TIETOTURVATIETOISUUDEN LISÄÄMINEN ORGANISAATIOSSA

Case Normet Group Oy

Opinnäytetyö

Jonna Kauppinen

Liiketalouden koulutusohjelma
Yrityksen tietojärjestelmät ja viestintä

SAVONIA-AMMATTIKORKEAKOULU **OPINNÄYTETYÖ**
Iisalmen yksikkö **Tiivistelmä**

Koulutusala: Yhteiskuntatieteiden, liiketalouden ja hallinnon ala	
Koulutusohjelma: Liiketalouden koulutusohjelma	Suuntautumisvaihtoehto: Yrityksen tietojärjestelmät ja viestintä
Työntekijä/tekijät: Jonna Kauppinen	
Työn nimi: Tietoturvatietoisuuden lisääminen organisaatiossa Case Normet Group Oy	
Päiväys: 8.10.2009	Sivumäärä/liitteet: 49/5
Ohjaaja/ohjaajat: Anja Kainulainen	
Toimeksiantaja: Normet Group Oy	

Tiivistelmä:

Tämän opinnäytetyön toimeksiantaja, Normet Group Oy, on globaali yritys, joka valmistaa ja kehittää ajoneuvoja maanalaisten kaivosten ja maanalaisen rakentamisen tarpeisiin. Normet Group Oy:n pääkonttori on Iisalmessa. Konsernilla on tytäryhtiöitä ympäri maailmaa ja tytäryhtiöiden pääkonttori Normet International Ltd. sijaitsee Sveitsissä.

Opinnäytetyön tuloksena syntyvät tietoturvakoulutukset ja käyttäjäohjeisto, joiden tarkoituksena on lisätä henkilökunnan tietoturvatietoisuutta. Ohjeistoa käytetään myös uuden työntekijän perehdyttämisessä. Koska konserni on kansainvälinen, toteutetaan ohjeisto ja tietoturvakoulutukset myös englanniksi. Käyttäjäohjeisto sekä tietoturvakoulutusmateriaali ovat osa konsernin tietoturvapolitiikkaa.

Opinnäytetyön viitekehys toimii käyttäjäohjeiden ja tietoturvakoulutuksien toteuttamisen runkona. Viitekehyksessä selvitetään tietoturvan tärkeimmät käsitteet ja osa-alueet. Koska tietoturva on laaja kokonaisuus, opinnäytetyön tuotos rajataan henkilöturvallisuuden ja tietoaineistoturvallisuuden osa-alueisiin. Ulkopuolelle jätetään esimerkiksi tietoturvan tekniset ratkaisut.

Opinnäytetyössä toteutuvat sille asetetut tavoitteet. Käyttäjäohjeet sekä koulutuksissa käytettävä materiaali on kaikkien työntekijöiden saatavilla. Koulutuksia järjestetään yhteensä 17, joista 11 on Iisalmessa työskenteleville toimihenkilölle ja tuotannon henkilökunnalle. Englanninkieliset koulutukset toteutetaan WebEx -puhelinkonferenssiohjelman avulla.

Avainsanat:
tietoturvapolitiikka, tietoturva, tietosuoja, perehdyttäminen

Luottamuksellisuus:
Luottamukselliset osat: liite 1 ja liite 2 8.10.2012 asti

SAVONIA UNIVERSITY OF APPLIED SCIENCES **THESIS**
Iisalmi **Abstract**

Field of study: Social Sciences, Business and Administration	
Degree Programme: Degree Programme in Business Administration	Option: Company Information Systems and Communication
Author(s): Jonna Kauppinen	
Title of Thesis: Increasing the information security awareness in organization Case Normet Group Oy	
Date: 8.10.2009	Pages/appendices: 49/5
Supervisor(s): Anja Kainulainen	
Project/Partners: Normet Group Oy	

Abstract:

The employer of this thesis is Normet Group Oy which is a global enterprise. The enterprise manufactures and develops machines for underground mining and construction. The headquarters of Normet Group Oy is located in Iisalmi. Normet Group Oy has subsidiaries around the world and their headquarters Normet International Ltd. is located in Switzerland.

As a result of this thesis, information security trainings and a user guide were created. The purpose of these matters is to increase information security awareness of the personnel. The user guide will be used when a new employee is hired. Because the enterprise is international the user guide and information security trainings will be created in English also. The user guide and the information security material are part of the information security policy.

The framework of the thesis is the backbone for the user guide and the information security trainings. The framework explains the most important concepts and areas of information security. Because the information security is a wide concept, the thesis defines personal security and information data domains/the thesis topic is defined to the domains of personal security and information data. For example the technical solutions of information security are left outside of the thesis.

Goals of the thesis were achieved. The user guide and the material of the information security trainings are available for employees. There will be 17 arranged trainings from which 11 is for Finnish employees. Trainings in English will be arranged by WebEx teleconference program.

Keywords:

information security policy, information security, data protection, familiarization

Confidentiality:

Confidential parts appendix 1 and appendix 2 till 8 October 2012

SISÄLTÖ

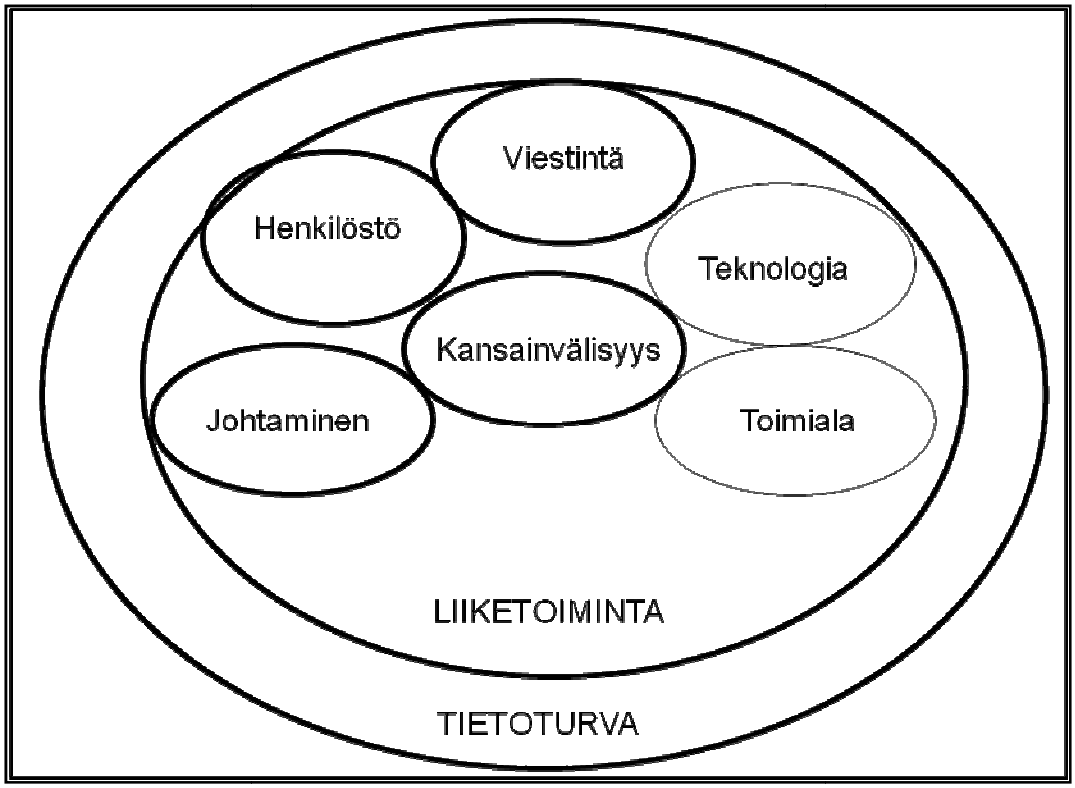
LIITTEET

1 JOHDANTO

1.1 Työn tausta ja tarkoitus

Tulevaisuudessa monet eri organisaatiot käsittelevät tietoturvaa strategisella tasolla tietoturvapolitiikkana ja tietoturvasuunnitelmina sekä ostamalla tietoturvaan liittyviä työkaluja ja tuotteita. Huomiot tietoturvan vajavaisuudesta aktivoivat tietoturvan johtamista jatkuvuus-analyyseihin, tietoturvapolitiikan kääntämistä teknisiin ratkaisuihin sekä tietoturvaratkaisujen ylläpitämiseen. (Van Bon, Kemmerling & Pondman 2002, 182.)

Tietoturva on yksi osa koko organisaation toimintaa. Liiketoimintaan sisältyvät johtaminen, henkilöstö, kansainvälisyys, viestintä, toimiala ja teknologia. Seuraavassa kuviossa 1 havainnollistetaan koko organisaation toimintaan liittyviä tekijöitä, mukaillen Kajavaa (Kajava 2001) ja Laaksosta (Laaksonen, Nevasalo & Tomula 2006, 23),



KUVIO 1. Pelkistetty organisaation toiminta (Kajava 2001; Laaksonen ym. 2006, 23)

Tietoturva toimii koko liiketoiminnan taustalla. Yrityksen johto vastaa tietoturvan hallinnasta ja henkilöstöstä, joka on olennainen osa turvallisuutta. Johdon on luotava koko yrityksen kattava, tietoturvatietoisuutta parantava ohjelma (Kajava 2001). Teknologialla tarkoitetaan kokonaisuutta, joka sisältää erilaiset organisaatiossa käytettävät tietojärjestelmät. Organisaation tehokkuus, toimivuus ja kehityskyky turvataan tietojärjestelmien luotettavuudella. (Kerttula 1999, 107.) Opinnäytetyö käsittelee tietoturvaa henkilöstön näkökulmasta eli tietoturvan käyttäjäohjeistona sekä tietoturvakoulutuksena. Kuviossa (kuvio 1) on lihavoitu ympyrät, joihin opinnäytetyössä on otettu kantaa. Opinnäytetyössä ei käsitellä tietoturvan teknisiä ratkaisuja sekä tuotos ei ole riippuvainen yrityksen toimialasta.

Tietoturvallisuuden takaaminen on suuriltaosin riippuvainen henkilöstön toimintatavoista. Henkilöstö käsittelee päivittäisessä työssään asiakkaiden, alihankkijoiden sekä toimittajien tietoja. Näitä tietoja kootaan ja prosessoidaan tiedonkäsittelyvälineillä. Tiedon säilyttäminen asiattomilta tai tuhoutumista vastaan edellyttää, että henkilökunta tunnistaa tiedon. Perusta tietoturvallisen toimintaympäristön rakentamiseen on ihmiset sekä heidän toimintatapansa. (Laaksonen ym. 2006, 19.) Tietoturvallisuuden ymmärtäminen ja toimintaohjeiden noudattaminen tukenaan tietoturvaohjelmat takaavat organisaatiolle luotettavan toimintaympäristön. Näin voidaan aikaan saada hallittuja tietoturvaratkaisuja salaisten tietojen suojaamiseksi ja välttää luvatonta käyttöä.

