
keskeinen tieto suojataan.					
tärkeä tieto salakirjoitetaan, jos siihen käsiksi pääseminen on mahdollista.					
varmuuskopioinnille laaditaan suunnitelma.					

6. Minä pyrin työtehtävissäni huomioimaan, että yrityksessämme	**En ollenkaan**	**Melko harvoin**	**Melko usein**	**Lähes aina**	**En osaa sanoa**
minä saan koulutusta yrityksen tietoturvakäytäntöihin.					
minä saan tietoturvan sisältävää ohjausta ja ohjeita työhöni.					
minun tietoturvaosaamistani kehitetään jatkuvasti.					
minä huomioin tietoturvan osana päivittäistä toimintaani.					
minä tunnen yrityksen tietoturvatoimenpiteet.					
tietoturvaa seurataan hallinnollisesti.					
minä tiedän toimintatavat eri tietoturvatilanteissa.					
minä osaan toimia rauhallisesti tietoturvapoikkeustilanteessa.					
vanhemmat kollegat toimivat hyvänä esimerkkinä tietoturvakäyttäytymisessä.					

7. Minä pyrin työtehtävissäni huomioimaan, että toiminnassani	**En ollenkaan**	**Melko harvoin**	**Melko usein**	**Lähes aina**	**En osaa sanoa**
minä noudatan yrityksen tietoturvakäytäntöjä.					
minä tiedän lähimmän tietoturvahenkilön.					
minä tiedän, mikä tieto on suojattavaa, missä se säilytetään ja kuka säilytystilaan pääsee.					
minä tunnen yrityksen yleisen varmuuskopiointikäytännön.					
minä noudatan puhtaan pöydän periaatetta.					
minä lukitsen lukituiksi ohjeistetut ovet.					
minä lukitsen tietokoneen, kun en ole käyttämässä sitä.					

8. Minä pyrin työtehtävissäni huomioimaan, että yrityksemme hallinnossa	**En ollenkaan**	**Melko harvoin**	**Melko usein**	**Lähes aina**	**En osaa sanoa**
varmistetaan yrityksen johdon tietoisuus tietoturvauhkista.					
osoitetaan selkeästi yrityksen johdon tuki tietoturvalle.					
huomioidaan yrityksen toimintaan vaikuttavat lakisääteiset vaatimukset.					
huomioidaan henkilöstöturvallisuus.					
huomioidaan toimitilaturvallisuus.					
huomioidaan tietoturvajohtamisen laajuus.					
huomioidaan tietoturvajohtamisen hyvä tietohallintotapa (IT Governance).					

9. Minä pyrin työtehtävissäni huomioimaan, että yrityksemme hallinnossa määritellään	**En ollenkaan**	**Melko harvoin**	**Melko usein**	**Lähes aina**	**En osaa sanoa**
selkeästi tahot, jotka johtavat tietoturvaa.					
selkeästi tahot, jotka vastaavat tietoturvasta.					
menettelyt, joilla tietoturvaa hallitaan.					
tietoturvan resursointi.					
tietoturvan yhteys yrityksen liiketoimintastrategiaan.					
yrityksen toiminnan kehittämisen jatkotoimenpiteet.					
käytännön tietoturvatoimenpiteet.					

10. Minä pyrin työtehtävissäni huomioimaan, että yrityksellämme	**En ollenkaan**	**Melko harvoin**	**Melko usein**	**Lähes aina**	**En osaa sanoa**
on selkeä tavoite yrityksen liiketoiminnalle.					
on selkeät tavoitteet, jotka tukevat yrityksen toiminnan tuloksen syntymistä.					
on tietoturvaohjelma tietoturvajohtamisen ja turvallisuustyön tavoitteiden saavuttamiseksi.					
on tietoturvapolitiikka, -ohjeistukset ja -dokumentaatio.					
on menettely kriittisten tapahtumien johtamiselle.					
on toipumissuunnitelmat.					
on menettelyt sidosryhmien tietoturvan hallintaan.					

11. Minä pyrin työtehtävissäni huomioimaan, että yrityksessämme	**En ollenkaan**	**Melko harvoin**	**Melko usein**	**Lähes aina**	**En osaa sanoa**
tietoturvan tavoitteita ja toteutumista seurataan ja arvioidaan.					
työntekijälle kerrotaan tietoturvariskeistä.					
varaudutaan tietoturvapoikkeamatilanteisiin.					
tunnistetaan toiminnalle tärkeät ja siten suojattavat kohteet.					
arvioidaan toiminnalle tärkeiden ja siten suojattavien kohteiden riskit.					
suojataan tietoverkot ja tietojärjestelmät.					
merkittäviä tietojenkäsittely-ympäristöjä muutetaan hallitusti.					
pidetään yhteyttä asiakkaisiin ja sidosryhmiin tietoturvaa varten.					