Helsinkiläinen ICT-alan yritys Nixu Oy on tehnyt tutkimuksen vuonna 2007 tietoturvallisuuden hallinnasta suomalaisissa organisaatioissa. Tutkimuksen mukaan kolme viidestä eri toimialasta kokivat tietoturvapolitiikat ja ohjeistukset kaikkein tärkeimmäksi organisaation kannalta. Toiselle sijalle sijoittui riskien hallinta ja kolmanneksi tärkeimpänä koettiin hyvän tietoturvan hallintatapa. Tämän perusteella voi päätellä, että tietoturvan tietämys ja hallitseminen ovat tärkeä osa suomalaisten yritysten toimintaa. Myös tietoturvapolitiikan kirjoittaminen ja sen esille laittaminen edistää turvallista toimintaa yrityksissä. (Tietoturvallisuuden hallinta suomalaisissa organisaatioissa 2007, 2007.)

Voimakkaan kansainvälistymisen myötä Normet Group Oy tarvitsi tietoturvaan liittyvää käyttäjäohjeistoa sekä henkilökunnan koulutusta tietoturvaan ennaltaeh-

käisemään tietojen leviämistä konsernin ulkopuolelle. Käyttäjäohjeiston tarkoituksena on lisätä henkilökunnan tietoturvatietoisuutta sekä ohjeistoa käytetään myös osana uuden työntekijän perehdyttämisessä. Koska konserni on kansainvälinen, toteutettiin ohjeisto ja tietoturvakoulutukset sekä suomeksi että englanniksi.

1.2 Toimeksiantajana Normet Group Oy

Opinnäytetyöni toimeksiantaja Normet Group Oy kehittää, valmistaa sekä markkinoi työkoneita ja ajoneuvoja maanalaisten kaivosten ja maanalaisen rakentamisen tarpeisiin. Normet Group Oy tarjoaa myös palveluita huoltoon ja käyttöprosesseihin tuotteen koko elinkaaren ajaksi. Konserni on tuoteryhmiensä globaali markkinajohtaja. Valtaosa tuotannosta menee ulkomaisille loppukäyttäjille. Konsernissa työskentelee noin 450 työntekijää. Konserni on perustettu vuonna 1962 Iisalmessa, Peltosalmella. Yrityksen ensimmäinen nimi oli Peltosalmen Konepaja Oy (kuvio 2).

KUVIO 2. Normet Group Oy ennen laajentumista (Arkisto, Normet Group Oy)

Vuodesta 1971 konserni tunnettiin nimellä Orion Corporation Normet. Vuonna 2008 konserni nimettiin Normet Group Oy:ksi. Koko elinikänsä aikana konserni on toimittanut yli 7000 kaivostyökonetta ympäri maailmaa. Koneiden tuotanto on pääosin Peltosalmella (kuvio 3).

KUVIO 3. Normet Group Oy laajentumisen jälkeen (Arkisto, Normet Group Oy)

Vuoden 2008 aikana konserni kansainvälistyi merkittävästi ja jatkoi kansainvälisten toimintojensa kehittämistä. Tällä hetkellä konsernin palveluverkosto toimii 15 maassa ja 23 paikkakunnalla. Konsernin kansainvälinen pääpaikka Normet International Ltd. sijaitsee Sveitsissä. Kyseisen vuoden aikana konserni teki kaksi yritysostoa. Konserni osti Chilessä toimivan betoniruiskutuslaitteita valmistavan Semmcon sekä Yhdysvalloissa toimivan varaosaliiketoimintaan erikoistuneen Rock-Tek yrityksen.

1.3 Opinnäytetyöraportin sisällöstä

Raportin alussa esitetään tuotoksena syntyneiden käyttäjäohjeiden ja tietoturvakoulutuksien laadintaan liittyvää tietoa. Tieto-osuuden jälkeen esitellään työssä käytetyt menetelmät perusteluineen. Opinnäytetyönä syntynyttä tuotosta kuvaillaan luvussa neljä. Viimeisessä luvussa pohditaan työn onnistumista sekä mahdollisia kehitysideoita. Opinnäytetyön tuotos, liitteet 1 ja 2, ovat luottamuksellisia toimeksiantajan pyynnöstä kolme vuotta.

2 TIETOTURVA YRITYKSESSÄ

2.1 Tietoturvapolitiikka

Tietoturvapolitiikka on tietoturvapäätöksien dokumentti, jossa määritellään kenellä on oikeus ja mihin resursseihin, miten pääsyä säännellään sekä kenellä on vastuu ja mihin toimenpiteisiin ryhdytään, jos rikkomuksia tapahtuu (Hallinnollinen näkökulma, 2002). Tietoturvapolitiikasta voidaan puhua valtakunnan ja organisaation tasolla. Valtakunnan tasolla tietoturvapolitiikalla tarkoitetaan tietoturvanormien ja niiden käytäntöönpanon muodostamaa kokonaisuutta. Organisaation tasolla tietoturvapolitiikka puolestaan tarkoittaa johdon hyväksymää näkemystä tietoturvallisuuden päämääristä, periaatteista sekä toteutuksesta. (Valtionhallinnon tietoturvasanasto VAHTI 8/2008, 2008.)

Tietoturvapolitiikan avulla yrityksen johto määrittelee, kuinka tietoturva-asioita käsitellään päivittäin ja miten niitä kehitetään tulevaisuudessa. Tietoturvapolitiikka on koko yrityksen tietoturvallisuusohjeistuksen sekä -koulutuksen perusta. Toisaalta Laaksosen (Laaksonen ym. 2006, 147) mukaan tietoturvapolitiikka ottaa kantaa seuraaviin asioihin yrityksen tietoturvallisuudessa: tietoturvallisuuden tavoitteet ja niihin liittyvät toimet, tietoturvallisuuden roolit ja vastuut, tietoturvallisuuskoulutus, tietojenkäsittelyn suojaaminen, yleiset linjaukset sekä seuraukset tietoturvapolitiikan laiminlyömisestä.

Tietoturvallisuuden tavoitteilla ja niihin liittyvillä toimilla tarkoitetaan tietoturvapolitiikassa johdon näkemystä, miten tietoturvallisuus vaikuttaa organisaation toimintaan sekä miten tietoturva-asioihin suhtaudutaan organisaatiossa (Laaksonen ym. 2006, 147). Tietoturvapolitiikassa määritellään myös tahot, jotka vastaavat eri tavoitteista ja niiden saavuttamisesta. Tietoturvakoulutuksen avulla pyritään saamaan henkilökunta ymmärtämään ja sisäistämään tietoturvapolitiikan eri tavoitteet sekä toimenpiteet tietoturvapolitiikan toteutumiseksi. Tietoturvapolitiikassa on myös hyvä määritellä suuntaviivat tietojenkäsittelyn suojaamiseen, esimerkiksi tietosisällön luokittelu sekä laitteiden ja sovellusten suojaaminen. Yleisillä linjauksilla käsitetään liiketoiminnan jatkuvuus- ja toipumissuunnittelun toteutuminen.

Tietoturvapolitiikan tulee myös ottaa kantaa toimenpiteisiin tietoturvapolitiikan laiminlyöntejä varten. Toimenpiteet ja sanktiot ohjeiden laiminlyönnistä tulee tiedottaa käyttäjille, jotta he ymmärtävät erilaisten tekojen seuraamukset. Ohjeissa tulee määritellä selkeästi ja ymmärrettävästi, millainen toiminta on kiellettyä. Tämä helpottaa väärinkäytöstilanteissa osoittamaan, että työntekijä on toiminut vastoin annettuja ohjeita. Teon tahallisuus voidaan osoittaa helpommin, koska sillä on merkitystä arvioidessa väärinkäytöstä rikosoikeudellisesti. (Laaksonen ym. 2006, 147.)

Yrityksen tietoturvapolitiikkaa ohjaavat tietoturvapalvelut, joita ovat mm. pääsynvalvonta ja tietojen suojaaminen sekä tietoturvateknologiat. Tietoturvateknologioita sovelletaan yrityksen eri elementteihin kuten verkkoihin, tietokantoihin, palvelimiin, päätejärjestelmiin ja ihmisiin, että yritys voi saada aikaan tietojen suojaamiseksi ja luvattoman käytön estämiseksi hallittuja tietoturvaratkaisuja. Liiketoimintaa pitää kuitenkin pystyä hoitamaan joustavasti, tehokkaasti ja turvallisesti. (Kerttula 1999, 107–108.)

Tietoturvapolitiikkaa sovelletaan yrityksen liiketoiminnan mukaan eli politiikalle ei ole yhtä ainoaa mallia. Liiketoimintaan ja tietoturvaan liittyviä asioita on hyvä pohtia yrityksen sisällä ja niiden kautta aloittaa yhtenäisen kirjallisen ohjeistuksen rakentaminen tiedon turvaamiseksi. Politiikan tulee olla tiivis ja selkeä, koska se helpottaa ymmärtämistä. (Laaksonen ym. 2006, 148.) Tietoturvapolitiikka laaditaan kirjalliseen muotoon. Sen tarkoitus on toimia ohjeena tietojärjestelmien suunnittelijoille.

Tietoturvapolitiikka toimii eri liiketoimintaprosessien taustalla keskipitkän tai pitkän aikavälin. Keskipitkällä aikavälillä tarkoitetaan noin viittä vuotta ja pitkällä aikavälillä on noin kymmentä vuotta. (Hakala ym. 2006, 7.) Politiikan kieli tulee olla selkeää ja ymmärrettävää niin, että jokainen yrityksen työntekijä ymmärtää sen sisällön. Tietoturvapolitiikka voidaan esittää myös julkisena asiakirjana, joka on tarkoitettu koko henkilökunnalle, asiakkaille ja yhteistyökumppaneille. Yhteistyökumppaneille ja asiakkaille tietoturvapolitiikalla osoitetaan, että halutaan suojata myös heidän tietonsa. (Hakala ym. 2006, 9.)

2.2 Tietoturvallisuus

2.2.1 Näkökulmia yrityksen tietoturvallisuudesta

Tietoturva tarkoittaa sähköisessä muodossa säilytettävien, käsiteltävien sekä siirrettävien tietojen, tietojärjestelmien ja palveluiden turvaamista (Sanasto, 2008). Tietoturva on perusta kaikkien tärkeiden ja luottamuksellisten tietojen käsittelyyn. Yrityksille tärkeitä tietoja ovat mm. henkilöstö, palkat, tuotteet ja myyntiluvut. Näiden tietojen suojaaminen erilaisilta väärinkäytöksiltä on edellytys yrityksen toiminnan jatkumiselle. (Järvinen 2002, 21.) Yrityksen tietoturvaopas (Yrityksen tietoturvaopas: Toimiva tietoturva - avainkysymykset, 2009) asettaa toimivalle tietoturvalle kuusi pääkysymystä, joiden avulla voidaan pohtia tietoturvatilannetta yrityksessä:

1. Tiedetäänkö tiedon säilytyspaikka sekä ketkä pääsevät tiloihin?
2. Tietääkö henkilöstö kuinka toimia eri tilanteissa sekä mitkä ovat tietoturvan pelisäännöt?
3. Ovatko tietokoneiden sekä verkon suojaukset ajantasaisia?
4. Noudatetaanko yrityksessä ohjeita?
5. Tiedetäänkö suojattava tieto?
6. Onko yrityksen johto määritellyt tietoturvan periaatteet sekä siihen liittyvät päätökset?

Yritysten tietoturva ymmärretään helposti ainoastaan tietokoneina ja niihin liittyvinä tekniikoina, kuten virusten torjunta ja varmuuskopiointi. Tietoturva kuitenkin käsittää useita erilaisia osa-alueita, joita Järvisen (Järvinen 2002, 112) mukaan ovat seuraavat: hallinnollinen turvallisuus, henkilöturvallisuus, toimitilaturvallisuus, tietojenkäsittelyn turvallisuus, tietoliikenteen turvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus, käyttötoimintojen turvallisuus, tietoaineistoturvallisuus ja yksityisyyden suoja.

Hallinnollinen turvallisuus käsittää yrityksen tietoturvaan liittyvät linjaukset, kuten tietoturvapolitiikka, sekä muut hallinnoinnin toiminnot mm. johtaminen, toiminnan organisointi ja vastuut. Henkilöturvallisuus jo nimensä puolesta käsittää henkilöstöön liittyvät toiminnot kuten työntekijöiden ohjeistuksen, koulutuksen, henkilöi-

den aiheuttamat vahingot, tahattomat ja tahalliset, sekä perehdytyskoulutukset ja salassapitosopimukset. Toimitilaturvallisuus on fyysisesti toimitilojen suojaamista ulkopuolisilta kuten kulunvalvonta ja murtosuojaus sekä myös tilojen suojaamista erilaisilta vahingoilta kuten palo- ja vesivahingot. (Järvinen 2002, 112.)

Tietojenkäsittelyn turvallisuudella pyritään varmistamaan laitteiden käyttöön ja operointiin liittyvät työtehtävät poikkeustilanteissa. Tietoliikenteen turvallisuudella turvataan tietoliikenteen jatkuvuus, siirrettävän tiedon salaaminen sekä eheyden varmistaminen. Laitteistoturvallisuudella pyritään varmistamaan tietokoneiden ja verkon toiminta sekä varautumaan mm. sähkökatkoksiin. Ohjelmistoturvallisuudella suojataan käytettyjä ohjelmia, hallitaan lisenssejä sekä rekisteröidään ohjelmia. Sen tavoite on varmistaa eri ohjelmien luvallisuus sekä estää laiton kopiointi ja käyttö. Käyttötoimintojen turvallisuudella tarkoitetaan tietokoneisiin sekä muihin aktiivilaitteisiin liittyvien asioiden turvaamista eli ylläpitotoiminnot, käyttö, huoltaminen ja valvonta. Tietoaineistoturvallisuus on erilaisten levyjen, levykkeiden ja tulosteiden turvallista käsittelyä eli pyritään suojaamaan tietojen joutumisen vääriin käsiin. Yksityisyyden suojalla halutaan suojata työntekijöiden sekä yrityksen toimintaa läheisesti liittyvät tiedot niin, että niitä käytetään vain asian mukaisiin tarkoituksiin. (Järvinen 2002, 112–113.)

Tietojärjestelmiin voi hyökätä esimerkiksi kilpailijat tai hakkerit ja näin yrityksen salassa pidettävät tiedot altistuvat väärinkäytöksille. Myös yrityksen sisällä voi ilmetä väärinkäytöksiä. Kerttulan (Kerttula 1999, 37) mukaan monet tietoturvarikkomukset tapahtuvat yrityksen sisällä, henkilökunnan, aikaisempien työntekijöiden tai vieraan työvoiman aiheuttamana. Näiden rikkomusten välttämiseen on hyvä selvittää henkilökunnalle, miksi rajoitukset ovat olemassa ja mitä tapahtuu, jos rajoituksia ei noudateta. Järvisen (Järvinen 2002, 111) mukaan työntekijöiden tulee hahmottaa heidän oma asema yrityksessä ja laajassa tietoturvan käsitteessä. Henkilökunnan tietoutta tietoturva-asioissa voi lisätä perehdytyskoulutuksella. Havainnollinen näyttäminen auttaa henkilökuntaa ymmärtämään, miten tärkeä asia tietoturva on yrityksen toiminnan jatkumisen kannalta.

2.2.2 Tietoturvallisuuden käsitteistöä

Tietoturvaan liittyy kolme keskeistä käsitettä: **luottamuksellisuus**, **käytettävyys** ja **eheys**. . Hakalan (Hakala 2006, 5) mukaan tietoturvallisuuden voi määritellä kahdella eri tavalla. Ensimmäinen määritelmä on klassisen tiedon arvoon perustuva määritelmä, joka koostuu tietoturvan kolmesta keskeisestä käsitteestä. Kerttulan (Kerttula 1999, 81) määritelmä poikkeaa hieman Hakalan määritelmästä. Kerttula käyttää muuten samoja käsitteitä kuin Hakala, mutta käytettävyydestä hän käyttää käsitettä palvelun saatavuus. Nämä käsitteet ovat Kerttulan mukaan tiedon siirron ja tiedon jakamisen perustarpeita.

Hakalan mukaan luottamuksellisuudella tarkoitetaan, että tietojärjestelmän tiedot ovat ainoastaan niihin oikeutettujen henkilöiden käytössä. Kerttulan mukaan luottamuksellisuudella pyritään pitämään tiedot salassa. Eheydellä Hakala tarkoittaa, että tietojärjestelmän tiedot ovat oikeita eivätkä sisällä tahallisia tai tahattomia virheitä. Kerttulan määritelmän mukaan eheydellä vakuutetaan, etteivät tiedot ole muuttuneet. Viimeinen käsite on molemmilla erilainen. Hakala puhuu käytettävyydestä, joka tarkoittaa, että tiedot ovat oikeassa muodossa ja nopeasti saatavilla. Kerttula puolestaan puhuu palvelun saatavuudesta, jolla pyritään pitämään tietojärjestelmä sekä sen palvelut toiminnassa sisäisesti ja ulkoisesti. (Hakala 2006, 5; Kerttula 1999, 81.)

Toinen Hakalan (Hakala 2006, 5) määritelmä tietoturvallisuudelle on laajennettu tietoturvallisuuden määritelmä. Tämä määritelmä käsittää puolestaan viisi osatekijää, joita ovat: luottamuksellisuus, käytettävyys, eheys, kiistämättömyys ja pääsynvalvonta. Kolme ensimmäistä osatekijää ovat samat kuin klassisessa määritelmässä. Laajemman määritelmän kiistämättömyydellä tarkoitetaan tietojärjestelmien kykyä sekä tunnistaa että tallentaa sen käyttäjän tiedot luotettavasti. Pääsynvalvonnalla rajoitetaan yrityksen tietojenkäsittelyinfrastruktuurin käyttöä erilaisilla menetelmillä. (Hakala 2006, 5.)

Tässä opinnäytetyössä luottamuksellisuudella tarkoitetaan, että yrityksen tietojärjestelmät ovat niihin oikeutettujen henkilöiden käytössä. Eheydellä puolestaan ha-

lutaan varmistaa tietojen virheettömyys. Käytettävyydellä pyritään pitämään tietojärjestelmä toiminnassa sisäisesti ja ulkoisesti.

2.3 Tietoturvariskit ja niihin varautuminen

2.3.1 Tietoturvan riskit ja uhat

Uhka on kohde, henkilö tai muu kokonaisuus, joka edustaa alituista vaaraa omaisuudelle. Ymmärtääkseen yrityksien kohtaamat uhat, on hyvä luokitella ne eri ominaisuuksien mukaan. Whitman ja Mattord (Whitman & Mattord 2003, 43) ovat luokitelleet erilaiset uhat viiteen ryhmään: tahattomiin toimintoihin, tahallisiin toimintoihin, ylivoimaisiin esteisiin, teknisiin häiriöihin sekä hallinnointivirheisiin.

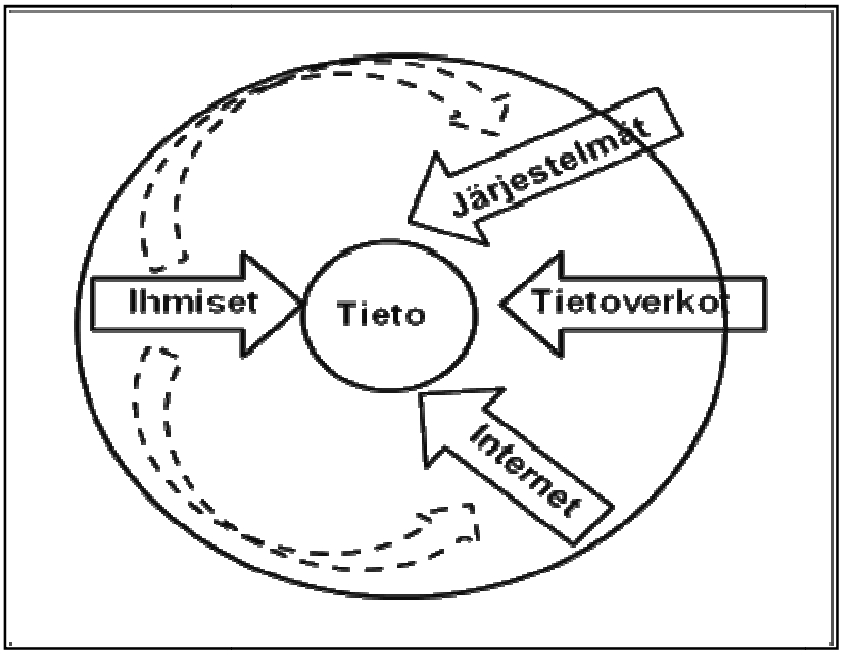
Tahattomat toiminnot sisältävät ihmisten toimintojen aiheuttamat erehdykset ja häiriöt. Tahalliset toiminnot nimensä mukaan tarkoittavat ihmisten tai yrityksen suunnitelmallista toimintaa, jonka tarkoituksena on aiheuttaa harmia ihmisille, yritykselle tai kulttuurille. Toimintoja voivat olla esimerkiksi teollisuusvakoilu, tunkeilu tai virukset. Ylivoimaiset esteet ovat sellaisia, joita ei voi estää tai kontrolloida. Tällaisia esteitä voivat olla mm. luonnonvoimien aiheuttamat vahingot palvelimille tai muille laitteille ja tiedostoille. Teknisillä häiriöillä tarkoitetaan kovalevyjen rikkoontumista tai teknisien ohjelmistojen häiriöitä ja virheitä. Viimeinen ryhmä eli hallinnolliset virheet aiheuttavat uhat, jotka johtuvat puutteellisesta suunnittelusta ja ennakoinnista. Yritys ei ole onnistunut ennakoimaan teknologian tarpeita kehittääkseen liiketoiminnan tuomia vaatimuksia. (Whitman. & Mattord 2003, 44–64.)