Liite 5. Kyselyn tulokset**.**

Väitöskirjatutkimus Kahan työntekijöille: Viranomaisten tietoturvaohjeistusten motivoivuus – Tulokset

Tässä 4-sivuisessa liitteessä on esitetty kaikki kyselytutkimuksen tulokset sekä tulokset eroteltuna erikseen aseman mukaan esimiesten ja työntekijöiden tulokset.

	2. Minä pyrin työtehtävissäni ymmärtämään, että												3. Minä pyrin työtehtävissäni tukemaan yrityksemme yleistä toiminnallista tavoitetta, että								
	tietoturvalle on olemassa pelisäännöt.	tietoturvaan liittyy yleisiä oikeuksia ja velvollisuuksia.	työtietokoneellani on tietyt käyttötarkoitukset ja -oikeudet.	minulla on vastuu käyttäjätunnuksillani tehdyistä asioista.	salasanalle on vaatimuksia.	työtietokoneen ohjelmiin liittyy vaatimuksia.	yrityksemme palomuuriin ja virustorjuntaohjelmistoon liittyy vaatimuksia.	työsähköpostiin ja roskapostiin liittyy vaatimuksia.	tietoturvatarkastuksia on tehtävä säännöllisesti.	tiedostojen tallentamiseen liittyy vaatimuksia.	tiedon ja tiedoston alkuperän selvittäminen on tärkeää.	joku voi salakuunnella minua.	tietoturva varmistaa yrityksen liiketoiminnan ja palveluiden jatkuvuuden.	tietoturvaa kehitetään tietoturvatoiminnan prosessikuvauksia hyödyntäen.	tietoturva säästää aikaa ja rahaa.	tietoturva on teknistä (20 %) ja hallinnollista (80 %) työtä.	tietoturvatavoitteita ja -vaikutuksia mitataan.	tietoturvariskejä ennakoidaan ja niihin varaudutaan.	tietokoneiden ja verkkojen suojaukset ovat ajan tasalla.	tietoturvaa tuetaan yrityksen arvoilla.	tietoturvaa varten luodaan tietoturvapolitiikka ja -ohjeet.
Kaikki (n=58)																					
1	0	0	0	0	0	0	0	0	0	0	1	6	0	1	1	1	1	0	0	1	0
2	1	2	1	0	1	1	1	1	3	7	7	20	1	5	8	7	13	3	1	4	6
3	6	6	7	4	10	9	6	14	17	12	17	6	12	15	19	12	13	14	12	14	13
4	51	50	50	54	47	46	47	42	35	37	31	15	42	24	29	23	21	37	38	30	31
5	0	0	0	0	0	2	4	1	3	2	2	11	3	13	1	15	10	4	7	9	8
Johtoryhmä/esimies (n=13)																					
1	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0
2	1	1	0	0	1	1	0	0	1	1	2	4	0	0	1	1	4	0	0	1	1
3	0	1	2	0	2	2	2	4	3	2	3	0	4	6	5	2	3	3	4	4	5
4	12	11	11	13	10	10	10	9	9	9	6	4	9	5	7	5	3	10	9	7	7
5	0	0	0	0	0	0	1	0	0	1	1	4	0	2	0	5	3	0	0	1	0
Työntekijä (n=45)																					
1	0	0	0	0	0	0	0	0	0	0	0	5	0	1	1	1	1	0	0	1	0
2	0	1	1	0	0	0	1	1	2	6	5	16	1	5	7	6	9	3	1	3	5
3	6	5	5	4	8	7	4	10	14	10	14	6	8	9	14	10	10	11	8	10	8
4	39	39	39	41	37	36	37	33	26	28	25	11	33	19	22	18	18	27	29	23	24
5	0	0	0	0	0	2	3	1	3	1	1	7	3	11	1	10	7	4	7	8	8

1 = En ollenkaan
2 = Melko harvoin
3 = Melko usein
4 = Lähes aina
5 = En osaa sanoa