Hakala luokittelee riskejä seuraavasti: hallinnolliset, inhimilliset, laitteisto, ohjelmisto, ympäristö ja juridiset riskit. Riskejä tarkastellaan luottamuksellisuuden, eheyden ja käytettävyyden näkökulmasta. Hallinnollisia riskejä ovat mm. vaitiolositoumusten puuttuminen tai luottamuksellisuuden määritysten epäselvyys. Hallinnollisia eheys riskejä voi olla mm. ohjeistuksien puuttuminen. Käytettävyyden näkökulmasta hallinnollinen riski voi olla osaavan työvoiman puuttuminen esimerkiksi tietojärjestelmäasiantuntija. (Hakala ym. 2006, 66.)

Inhimilliset riskit aiheutuvat työntekijöiden toiminnasta, kun he käyttävät yrityksen tietojärjestelmiä. Riskejä ovat työntekijän vahingot ja inhimilliset erehdykset, mutta myös tahallinen yrityksen vahingoittaminen tai oman edun tavoittelu. Tietokoneiden ja tietoliikennelaitteiden käytöstä syntyvät laitteistoriskit. Laitteistoriskejä voi olla kahden tyyppistä: äkillinen toimintahäiriö tai kulumisesta aiheutuva toimintahäiriö. Ohjelmistoriskejä aiheuttavat erilaiset haittaohjelmat.

Luonnonvoimien ja fyysisten riskien aiheuttajia ovat mm. sähkökatkokset ja omaisuuden varastaminen. Näitä riskejä kutsutaan ympäristöriskeiksi. Juridisia riskejä ovat erilaisiin sopimuksiin ja lainsäädäntöön liittyvät asiat, kuten lisenssi-, käyttöoikeus-, ja palvelusopimukset. Lainsäädännössä tapahtuvat muutokset saattavat olla merkittävä riski yrityksen toiminnalle. Muutokset saattavat estää esimerkiksi tietojen hankkimisen yrityksen ulkopuolelta. (Hakala ym. 2006, 66–67.) Tämä opinnäytetyön tarkoituksena on ennaltaehkäistä työntekijöiden tahattomia ja tahallisia toimintoja sekä hallinnollisia riskejä.

Seuraavassa pelkistetyssä turvallisuusympyrässä (kuvio 4) kuvataan, kuinka ihmiset voivat päästä tietoon käsiksi, mukaillen Whitmania ja Mattordia (Whitman & Mattord 2003, 221).



KUVIO 4. Turvallisuusympyrä (M,Whitman. & H, Mattord 2003, 221)

Yleisesti tietoturvaympyrästä huomataan, kuinka tieto on eri suunnista tulevien hyökkäysten kohteena. Ihmiset pääsevät käsiksi tietoon suoraan esimerkiksi lukemalla dokumentteja suoraan yrityksen tietojärjestelmistä. He pääsevät myös käsiksi tietoon tietojärjestelmien kautta. Tieto on yrityksen tärkein omaisuus, siksi se on sijoitettu tietoturvaympyrässä keskelle. Tieto on aina riskialtis eri suunnilta tuleville hyökkäyksille. Varsinkin, kun ihmisillä ja tietojärjestelmillä on yhteys tietoihin. Järjestelmillä ja Internetillä kuvataan ympyrässä epäsuoria uhkia, esimerkiksi henkilö koettaa päästä tietoon käsiksi Internetin kautta. Ensiksi henkilön täytyy päästä sisään paikalliseen verkkoon ja sen kautta tunkeutua tietojärjestelmiin, jotka sisältävät henkilön tarvitsemaa tietoa. (Whitman. & Mattord 2003, 220.)

Alla esitellään taulukko (taulukko 1), jossa vasemman puoleisessa sarakkeessa on lueteltu yleisimpiä tietoturvariskejä. Oikean puoleisessa sarakkeessa on lueteltu keinoja, kuinka välttyä tietoturvariskien toteutumiselta, mukaillen Kerttulaa. (Kerttula 1999, 43.)

TAULUKKO 1. Tietoturvariskit ja niihin varautuminen (Kerttula 1999, 43)

Tietoturvariski	**Varautuminen**
Laiton tunkeutuminen	Palomuurit
Tietojen anastaminen yhteydeltä	Salaaminen
Tietojen muuttaminen	Palomuurit, host-koneen suojaaminen, datan eheystyökalut
Sähköpostin sieppaaminen tai väärentäminen	Suojattu sähköposti
Tietokonevarkaus	Fyysiset turvatoimenpiteet, laptop-tietojen salaaminen
Virukset	Virustentorjuntaohjelmat
Sisäinen tietoturvarikkomus	Käytön valvonta ja henkilökunnan ohjeistaminen, pääsynvalvonnan huolellinen suunnittelu, järjestelmäsuojausten käyttö

Organisaatioiden on hyvä tiedostaa sekä myös kartoittaa omaan tietoturvallisuuteen liittyvät mahdolliset riskit ja uhat. Kun riskit ja uhat on kartoitettu, kuten esimerkkinä voisi toimia yllä oleva tauluko (taulukko 1), on organisaation mietittävä myös

niiden vaikutuksia toimintaan ja sen jatkuvuuteen. Kun riskit ja uhat sekä niiden vaikutukset ovat selvitetty, on etsittävä keinoja ja menetelmiä niiden toteutumisen välttämiseksi. (Hakala ym. 2006, 29,31.)

Tietoturva Ry:n ja Tampereen yliopiston teettämän kyselytutkimuksen mukaan suomalaisyritykset ovat tiedostaneet tietoturvan uhat melko hyvin. Yleisimmin havaitut tietoturvaongelmien syyt olivat virukset, järjestelmän virheet ja käyttäjän virheet. Harvinaisempia syitä olivat salakuuntelu ja ylläpitovirheet. Tutkimus osoittaa, että henkilöstön tietoturvakoulutukseen kannattaa edelleen panostaa. Tutkimuksen toteuttaja Juhani Paavilaisen mukaan suomalaisyritykset aliarvioivat järjestäytyneen rikollisuuden ja vakoiluorganisaatioiden uhkaa. Paavilainen kertoo, että suojelupoliisi on jo muutaman vuoden ajan varoitellut yrityksiä, että Suomessakin harjoitetaan ammattimaista teollisuusvakoilua. Tällainen uhka koetaan kuitenkin pieneksi. Paavilainen muistuttaa, että kännykkään hölöttävä myyntitykki on yhtälailla tietoturvariski kuin jokin teknisempi tekijä. (Kyselytutkimus: tietoturvauhat tiedostettu, 2001.)

IT-viikon artikkelissa ”Omat työntekijät suurin tietoturvauhka” kerrotaan 2008 Study on the Uncertainty of Data Breach Detection -tutkimuksen tuloksista. Kyselytutkimuksen mukaan yli puolet eurooppalaisissa yrityksissä tehdyissä tietomurroissa aiheuttaja on ollut yrityksen oma työntekijä. Ainoastaan kuudesta prosentista vastaavat erilaiset hakkerit. Tutkimus todistaa, että luottamuksellinen tieto päätyy yrityksen ulkopuolelle niiden kautta, kenelle luottamuksellinen tieto on uskottu. (Omat työntekijät suurin tietoturvauhka, 2008.)

2.3.2 Tietoturvaohje

Yrityksen näkökulmasta henkilöstön tietoturvakäyttäytymiseen liittyvät kolme asiaa:

1. tietoturvapolitiikka, -ohjeistus ja -koulutus
2. vanhempien kollegojen näyttämä esimerkki
3. työntekijöiden oma ”maalaisjärki”.

Yrityksen arvot, politiikat ja toimintaohjeet toimivat työntekijöiden tiedonlähteinä. Nämä auttavat työntekijöitä ymmärtämään henkilöstöön kohdistuvat odotukset. Tietoturvapolitiikka ja -ohjeet ovat henkilöstön toimintatapojen runko. Ohjeet muodostavat yrityksen hyväksymän turvallisuuteen liittyvän käyttäytymismallin. Tähän vaikuttavat ohjeiden kattavuus, selkeys ja yhdenmukaisuus. Eteen tulevat tilanteet pyritään hoitamaan yrityksessä olevien käytäntöjen mukaan. (Laaksonen ym. 2006, 249.)

Järvinen (Järvinen 2002, 117–120) on luetellut kuusi pääaluetta, joihin pelisäännöt ja ohjeistaminen ovat tarpeen. Pääalueet ovat: tietokoneet, nettikäyttö, sähköposti, yrityksen verkkosivut, yleiset asiat ja etätyö. Tietokoneet -alueen ohjeistukset liittyvät laitteisiin, ohjelmiin ja käyttötapoihin. Nettikäyttö -alueessa ohjeistettavat asiat liittyvät verkon käytön vaaroihin ja valvontaan sekä mikä on yrityksessä sallittua ja mikä ei. Sähköposti -alueen ohjeistuksessa muistutetaan mm. sähköpostietiketistä ja viestien käsittelystä, yksityisten asioiden hoidosta ja lomavastaajan käytöstä. Yrityksen verkkosivut -alueessa ohjeistetaan verkkosivujen päivittämisen vastuusta, hyökkäyksien seuraamisesta ja palautteiden sekä kysymysten vastaanottamisesta. Yleiset asiat -alue ohjeistaa arkipäiväiseen toimintaan ja yrityksen kulunvalvontaan liittyviin asioihin. Viimeinen alue, etätyö, ohjeistaa etätyöhön liittyviin asioihin. (Järvinen 2002, 117–120.)

Laadittaessa ohjeistusta on hyvä pyrkiä mahdollisimman yksiselitteiseen ja helposti ymmärrettävään tekstiin. Ohjeiden merkityksen pilaa ristiriitainen ja epäselvä teksti. Ohjetta suunnitellessa on hyvä käydä läpi ensin kaikki muut yrityksen ohjeet. Näin varmistetaan, että tietoturvaohjeistus esitetään samalla tavalla ja tarkkuudella muiden ohjeiden kanssa. (Laaksonen ym. 2006, 250.)

2.3.3 Tietoturvatutkimukset

Organisaatioiden tietoturvaan liittyviä tutkimuksia julkaistaan vuosittain useita. Suurin osa tutkimuksista on kansainvälisiä. Opinnäytetyön kannalta merkityksellisiä tutkimuksista ensimmäinen on suomalaisen ICT-alan yrityksen NIXU:n vuonna 2007 tekemä tutkimus: tietoturvallisuuden hallinta suomalaisissa organisaatioissa. Tutkimuksen tarkoituksena oli selvittää suomalaisten yritysten tietoturvan nykyti-

laa, haasteita ja hallintaa. Tutkimustuloksista ilmeni, että suurin haaste tietoturvan toteuttamiselle ovat resurssit sekä vastauksissa painottui useasti tietoturvan tekninen puoli. (Tietoturvallisuuden hallinta suomalaisissa organisaatioissa 2007, 2007.)

Toinen tutkimus oli Security Transcends Technologyn teettämä kansainvälinen tutkimus tietoturvan työpanoksesta, Global Information Security Workforce (. Tutkimuksen tarkoituksena oli selvittää tietoturva-alan tärkeimmät kehityssuunnat ja mahdollisuudet maailman laajuisesti. Tutkimuksesta nousi esiin muutamia avain-asioita, joita olivat mm. hallinnon tietoturvakoulutuksen kasvava kysyntä, tietoturvan käyttö- ja järjestelmäkehitys, liiketoiminnan jatkuminen ja onnettomuuksista selviytymisen suunnittelu ja yksityisyys. Frost & Sullivan, 2008.)

Kolmanneksi tutustuin The Ernst & Youngin vuonna 2008 tekemään kansainväliseen tietoturvatutkimukseen, The Global Information Security. Kyseisessä tutkimuksessa oli havaittu kymmenen avain-asiaa, joita olivat mm. maineen ja brändin suojaaminen, kansainväliset tietoturvastandardit, tietoturvan strateginen näkökulma ja tietoturvan heikkoudet. (Ernst & Young, 2008.)

Näiden esille otettujen tutkimusten tuloksista huomataan, miten tärkeä osa tietoturva ja sen ymmärtäminen on päivittäistä yrityksen toimintaa ja sen jatkumista. Tulokset osoittavat myös, että tietoturvan hallitseminen on pääasiassa teknistä sekä henkilökunnan kouluttamiseen, tietoturvan suunnitteluun ja onnettomuuksiin varautumiseen on tarvetta.

2.4 Tietosuoja

Tietosuoja on henkilötietojen suojaamista ulkopuolisilta tai henkilöä vahingoittavalta käytöltä (Sanasto, 2008). Ennen tietoturva ja tietosuoja ymmärrettiin lähes samaksi käsitteeksi. Käsitteet kuitenkin erotetaan toisistaan henkilökohtaisten tietojen suojaamiseksi ja organisaation tietojen turvaamiseksi. (Gollmann 1999, 6.) Markkinoinnin, sähköisen kaupankäynnin, kansallisen turvallisuuden ja monien muiden asioiden myötä ovat tietosuojaan liittyvät kysymykset nousseet esiin. Itse tiedot eivät ole salaisia, esimerkiksi henkilön nimi tai osoite. Kuitenkin niiden aiheeton rekisteröinti ja yhdistely eri lähteistä aiheuttavat henkilölle itselleen haittoja.

Kuitenkaan kaikki seuranta ja valvonta eivät vaaranna yksityisyyttä mm. tietojärjestelmää käytettäessä henkilön toimet saatetaan usein rekisteröidä ja tallentaa lokiin. Lokien avulla voidaan jäljittää tekijä, jos väärinkäytöksiä tapahtuu. Viranomaisilla voi olla myös oikeus eri tietojen keräämiseen ja käsittelyyn. (Järvinen 2002, 30.)

Kleemola (Kleemola & Pellikka 1998, 1) on määritellyt tietosuojan seuraavanlaisesti:

> *Tietosuojalla tarkoitetaan henkilörekisterilain tarkoittamalla tavalla ko. lailla säänneltyjen henkilötietojen käsittelyä koskevien vaatimusten huomioon ottamista yksityisten henkilöiden yksityisyyden ja oikeusturvan varmistamiseksi* (Kleemola & Pellikka 1998, 1).

Näin ollen, tietosuojalla pyritään rajoittamaan ihmisen henkilötietojen keräämistä ja käsittelyä. Järvisen (Järvinen 2002, 21) mukaan esimerkiksi henkilön nimi tai osoite ei ole salainen, mutta niiden tarpeeton rekisteröinti ja yhdistely eri lähteistä voi aiheuttaa henkilölle itselleen haittaa. Tietosuojan taustalla on lakipaketti, joka sisältää henkilötietolain, lain yksityisyyden suojasta televiestinnässä ja lain yksityisyyden suojasta työsuhteessa. Henkilötietolaki on kaikkien taustalla oleva yleislaki. (Helsilä 2002, 201.)

2.5 Perehdyttäminen ja tietoturvakoulutus

2.5.1 Perehdyttäminen

Perehdyttämisellä tarkoitetaan toimenpiteitä, joiden avulla yritys pyrkii sopeuttamaan uuden henkilön mahdollisimman joustavasti työhön ja työympäristöön. Perehdyttämisellä, etenkin työhön opastamisella, voidaan erotella hyvät yritykset huonoista. (Helsilä 2002, 52.) Perehdytys on puolestaan se vaihe, kun uusi työntekijä tulee taloon ja hänelle aletaan kertoa olennaisia asioita hänen työstään, työyhteisöstään, koko organisaatiosta ja sen toimialasta (Juholin 2008, 233).

Helsilän (Helsilä 2002, 15) mukaan henkilöstötyö sisältää kolme eri kokonaisuutta: henkilöstön muodostamisen, henkilöstön suuntaamisen ja ylläpidon sekä henkilöstön osaamisen kehittämisen. Henkilöstön muodostamisella tarkoitetaan rekrytointia, perehdyttämistä ja työpaikkakoulutusta. Henkilöstön kehittämisen osa-alue sisältää jatkuvan parantamisen ja kehityskeskustelut. Opinnäytetyön tuotos sisältää henkilöstön muodostamisen osa-alueesta perehdyttämisen sekä työpaikalla tapahtuvan koulutuksen.

Yrityksen sisällä jokaisella työntekijällä on vastuu tietojen säilymisestä. Tietoturva toimii parhaiten, kun jokainen yrityksen sisällä tuntee toimintaohjeet. Tietoturvaoppaan mukaan suurin työpanos kannattaa sijoittaa ihmisten perehdyttämiseen, ei paksujen ohjekirjojen tekemiseen. Välinpitämätön henkilöstö voi romuttaa hyvin toteutetut tekniset turvaratkaisut. Kouluttamisella voidaan myös vähentää työyhteisön sisällä tapahtuvia väärinkäytöksiä. (Yrityksen tietoturvaopas: Toimiva tietoturva – panosta henkilöstön osaamiseen, 2009.)

2.5.2 Tietoturvakoulutus

Jokainen yrityksessä työskentelevä tulisi kouluttaa tietoturvaan, mutta jokaisella ei tarvitse olla tietoturvan muodollista koulutusta tai todistusta. Tietoturvakoulutus liittyy yrityksen jäseniin yksityiskohtaisella tiedolla sekä hyvin suunnitellulla johdannolla. (M,Whitman. & H, Mattord 2003, 223–224.)

Tietoturvakoulutuksen tavoite on saada työntekijät toimimaan johdon haluamalla tavalla niin, että yrityksen tiedot suojataan tarkoituksen mukaisesti. Henkilökunnan ei tarvitse tietää kaikkea tietoturvasta. Työntekijöiden tulee ymmärtää omaan työhönsä liittyvät riskit ja niiden minimointi. Tietoturvan tekniset ratkaisut tulisi näkyä työntekijälle mahdollisimman vähän. (Laaksonen ym. 2006, 254.)

Koulutuksen suunnittelun tulisi ensisijaisesti pohjautua tietoturvapolitiikkaan ja sitä täydentäviin toimintaohjeisiin sekä prosessikuvauksiin ja erilaisissa auditoinneissa tai katselmoinneissa havaittuihin tietoturvakäyttäytymisen puutteisiin. Koulutuksen tehokkuus kuitenkin riippuu henkilöstön motivaatiosta. Tietoturvakoulutuksessa tulisi huomioida erilaisten motiivien vaikutus oppimiseen. Käytännön esimerkkien

avulla henkilöstölle avautuu parhaiten mitä politiikalla, ohjeilla ja toimintamalleilla tarkoitetaan. Jos tietoturvaohjeita ei avata käytännön tasolle, tietoturvallisuus ei tule olemaan tavoitteiden edellyttämällä tasolla. Erilaisten esimerkkien tarkoitus on saada työntekijöiden kanssa keskustelua aikaiseksi erilaisista toimintatavoista sekä myös miten tietoturvaohjeita käytännössä noudatetaan ja miksi niitä tulee noudattaa. (Laaksonen ym. 2006, 254–255.)

Tehokas tapa saada ihmiset ajattelemaan omaa päivittäistä käyttäytymistään on kysymysten asettelu. Yksinkertaisella kysymyksellä esimerkiksi siitä, minkälaista luottamuksellista tietoa henkilö käsittelee päivittäisessä työssään, saa aikaan keskustelua tiedon luottamuksellisuudesta ja julkisuudesta. Päivittäin käsiteltävää tietoa ei aina mielletä niin luottamukselliseksi kuin esimerkiksi tietoturvaohjeistus edellyttää. (Laaksonen ym. 2006, 256.) Koulutuksen yhteydessä havainnollinen esitys voi olla tehokkaampaa kuin eri kieltojen luetteleminen. Kun esimerkki näyttää, kuinka hakkeri voi saada tiedon haltuunsa, katsojat ymmärtävät asian merkityksen paremmin. Esimerkiksi pelkkä hupiohjelmien lähettämisen kieltäminen sähköpostissa unohtuu nopeasti, koska sen merkitystä ei ymmärretä. (Järvinen 2002, 117.)

Työyhteisössä oppimiselle on erilaisia näkökulmia mm. toimintaoppiminen, oppiva yhteisö ja tietämisen yhteisö. Toimintaoppimisen mukaan oppiminen on sekä autonomista että sosiaalista. Autonomisesta näkökulmasta oppija hallitsee toimintaansa ja oppimistaan itse. Sosiaalisesta näkökulmasta oppiminen tapahtuu niin, että työntekijät oppivat toisiltaan. Työyhteisössä oppimisen sosiaalisuus tarkoittaa, että jaetaan erilaiset vastoinkäymiset työyhteisön sisällä. Olennaista oppimisessa on kokemusten jakaminen toisten kanssa. Oppivan yhteisön näkökulma tarkoittaa, että oppiminen tapahtuu ilman kouluttajaa tai asiantuntijaa. Työyhteisö oppii toistensa kokemuksista. Tietämisen yhteisön näkökulma liittyy lisääntyvään tiedon ja viestinnän merkitykseen organisaatiossa. Organisaatiossa tietämisen yhteisöt muodostavat osaamisen verkoston. (Järvinen, Koivisto & Poikela 2000, 103, 105–106.)