	4. Minä pyrin työtehtävissäni tukemaan yrityksemme toiminnallista tavoitetta, että								5. Minä pyrin työtehtävissäni tukemaan yrityksemme tietoihin liittyvää tavoitetta, että							6. Minä pyrin työtehtävissäni huomioimaan, että yrityksessämme								
	tietoturva on kiinteä ja keskeinen osa koko yrityksen toimintaa.	tietoturva on yrityksen liiketoiminnan osa.	tietoturva on suunniteltua ja seurattua toimintaa.	tietoturva sisältyy perehdytykseen.	tietoturvassa huomioidaan työntekijän maalaisjärki ja päätöksentekotaidot.	yrityksen johto määrittelee tietoturvaperiaatteet.	yrityksen johto tekee tietoturvapäätökset.	työntekijä ja inhimillinen toiminta ymmärretään tietoturvan suurimpana uhkana.	tiedolle laaditaan elinkaari.	asiakastiedot varmistetaan.	taloudellisesti ja toiminnallisesti merkittävä tieto selvitetään tiedon luokittelulla.	suojattava tieto kartoitetaan riskianalyysillä.	keskeinen tieto suojataan.	tärkeä tieto salakirjoitetaan, jos siihen käsiksi pääseminen on mahdollista.	varmuuskopioinnille laaditaan suunnitelma.	minä saan koulutusta yrityksen tietoturvakäytäntöihin.	minä saan tietoturvan sisältävää ohjausta ja ohjeita työhöni.	minun tietoturvaosaamistani kehitetään jatkuvasti.	minä huomioin tietoturvan osana päivittäistä toimintaani.	minä tunnen yrityksen tietoturvatoimenpiteet.	tietoturvaa seurataan hallinnollisesti.	minä tiedän toimintatavat eri tietoturvatilanteissa.	minä osaan toimia rauhallisesti tietoturvapoikkeustilanteessa.	vanhemmat kollegat toimivat hyvänä esimerkkinä tietoturvakäyttäytymisessä.
Kaikki (n=58)																									
1	1	2	0	5	4	2	0	0	4	1	1	5	1	11	3	10	4	5	0	7	0	5	1	6	
2	4	6	9	13	3	4	8	6	15	5	6	7	1	10	8	17	20	23	6	13	12	12	5	21	
3	13	12	8	16	20	17	12	18	17	11	17	15	13	10	8	15	19	17	19	19	11	21	14	14	
4	39	36	38	17	25	28	33	24	12	37	24	20	38	12	27	13	12	8	31	15	20	12	27	9	
5	1	2	3	7	6	7	5	10	10	4	10	11	5	15	12	3	3	5	2	4	15	8	11	8	
Johtoryhmä/esimies (n=13)																									
1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	1	0	1	1	1	
2	1	1	1	3	0	0	2	1	2	0	0	4	1	5	1	4	3	4	2	3	5	4	2	5	
3	5	3	2	8	6	4	3	5	5	2	8	3	4	3	3	4	7	7	5	6	4	5	2	7	
4	7	8	10	2	7	8	8	6	3	11	4	4	8	2	7	3	2	1	6	3	4	2	7	0	
5	0	1	0	0	0	1	0	1	2	0	1	2	0	3	2	1	1	1	0	0	0	1	1	0	
Työntekijä (n=45)																									
1	1	2	0	5	4	2	0	0	3	1	1	5	1	11	3	9	4	5	0	6	0	4	0	5	
2	3	5	8	10	3	4	6	5	13	5	6	3	0	5	7	13	17	19	4	10	7	8	3	16	
3	8	9	6	8	14	13	9	13	12	9	9	12	9	7	5	11	12	10	14	13	7	16	12	7	
4	32	28	28	15	18	20	25	18	9	26	20	16	30	10	20	10	10	7	25	12	16	10	20	9	
5	1	1	3	7	6	6	5	9	8	4	9	9	5	12	10	2	2	4	2	4	15	7	10	8	

1 = En ollenkaan
2 = Melko harvoin
3 = Melko usein
4 = Lähes aina
5 = En osaa sanoa