3 OPINNÄYTETYÖN TOTEUTTAMINEN

3.1 Lähtökohta ja tarve tietoturvakoulutukselle

Yrityksen historiassa on tapahtunut viime vuosien aikana nopea laajentuminen maailmanlaajuiseksi yritykseksi. Uusien tytäryhtiöiden syntyminen ja jatkuva kehittyminen on lisännyt salaisten ja luottamuksellisten tietojen säilyttämistä. Opinnäytetyö tarjosi yritykselle mahdollisuuden yhdentää sekä parantaa Normet Group Oy:n tietoturvaa ja näin saada yhtenäinen ohjeistus koko konsernin henkilökunnalle. Tuotoksena syntyi käyttäjäohjeisto ja henkilökunnalle järjestettävät tietoturvakoulutukset sekä suomeksi että englanniksi. Käyttäjäohjeisto ja tietoturvakoulutusmateriaali tulevat jatkossa olemaan osa uuden työntekijän perehdyttämistä sekä konsernin tietoturvapolitiikkaa (katso luku 2.1).

Aiheena tietoturva tulee aina olemaan yksi osa yrityksen toimintaa ja se on yksi tärkeimmistä kehitysalueista, jos haluaa pysyä markkinoilla. Tietoturva ei ole ainoastaan tietoteknisiä ratkaisuja. Tietoturva on käsitteenä erittäin laaja, joten toimeksiantajan kanssa sovittiin, mitä tietoturvan alueita käyttäjäohjeissa tullaan käymään tarkemmin läpi. Pääasiassa aineisto rajattiin henkilöturvallisuuden ja tietoaineistoturvallisuuden osa-alueelle. Ulkopuolelle jäi tietoturvan tekniset ratkaisut sekä toimitilaturvallisuus. Tietoturvakoulutuksessa kuitenkin käytiin lyhyesti läpi kaikki tietoturvan kymmenen osa-aluetta. (katso luku 2.2.1.)

Työn tehtävä oli saada koko Normet Group Oy:n henkilökunta ymmärtämään tietoturvan tärkeys sekä millaisilla keinoilla he voivat omassa työssään välttää tietoturvariskien toteutumista. Käyttäjäohjeiden tarkoitus on tuoda esille, millaisia riskejä työntekijöiden tietämättömyys ja huolimattomuus voi aiheuttaa yritykselle ja mahdollisesti myös työntekijälle itselleen. Työn tarkoituksena oli myös muistuttaa koko konsernin henkilökuntaa tietoturvan tärkeydestä sekä mitä kaikkea tietoturva kattaa. Tietoturvaohjeistus on henkilökunnan toimintatapojen runko. Ohjeet muodostavat yrityksen hyväksymän tietoturvallisuuteen liittyvän käyttäytymismallin (katso luku 2.3.2).

Syy tietoturvakoulutuksen järjestämiseen oli varmistaa tietoturvaohjeiden sisältö kaikkien tietoon, koska pelkkä ohjeistus olisi monelta jäänyt lukematta. Tietoturvakoulutuksen yksi tavoite oli saada henkilökunta ymmärtämään omaan työhönsä liittyvät riskit sekä niiden minimoiminen (katso luku 2.3.1.) Koulutuksella pyrittiin myös saamaan aikaiseksi keskustelua sekä ehdotuksia mahdollisesti myös tietoturvan parantamiseksi. Käyttäjäohjeisto sekä tietoturvakoulutusmateriaali ovat kaikkien työntekijöiden saatavilla. Usein tietoturvaan kiinnitetään vasta silloin huomiota, kun vahinko on tapahtunut.

Tietoturvakoulutus suunnattiin Normet Group Oy:n toimihenkilöille Suomessa ja ulkomailla toimiviin tytäryhtiöihin. Koulutusten alkaessa myös tuotannon työntekijöitä koulutettiin hieman tiiviimmällä koulutuksella, koska tuotannon työntekijöitä ei koske esimerkiksi matkapuhelimen käyttöön tai matkustamiseen liittyvät tietoturva-asiat. Lopulliseksi tuotokseksi valmistuivat käyttäjäohjeet sekä suomeksi että englanniksi ja kolme eri koulutusmateriaalia, koulutusmateriaali suomeksi ja englanniksi sekä tiiviimpi koulutusmateriaali tuotannon henkilökunnalle. Käyttäjäohjeisto ja koulutusmateriaalit tulostettiin PDF -muotoon ja tallennettiin yrityksen dokumentinhallintajärjestelmään myöhempää käyttöä varten.

3.2 Käyttäjäohjeen toteuttaminen

Varsinainen opinnäytetyö alkoi suomenkielisten käyttäjäohjeiden suunnittelulla. Koska tradenomin tutkintokokonaisuuteen kuuluu syventävä harjoittelu, yhdistettiin opinnäytetyö harjoitteluun Normet Group Oy:n ICT-osastolla. Näin tietoturvan käyttäjäohje sekä tietoturvakoulutukset palvelevat paremmin yrityksen tarpeita, kun oli tilaisuus tutustua olemassa oleviin tietoturvaohjeistoihin ja laatukäsikirjaan. Harjoittelun aikana oli mahdollisuus keskustella ICT -osaston että muiden Normet Group Oy:n työntekijöiden kanssa. Käyttäjäohjetta tehdessä tutustuttiin tietoturvaan liittyvään kirjallisuuteen, tutkimuksiin, lehtiin sekä luotettaviin lähteisiin Internetissä.

Aluksi kirjoitettiin ohjeistolle johdanto, jossa selvitettiin, miksi käyttäjäohje on tehty, kuka huolehtii sen päivittämisestä sekä mitkä kaikki asiat vaikuttavat ohjeiston taustalla. Käyttäjäohjeen runko muodostui teoriatiedon pohjalta eli millaisia tietoturvaan liittyviä asioita henkilökunnalle tulisi ohjeistaa. Käyttäjäohjeelle muodostui näiden pohjalta seitsemän pääotsikkoa: salassapito- ja vaitiolovelvollisuus, käyttäjätunnukset - ja oikeudet, salasana, Internetin käyttö, sähköposti, tiedon siirtäminen ja matkapuhelimen käyttö sekä hyvä tietää ja muistaa. Hyvä tietää ja muistaa -osioon kerättiin ohjeita tietoaineistoturvallisuuden ja tietosuojan osa-alueista (katso luku 2.4).

Pääotsikoiden alla olevat ohjelauseet pyrittiin muodostamaan mahdollisimman yksinkertaisiksi ymmärtää, koska ohjeistusta tehdessä on pyrittävä yksiselitteiseen ja helposti ymmärrettävään tekstiin. Ohjelauseiden väliin etsittiin asiaan liittyviä esimerkkejä. Esimerkkien tarkoitus on havainnollistaa esimerkiksi ohjeen laiminlyönnistä aiheutuvaa seurausta yritykselle tai työntekijälle. Koska opinnäytetyötä tehdessä käytiin läpi yrityksessä jo olevia tietoturvaan liittyviä ohjeistuksia, tarkoitus ei ollut muuttaa ohjeistolla aiemmin ohjeistettuja, vaan käyttää samaa linjausta ja mahdollisesti tarkentaa tai lisätä ohjeistettua asiaa Jos ohjelauseessa viitattiin johonkin ohjeeseen, esimerkiksi ohje salasanan vaihtamiseen, merkittiin sulkuihin liitteen numero, josta ohje löytyy. Sanoja, joita haluttiin korostaa sekä painottaa, lihavoitiin ja alleviivattiin. (katso luku 2.3.2.)

Kun käyttäjäohjeen pääotsikoiden ohjeistukset alkoivat hahmottua, poimittiin ohjeista erilaisia käsitteitä, jotka vaativat selitystä ohjeen ymmärtämiseksi. Käsitteitä olivat: asiakastuki, Bluetooth, käyttäjätunnus, käyttäjäoikeus, salasana, salassapitovelvollisuus, vaitiolovelvollisuus ja tietomurto. Käsiteluettelo sijoitettiin heti johdannon jälkeen. Käsitteiden jälkeen lisättiin yhteystiedot, jotka sisältävät asiakastuen ja ICT- osaston yhteystiedot. Ohjelauseissa viitattiin yhteystietoihin.

Yrityksen ICT-osaston työntekijät Daniel Ranta-aho ja Mika Moilanen sekä esimies, Jussi Ahomaa, lukivat käyttäjäohjeen läpi, yhteensä neljä kertaa. Käyttäjäohjeeseen tehtiin tarkennuksia sekä muutoksia heidän kommenttien ja ehdotusten perusteella. Myös henkilöstöpäällikkö, Annu Tuominen, tarkisti ohjeiston salassapito- ja vaitiolovelvollisuusosion asianmukaisuuden. Kun käyttäjäohjeisto oli val-

mistunut Suomeksi, käännettiin käyttäjäohjeisto Englanniksi. Englanninkielisen käyttäjäohjeen kielitarkistuksen teki Savonia-ammattikorkeakoulun englanninkielen lehtori.

3.3 Koulutuksien suunnittelu ja toteutukset

Koulutusmateriaalin runko muodostui käyttäjäohjeiden pohjalta. ICT-osaston esimiehen avustuksella valittiin käyttäjäohjeesta asiat, jotka käydään tietoturvakoulutuksessa läpi. Materiaalin pääotsikot poimittiin suoraan käyttäjäohjeesta. Näin käyttäjäohjeen lukijan on helppo yhdistää ohjeiston ja koulutuksen materiaalit. Koulutusmateriaalin liitteeksi tehtiin myös taulukko riskeistä ja uhkista (katso liite 3). Taulukon tiedot poimittiin teoriatiedon (katso luku 2.3.1) sekä yrityksessä voimassa olevien ohjeistojen pohjalta esimerkiksi paloturvallisuusohje. Taulukon avulla pyrittiin yhdistämään sekä havainnollistamaan myös kaikki tietoturvan osa-alueet. Koulutusmateriaali toteutettiin MS PowerPoint -ohjelmalla. Ohjelman avulla tehtiin koulutusmateriaaliin muutaman havainnollistavan animaation, koska Järvinen mainitsee teoksessaan, että koulutuksen yhteydessä havainnollinen esitys voi olla tehokkaampaa kuin kieltojen luetteleminen (Järvinen 2002, 117.) Näin saadaan koulutettavat paremmin ymmärtämään asian merkitys.

Ennen varsinaista koulutustilaisuutta pidettiin testikoulutus, johon osallistui kahdeksan Normet Groupin toimihenkilöä. Suurin osa osallistujista oli esimiestasolla työskenteleviä. Testikoulutus pidettiin noin kahta viikkoa ennen varsinaisia koulutustilaisuuksia. Testikoulutettavien palautteiden mukaan muutettiin koulutusdiojen esittämisjärjestys ja tehtiin muutoksia koulutustilaisuuden arviointilomakkeeseen. Arviointilomakkeen parantamiseksi pienennettiin arviointiasteikkoa 1–5 asteikkoon 1–4. Näin saadaan karsittua niin sanotut ”en osaa sanoa” -vastaukset ja arvioinnista saadaan totuudenmukaisempi. Arviointilomakkeeseen lisättiin myös yleisarvosana sekä kouluttajan arvioiminen. Kouluttajaa arvioitiin esiintymisen sekä asiantuntijuuden alueilta (katso liite 4).

Koulutuksen alkuun suunniteltiin johdanto-osio, jossa selvitettiin, mitä tietoturva tarkoittaa sekä miksi tietoja suojataan. Johdantoon liitettiin myös tehtäviä (osa kysymysmuodossa), koska Laaksosen (Laaksonen ym. 2006, 256) mukaan tehokas

tapa saada käyttäjät ajattelemaan päivittäistä käyttäytymistään on kysymysten asettelu.

Koulutuksen vuorovaikutteisuutta lisättäviä tehtäviä olivat seuraavat:

- Millaisia tietoturvaan liittyviä asioita käsittelet päivittäisessä työssäsi?
- Kirjaa tilanteita, joissa tietoturva tulisi huomioida
- Mitä tietojen katoaminen tai leviäminen merkitsisi työn kannalta?

Vastaukset pyydettiin kirjoittamaan paperille. Näin pyritään varmistamaan, että jokainen pohtii asioita omalta kohdaltaan. Johdanto-osiossa tullaan keskustelemaan myös siitä, mitä on tietoturva ja sitten käydään tiiviisti läpi kaikki tietoturvan osa-alueet Järvisen (Järvinen 2002, 112.) mukaan.

Lisäksi käsitellään tietoturvan uhkia. Lopulliseksi tietoturvakoulutuksen sisällöksi muodostuivat seuraavat otsikot: johdanto, koulutuksen sisältö, salassapito- ja vaitiolovelvollisuus, käyttäjätunnukset- ja oikeudet, salasana, Internetin käyttö, sähköposti, tiedonsiirtäminen ja matkapuhelimen käyttö sekä hyvä tietää ja muistaa. Tuotannon koulutuksien otsikot olivat muuten samat, paitsi pois jätettiin tiedonsiirtäminen ja matkapuhelimen käyttö.

Tietoturvakoulutuksiin lähetettiin kutsut noin kuukautta ennen koulutustilaisuuksia. Englanninkielisien koulutuksien kutsut lähetettiin noin neljää viikkoa ennen koulutuksia. Kutsut lähetettiin yrityksessä käytössä olevan sähköpostiohjelman kautta. Yritys antoi Excel-taulukon, johon oli listattu työntekijät osastoittain. Excel-taulukon perusteella kutsu koulutukseen lähetettiin eri osaston työntekijöille. Jokaiselle ryhmälle jaettiin koulutusajankohta osastoittain. Koulutusajankohdat olivat joka aamupäivä 8–12 tai iltapäivä 12–16.

Viestissä pyydettiin myös ilmoittamaan sekä sopimaan koulutus toisen ryhmän mukana, mikäli kyseinen ajankohta ei jostain syystä käy. Viestiin liitettiin lista, johon oli merkitty päivä, kellonaika ja osallistujat. Liitteenä (liite 5) on toimihenki-

löille lähetetty sähköpostiviesti suomeksi ja englanniksi. Viesti kirjoitettiin yhdessä toimeksiantajan kanssa. Viestissä painotettiin, että koulutus on pakollinen.

3.4 Opinnäytetyön edistyminen

Opinnäytetyö edistyi ja valmistui suunnitellun aikataulun mukaan. Tietoturvaan liittyvää materiaalia on runsaasti tarjolla, joten haasteena oli löytää mahdollisimman tuoreet sekä luotettavat lähteet. Materiaalia löytyi myös runsaasti vieraalla kielellä. Tässä opinnäytetyössä on käytetty englanninkielisiä lähteitä. Opinnäytetyössä hyödynnettiin myös tuoreita tietoturvaan liittyviä tutkimuksia (katso luku 2.3.3). Tuotos valmistui viikkojen 10–22 aikana.

Työnantaja tarjosi tietokoneen ja käyttäjäoikeudet opinnäytetyön tekemistä varten. Opinnäytetyön toteuttamisesta ei kertynyt toimeksiantajalle merkittäviä kustannuksia, tuotos tallennettiin sähköiseen muotoon. Kustannuksia kertyi ainoastaan palautelomakkeiden ja kouluttajan materiaalin tulostamisesta.

Alla olevassa taulukossa (taulukko 2) kuvataan eri resurssien käyttöä sekä opinnäytetyön edistymistä viikkotasolla. Vasemman puoleisiin sarakkeisiin on merkitty viikot ja tehtävät. Oikean puoleisiin sarakkeisiin on merkitty toteutuminen ja tehtävään käytetyt resurssit. Taulukko on tehty opinnäytetyösuunnitelmaan suunnitellun aikataulun pohjalta.

TAULUKKO 2. Opinnäytetyön edistyminen

Viikko	**Tehtävä**	**Toteutuminen**	**Resurssit**
10-11	Tutustuminen yrityksen tietoturvaohjelmaan, toimintaan ja käyttäjien päivittäiseen työskentelyyn	Toteutunut	Toimeksiantajan tarjoama tietokone, työtila, käyttöoikeudet
11-16	Käyttäjäohjeiden laadinta sekä koulutusmateriaalin tekeminen	Toteutunut	Toimeksiantajan tarjoama tietokone, työtila, käyttöoikeudet
17-19	Testikoulutus, toimeksiantajan tarkistukset ja täsmennykset	Testikoulutus 29.4.2009, Täsmennykset viikolla 19	Toimeksiantajan tarjoama tietokone, työtila, käyttöoikeudet
20-22	Tietoturvakoulutukset eri käyttäjäryhmille	18.-19.5.2009 25.-26.5.2009	Auditorio, Normet Oy
23-	Opinnäytetyönraportin kirjoittaminen, viimeistely ym.	Kesä/Syksy 2009	Toimeksiantajan sekä Savonia AMK:n tarjoama tietokone sekä ohjelmat

Tuotoksen toteutusaikataulu oli tiivis, mutta opinnäytetyön yhdistäminen syventävään harjoittelujaksoon auttoi materiaalin valmistumiseen tiiviissä aikataulussa. Toimeksiantaja tarjosi tuotoksen toteuttamiseen myös tietokoneen, käyttäjäoikeudet sekä ohjelmat. Opinnäytetyön tekemisessä käytettiin seuraavia ohjelmia: Word, PowerPoint sekä PDF Creator.

4 KÄYTTÄJÄOHJEET JA TIETOTURVAKOULUTUS

4.1 Käyttäjäohjeisto

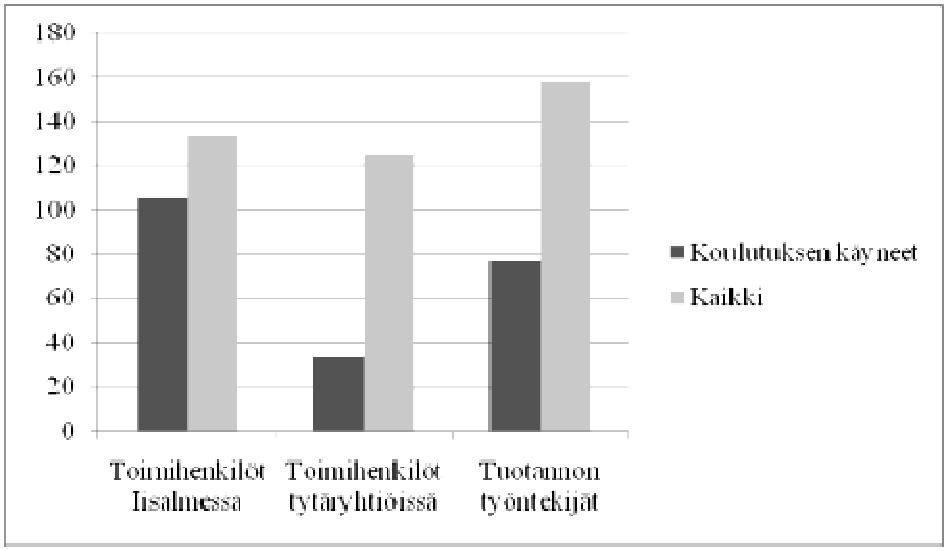
Tuotoksena syntynyt käyttäjäohjeisto ja tietoturvakoulutusmateriaali suomeksi ja englanniksi ovat toimeksiantajan pyynnöstä luottamuksellisia 8. lokakuuta 2009 alkaen kolmen vuoden ajan (liitteet 1–2). Luottamuksellisuus päättyy 8.lokakuuta 2012. Käyttäjäohjeisto on sivumäärältään tiivis (12 sivua, lisäksi liitteet), sillä asiat on pyritty kertomaan mahdollisimman selkeästi ja yksinkertaisesti. Käyttäjäohjeisto sisältää johdannon, käsiteluettelon ja yhteystietolistan lisäksi seitsemän pääotsikkoa: salassapito- ja vaitiolo velvollisuus, käyttäjätunnukset ja -oikeudet, salasana, Internetin käyttö, sähköposti, tiedon siirtäminen ja matkapuhelimen käyttö sekä hyvä tietää ja muistaa.

Johdannossa kerrotaan käyttäjäohjeiston tarkoitus, kenen vastuulla on päivittäminen sekä mitkä asiat vaikuttavat ohjeistuksen taustalla. Johdannon jälkeen on selitetty muutamia käsitteitä, joita ohjeistossa mainitaan. ICT -osaston yhteystiedot löytyvät ennen varsinaista ohjeiston alkamista. Pääotsikoiden alla kerrotut ohjeet ovat esitetty yksinkertaisesti lyhyillä lauseilla. Ohjelauseiden väliin on sijoitettu myös esimerkkejä, joiden avulla pyritään vielä tarkentamaan ohjeen tarkoitusta, tärkeyttä ja mahdollisia seurauksia. Käyttäjäohjeisto sisältää myös kuusi liitettä. Liitteet käsittelevät mm. erilaisia ohjeistuksia, joihin on viitattu ohjelauseen yhteydessä. Ohjeiden loppuun on liitetty myös lähdeluettelo. Käyttäjäohjeiston sisältö tulee esille tietoturvakoulutuksista (katso luku 4.2), sillä koulutusmateriaali on muodostettu käyttäjäohjeen pohjalta.

4.2 Tietoturvakoulutukset

Tietoturvakoulutukset järjestettiin keväällä ja kesällä 2009. Koulutukset venyivät kesälle tytäryhtiöiden koulutuksien takia, koska yhteistä ajankohtaa oli erittäin vaikea löytää. Kuitenkin ennen varsinaisia koulutuksia pidettiin testikoulutustilaisuus, jonka avulla testattiin koulutuksessa käsiteltävää materiaalia. Testikoulutuksen tarkoitus oli tarkentaa materiaalia. Samalla testattiin myös koulutuksia varten suunniteltu palautelomake. Koulutusmateriaali tehtiin käyttäjäohjeiston pohjalta. Kaikkiaan koulutuksia järjestettiin 17 kappaletta, joihin osallistui yhteensä 208 työnteki-

jää ympäri maailmaa. Suunnitelman mukaan tarkoitus oli pitää ainoastaan Suomessa sekä tytäryhtiöissä työskenteleville toimihenkilöille, mutta koulutusten aikana kuitenkin huomattiin, että koulutus on tarpeellinen myös tuotannon työntekijöille. Koulutusmateriaalia tiivistettiin vastaamaan heidän tarpeitaan (katso luku 4.5). Alla olevassa kuviossa (kuvio 5) on verrattu koulutuksen käyneitä työntekijöitä koko työntekijäryhmään.