	7. Minä pyrin työtehtävissäni huomioimaan, että toiminnassani							8. Minä pyrin työtehtävissäni huomioimaan, että yrityksemme hallinnossa							9. Minä pyrin työtehtävissäni huomioimaan, että yrityksemme hallinnossa määritellään						
	minä noudatan yrityksen tietoturvakäytäntöjä.	minä tiedän lähimmän tietoturvahenkilön.	minä tiedän, mikä tieto on suojattavaa, missä se säilytetään ja kuka säilytystilaan pääsee.	minä tunnen yrityksen yleisen varmuuskopiointikäytännön.	minä noudatan puhtaan pöydän periaatetta.	minä lukitsen lukituiksi ohjeistetut ovet.	minä lukitsen tietokoneen, kun en ole käyttämässä sitä.	varmistetaan yrityksen johdon tietoisuus tietoturvauhkista.	osoitetaan selkeästi yrityksen johdon tuki tietoturvalle.	huomioidaan yrityksen toimintaan vaikuttavat lakisääteiset vaatimukset.	huomioidaan henkilöstöturvallisuus.	huomioidaan toimitilaturvallisuus.	huomioidaan tietoturvajohtamisen laajuus.	huomioidaan tietoturvajohtamisen hyvä tietohallintotapa (IT Governance).	selkeästi tahot, jotka johtavat tietoturvaa.	selkeästi tahot, jotka vastaavat tietoturvasta.	menettelyt, joilla tietoturvaa hallitaan.	tietoturvan resursointi.	tietoturvan yhteys yrityksen liiketoimintastrategiaan.	yrityksen toiminnan kehittämisen jatkotoimenpiteet.	käytännön tietoturvatoimenpiteet.
Kaikki (n=58)																					
1	0	3	5	12	3	1	0	2	2	2	2	2	2	2	3	3	3	3	3	3	3
2	1	3	10	11	10	2	3	8	6	5	0	0	5	4	2	2	3	8	6	4	3
3	8	13	18	17	21	8	15	14	15	17	20	20	14	17	18	14	15	14	12	14	14
4	48	36	15	12	14	42	40	20	19	22	27	26	20	16	27	31	26	19	23	23	28
5	1	3	10	6	10	5	0	14	16	12	9	10	17	19	8	8	11	14	14	14	10
Johtoryhmä/esimies (n=13)																					
1	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	1	4	3	3	1	2	3	2	2	0	0	2	1	1	1	1	1	2	1	1
3	2	4	4	7	6	2	4	3	4	4	4	5	3	5	4	4	3	4	3	4	6
4	11	8	4	2	1	9	7	6	6	7	8	6	6	6	8	8	8	6	7	7	6
5	0	0	0	0	2	0	0	1	1	0	1	2	2	1	0	0	1	2	1	1	0
Työntekijä (n=45)																					
1	0	3	4	11	2	0	0	2	2	2	2	2	2	2	3	3	3	3	3	3	3
2	1	2	6	8	7	1	1	5	4	3	0	0	3	3	1	1	2	7	4	3	2
3	6	9	14	10	15	6	11	11	11	13	16	15	11	12	14	10	12	10	9	10	8
4	37	28	11	10	13	33	33	14	13	15	19	20	14	10	19	23	18	13	16	16	22
5	1	3	10	6	8	5	0	13	15	12	8	8	15	18	8	8	10	12	13	13	10

1 = En ollenkaan
2 = Melko harvoin
3 = Melko usein
4 = Lähes aina
5 = En osaa sanoa

	10. Minä pyrin työtehtävissäni huomioimaan, että yrityksellämme							11. Minä pyrin työtehtävissäni huomioimaan, että yrityksessämme							
	on selkeä tavoite yrityksen liiketoiminnalle.	on selkeät tavoitteet, jotka tukevat yrityksen toiminnan tuloksen syntymistä.	on tietoturvaohjelma tietoturvajohtamisen ja turvallisuustyön tavoitteiden saavuttamiseksi.	on tietoturvapolitiikka, -ohjeistukset ja -dokumentaatio.	on menettely kriittisten tapahtumien johtamiselle.	on toipumissuunnitelmat.	on menettelyt sidosryhmien tietoturvan hallintaan.	tietoturvan tavoitteita ja toteutumista seurataan ja arvioidaan.	työntekijälle kerrotaan tietoturvariskeistä.	varaudutaan tietoturvapoikkeamatilanteisiin.	tunnistetaan toiminnalle tärkeät ja siten suojattavat kohteet.	arvioidaan toiminnalle tärkeiden ja siten suojattavien kohteiden riskit.	suojataan tietoverkot ja tietojärjestelmät.	merkittäviä tietojenkäsittely-ympäristöjä muutetaan hallitusti.	pidetään yhteyttä asiakkaisiin ja sidosryhmiin tietoturvaa varten.
Kaikki (n=58)															
1	2	2	2	2	3	3	3	0	4	1	0	0	0	0	0
2	0	0	2	8	5	8	7	7	10	8	4	8	5	8	10
3	8	8	14	15	18	16	16	13	18	13	14	12	9	10	14
4	44	44	27	23	19	11	16	19	17	21	29	24	36	26	17
5	4	4	13	10	13	20	16	19	9	15	11	14	8	14	17
Johtoryhmä/esimies (n=13)															
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	1	3	1	3	2	2	2	3	1	1	2	1	2
3	1	2	4	4	4	3	5	5	6	2	2	2	2	4	5
4	12	11	6	5	6	4	3	4	5	7	9	8	9	7	3
5	0	0	2	1	2	3	3	2	0	1	1	2	0	1	3
Työntekijä (n=45)															
1	2	2	2	2	3	3	3	0	4	1	0	0	0	0	0
2	0	0	1	5	4	5	5	5	8	5	3	7	3	7	8
3	7	6	10	11	14	13	11	8	12	11	12	10	7	6	9
4	32	33	21	18	13	7	13	15	12	14	20	16	27	19	14
5	4	4	11	9	11	17	13	17	9	14	10	12	8	13	14

1 = En ollenkaan
2 = Melko harvoin
3 = Melko usein
4 = Lähes aina
5 = En osaa sanoa

Liite 6. Ensimmäisen haastattelututkimuksen runko.

Väitöskirjatutkimus Kahan työntekijöille - Haastattelututkimus

Esipuhe

Tämä haastattelututkimus liittyy Vaasan yliopistolle toteutettavaan hallinnollista tietoturvaa käsittelevään väitöskirjatutkimukseen **hallinnollisten tietoturvakriteerien motivoivuudesta**. Tämän haastattelututkimuksen perustana on helmikuussa 2013 Kahalla tehdyn kyselytutkimuksen tulosten **22 heikoimmin noudattamaan pyrittyä tietoturvakriteeriä**.

Haastattelun tavoitteena on keskustella 1) millaisia ajatuksia kriteerit herättävät sekä 2) mitkä syyt motivoisivat pyrkimyksessä noudattaa kriteerejä. Motivointisyitä tarkastellaan Decin ja Ryanin menetelmällä, jonka mukaan motivoituneisuuden tekijät voidaan jakaa neljään luokkaan: 1) toisen henkilön tai tilanteen vaatimus, 2) toteuttamisen tuottama mielihyvä tai oma kiinnostus, 3) toteuttamatta jättämisestä aiheutuva häpeä, syyllisyys tai ahdistus sekä 4) oma usko toteuttamisen tärkeydestä.

Haastattelun arvioitu kesto on 30 minuuttia.

- - -

Haastattelun aloittaminen

Haastateltavan taustatiedot

1. **Asema yrityksessä**

a) Johtoryhmä/esimies
b) Työntekijä

Lisäksi haluan sinun vastaavan seuraavien 22 kriteerin osalta: 1) Millaisia ajatuksia kriteeri herättää sinussa? sekä 2) Mikä tai mitkä syyt motivoisivat sinua pyrkimyksessä noudattaa kriteeriä?.

Yleiset							
		2) Syy kriteerin toteuttamiselle					
		Decin ja Ryanin menetelmän luokittelemat syyt					
Minä pyrin työtehtävissäni ymmärtämään/tukemaan, että	**1) Mitä ajatuksia kriteeri herättää sinussa?**	**Toisen henkilön tai tilanteen vaatimus**	**Toteuttamisen tuottama mielihyvä tai oma kiinnostus**	**Toteuttamatta jättämisestä aiheutuva häpeä, syyllisyys tai ahdistus**	**Oma usko toteuttamisen tärkeydestä**	**Muu syy, mikä?**	**En osaa sanoa syytä**
joku voi salakuunnella minua.							
tietoturva on teknistä (20 %) ja hallinnollista (80 %) työtä.							
tietoturva sisältyy perehdytykseen.							
tiedolle laaditaan elinkaari.							
tärkeä tieto salakirjoitetaan, jos siihen käsiksi pääseminen on mahdollista.							
minä saan koulutusta yrityksen tietoturvakäytäntöihin.							
minä saan tietoturvan sisältävää ohjausta ja ohjeita työhöni.							
minun tietoturvaosaamistani kehitetään jatkuvasti.							
minä tunnen yrityksen tietoturvatoimenpiteet.							
tietoturvaa seurataan hallinnollisesti.							
minä tiedän toimintatavat eri tietoturvatilanteissa.							
vanhemmat kollegat toimivat hyvänä esimerkkinä tietoturvakäyttäytymisessä.							
minä tiedän, mikä tieto on suojattavaa, missä se säilytetään ja kuka säilytystilaan pääsee.							
minä tunnen yrityksen yleisen varmuuskopiointikäytännön.							
Hallinnolliset							
		2) Syy kriteerin toteuttamiselle					
		Decin ja Ryanin menetelmän luokittelemat syyt					
Minä pyrin työtehtävissäni huomioimaan, että yrityksemme hallinnossa	**1) Mitä ajatuksia kriteeri herättää sinussa?**	**Toisen henkilön tai tilanteen vaatimus**	**Toteuttamisen tuottama mielihyvä tai oma kiinnostus**	**Toteuttamatta jättämisestä aiheutuva häpeä, syyllisyys tai ahdistus**	**Oma usko toteuttamisen tärkeydestä**	**Muu syy, mikä?**	**En osaa sanoa syytä**
osoitetaan selkeästi yrityksen johdon tuki tietoturvalle.							
huomioidaan tietoturvajohtamisen laajuus.							
huomioidaan tietoturvajohtamisen hyvä tietohallintotapa (IT Governance).							
määritellään tietoturvan resursointi.							
on toipumissuunnitelmat.							
on menettelyt sidosryhmien tietoturvan hallintaan.							
tietoturvan tavoitteita ja toteutumista seurataan ja arvioidaan.							
pidetään yhteyttä asiakkaisiin ja sidosryhmiin tietoturvaa varten.							

Liite 7. Toisen haastattelututkimuksen runko.

Väitöskirjatutkimus Kahan työntekijöille – toinen haastattelututkimus

Esipuhe

Tämä haastattelututkimus liittyy Vaasan yliopistolle toteutettavaan hallinnollista tietoturvaa käsittelevään väitöskirjatutkimukseen **hallinnollisten tietoturvakriteerien motivoivuudesta ja motivaation muutoksesta**.

Haastattelun **tavoitteena** on selvittää 1) mitkä tekijät vaikuttavat motivaation syntymiseen tietoturvakriteerien noudattamisessa ja 2) miten motivaatio muuttuu tietoturvakriteerien noudattamisessa.

Tässä haastattelututkimuksessa *tietoturvalla* tarkoitetaan *hallinnollisia tietoturvakriteerejä,* jotka ovat yksittäisiä toimenpiteitä, joilla pyritään varmistamaan tietoturvan toteutuminen yrityksessä.

Haastattelun arvioitu kesto on 30 minuuttia.

- - -

Haastattelun aloittaminen

Haastateltavan taustatiedot

1. Asema yrityksessä
a) Johtoryhmä/esimies
b) Työntekijä

2. Minä vuonna olet tullut yritykseen töihin?

Motivaation syntymistä ja muuttumista selvittäviä kysymyksiä

3. Miksi tietoturvasta huolehtiminen on sinusta tärkeää?

4. Miten motivaatiosi huomioida tietoturvaa on muuttunut sinulla siitä, kun tulit tähän yritykseen töihin? Mitkä tekijät ovat vaikuttaneet muutokseen?

5. Onko motivaatiosi tietoturvan toteuttamiseen sinulla nyt heikompaa vai parempaa verrattuna aikaan ennen tässä yrityksessä työskentelyä? Miksi?

6. Mitkä tekijät muuttavat sinun asennettasi tietoturvaa kohtaan? Miksi?

7. Mikä saa sinut kiinnostumaan tietoturvakriteerien noudattamisesta? Miksi?

8. Miten motivaatiosi tietoturvan huomioimiseen on muuttunut sinulla viimeisen 3 vuoden aikana? Mitkä tekijät ovat vaikuttaneet muutokseen? Miksi?

9. Miten motivaatiosi tietoturvan huomioimiseen on muuttunut sinulla 1v sitten tehdyn tietoturvakyselyni jälkeen? Mitkä tekijät ovat vaikuttaneet muutokseen?

10. Onko motivaatiosi tietoturvan toteuttamiseen sinulla nyt heikompaa vai parempaa verrattuna tilanteeseen ennen kyselyäni? Mistä tämä johtuu?

11. Millaisissa tilanteissa pyrit erityisesti huomioimaan tietoturvan? Miksi?

12. Mitkä tekijät lisäävät sinun motivaatiota tietoturvan toteuttamisessa? Mistä tämä johtuu?

13. Mikä saisi sinut toimimaan tietoisesti tietoturvaohjeiden vastaisesti? Miksi?

14. Mitkä tekijät vähentävät sinun motivaatiota tietoturvan toteuttamisessa? Miksi?