KUVIO 5. Tietoturvakoulutukseen osallistuneet ryhmittäin

Iisalmessa työskenteleviä toimihenkilöitä koulutettiin yhteensä 106 eli 79 prosenttia konsernin koko henkilökunnasta. Kaiken kaikkiaan Iisalmessa työskentelee 134 toimihenkilöä. Koulutettavissa ryhmissä oli vaihteleva määrä osanottajia, mutta kuitenkin koulutuksessa oli kerrallaan keskimäärin 12 toimihenkilöä. Koulutuksia varten varattiin yrityksen tiloissa sijaitseva auditorio, josta löytyi videoprojektori Power Point -esitystä varten. Kesto vaihteli kahden ja neljän tunnin välissä. Koulutuksille oli kuitenkin varattu aikaa neljä tuntia.

Tytäryhtiöissä työskenteleviä osallistui kaikista vähiten tietoturvakoulutuksiin. Yhtiöissä työskentelee yhteensä 125 toimihenkilöä, joista ainoastaan 33 osallistui koulutuksiin. Poisjäännin syynä olivat lähinnä aikaerot, lomat ja muut työasiat. Tuotannon osastolla työskentelee 158 henkilöä, joista noin puolet osallistui tietoturvakoulutukseen. Koulutukset kestivät tunnin verran ja työntekijöitä kävi kolmessa ryhmässä eli yhden päivän aikana 77 henkilöä.

Tietoturvakoulutusryhmät jaettiin osastoittain. Kuitenkin työntekijällä oli mahdollisuus vaihtaa ryhmää, jos ryhmän koulutusajankohta ei sopinut aikatauluun. Pohjana ryhmäjaolle oli toimintaoppimisen näkökulma (katso luku 2.5.3). Jokainen voi vaikuttaa oppimiseensa, mutta oppiminen tapahtuu myös muiden kommenttien, näkökulmien ja kokemusten kautta. Osastokohtainen jako toimintaoppimisen näkökulmasta tuo myös esille juuri sillä osastolla koettuja ja jaettuja kokemuksia tietoturvasta.

Koulutuksen lopuksi jaetussa palautelomakkeessa (liite 4) arvioitiin jokaista koulutuksessa käytyä osa-aluetta asteikolla 1–4 (1= välttävä, 2=tyydyttävä, 3=hyvä ja 4= erinomainen). Lomakkeessa pyydettiin antamaan koulutukselle myös kokonaisarvosanan, joista laskettiin koulutuskohtaiset keskiarvot, jokaiselle arvioitavalle osa-alueelle. Palautelomake oli tiiviimpi tuotannon koulutuksissa, koska tuotannon koulutus ei sisältänyt kaikkia toimihenkilöiden koulutusmateriaalin osa-alueita.

4.3 Tietoturvakoulutuksien sisältö ja palautteet

4.3.1 Johdanto

Ennen koulutuksen alkua jaettiin kaikille tyhjät paperilaput sekä kynät. Tietoturvakoulutus alkoi esittäytymisellä sekä mistä koulutuksen järjestäminen on saanut alkunsa eli koulutus on osa opinnäytetyötä ja se on toteutettu käyttäjäohjeiston pohjalta. Alussa kerrottiin myös, mistä käyttäjäohjeiston löytää koulutuksien jälkeen eli jokaiselle työntekijälle lähetetään linkki käyttäjäohjeisiin sähköpostilla. Varsinainen koulutus alkoi koulutuksen tavoitteiden ja tarkoituksen esittelyllä, josta siirryttiin johdanto osioon.

Johdannon alussa koulutettaville esitettiin kysymys: mitä termi tietoturva tuo mieleen. Koulutettavia pyydettiin kertomaan ääneen asioita, mitä kyseinen termi tuo mieleen. Tämän jälkeen kerrottiin lyhyt selitys termille tietoturva. Tässä yhteydessä käytiin lyhyesti läpi tietoturvan kymmenen eri osa-aluetta. Näiden jälkeen koulutettaville esitettiin kysymyksiä, joihin heidän tuli miettiä vastauksia omalta kohdaltaan. Vastaukset kirjatattiin tyhjälle paperille, joka jaettiin heti koulutuksen alussa. Ensimmäinen kysymys oli: millaisia tietoturvaan liittyviä asioita käsittelet päivit-

täisessä työssäsi. Koulutettaville annettiin muutama minuutti aikaa miettiä ja kirjata asioita paperille. Tämän jälkeen koulutettavia pyydettiin kertomaan kirjaamiaan asioita. Toinen kysymys oli: kirjaa tilanteita, joissa tietoturva tulisi huomioida. Tähän myös annettiin muutama minuutti kirjata paperille tilanteita. Viimeinen kysymys oli, että mitä tietojen katoaminen tai leviäminen merkitsisi työn kannalta. Kysymykseen ei tarvinnut vastata kirjallisesti, vaan koulutettavia pyydettiin suullisesti kertomaan tietojen häviämisen seurauksia.

Lopuksi kerrottiin lyhyesti, miksi tietoja suojataan sekä millaisia uhkia tietoturvaan liittyy. Koulutus jatkui tietoturvakoulutuksen sisällön esittelyllä. Koulutuksen sisältö sisältää seitsemän osa-aluetta, jotka ovat käyttäjäohjeiden otsikoita. Kevennykseksi, ennen ensimmäistä osa-aluetta eli salassapito- ja vaitiolovelvollisuus, näytettiin lyhyt animaatio, mitä kaikkea kallisarvoista voi kadota. Animaatiossa pieni mies kävelee dian poikki ja häneltä tippuu asiapapereita, käyttäjätunnuslappu, avaimet ja USB -tikku.

4.3.2 Salassapito - ja vaitiolovelvollisuus

Aluksi käytiin läpi salassapito- ja vaitiolovelvollisuutta eli mitä se tarkoittaa, ketä kaikkia se koskee ja mitä seuraa sen laiminlyönnistä. Koulutettavia muistutettiin myös miettimään, mitä kertoa yrityksen asioista ulkopuolelle. Varsinkin näin lamaaikana ihmisiä kiinnostaa yrityksen taloudellinen tilanne sekä lomautukset. Yleisesti ohjeistettiin, että kaikki mitä lehdissä on kerrottu, niistä voi puhua. Jokaisen kuitenkin tulee harkita tilanne- ja asiakohtaisesti, mitä ulkopuolelle kertoo. Tämän yhteydessä näytettiin taulukko (katso liite 3), johon oli listattu erilaisia tietoturvan uhkia, miten niihin voi varautua, mitä tapahtuu uhkan toteutuessa sekä kehen tulee ottaa yhteyttä havaitessaan uhkan. Taulukko käytiin koulutettavien kanssa lyhyesti läpi.

Salassapito - ja vaitiolovelvollisuus -osion aikana syntyi keskustelua koulutettavien kesken sekä myös asiaan löytyi konkreettisia esimerkkejä. Jokaisen osion jälkeen koulutettavilla oli mahdollisuus esittää kysymyksiä. Alla on kuvio (kuvio 6), jossa on kaikista kahdeksasta koulutuksesta saatujen arvioiden keskiarvot salassapito - ja

vaitiolovelvollisuus -osasta. Salassapito - ja vaitiolovelvollisuus koettiin toiseksi hyödyllisemmäksi koulutuksissa.

4.3.3 Käyttäjätunnukset - ja oikeudet

Toinen osa-alue oli käyttäjätunnukset - ja oikeudet. Ensiksi kerrottiin, mitä kyseinen termi tarkoittaa. Tässä yhteydessä selvitettiin koulutettaville yleisesti sekä kuinka Normet Groupissa on rajoitettu käyttäjien oikeuksia. Käyttäjätunnuksiin ja -oikeuksiin liitettiin myös esimerkki tietomurrosta. Näin koulutettaville haluttiin selventää, millaisia seurauksia voi olla, jos käyttää toisen tunnuksia ilman lupaa. Tietomurto herätti koulutettavissa kysymyksiä sekä kommentteja. Lopuksi haluttiin muistuttaa uloskirjautumisen tärkeydestä koneelta tai järjestelmästä poistuttaessa. Seurauksena voi olla ulkopuolisen tunkeutuminen järjestelmään verkon kautta tai suoraan käyttäjän tunnuksilla, jos kone on jätetty auki. Normet Groupin käytössä olevien ohjelmien uloskirjauksessa tuotiin esille lähinnä käytäntöön ja lisensseihin liittyviä asioita. Kuviossa (kuvio 6) nähdään arvioiden keskiarvo, kuinka hyödylliseksi osio koettiin.

4.3.4 Salasana

Salasanaan liittyvä ohjeistus oli luonnollisesti heti käyttäjätunnukset - ja oikeudet -osan jälkeen. Aluksi kerrottiin, mitä termillä tarkoitetaan; salasanan suositeltava minimi pituus sekä millaisia merkkejä salasanan tulisi sisältää. Tässä yhteydessä selvitettiin myös, kuinka salasana tulee muodostaa tiettyihin Normet Groupin ohjelmiin, koska ohjelmissa on tiettyjä rajoitteita salasanan muodostamiseen. Koulutettaville esitettiin lista, johon oli listattu asioita, joita ei tulisi käyttää salasanana. Asioita, joita ei tulisi käyttää salasanana, ovat mm. käyttäjätunnus, yritystoimintaan liittyvä asia tai oma syntymäaika. Erityisesti keskustelua koulutettavien kesken synnytti salasanan vaihtaminen sekä lista, joita ei tulisi käyttää salasanana. Koulutettavat kokivat salasanan vaihtamisen moneen eri järjestelmään työläänä sekä uuden salasanan muistamisen. Koulutettavia neuvottiin muodostamaan salasana jonkun itselle mieluisan laulun tai runon ensimmäisistä tavuista. Näin salasanan voi muistaa paremmin ja se ei ole helposti arvattavissa. Koulutuksien salasana-osio koettiin hyödylliseksi alla olevan kuvion (kuvio 6) mukaan.

4.3.5 Internetin käyttö

Koulutuksen puolessa välissä käytiin läpi Internetin käyttöön liittyviä asioita. Näkökulma ja lähtökohta olivat työnantajan tarjoaman tietokoneen Internetin käyttö. Koska Normet Groupissa on käytettävissä sekä pöytäkoneita että kannettavia tietokoneita, jotkut ohjeistukset saattoivat enemmän koskea kannettavia tietokoneita. Tämä osa-alue aloitettiin yleisesti kertoen, kuinka käyttäjien vastuu hämärtyy Internetissä eli Internetissä tehdyt asiat eivät tunnu oikeilta, koska niitä ei tee konkreettisesti. Tässä yhteydessä kerrottiin pelkistetty esimerkki, että ohjelman varastaminen kaupan hyllyltä on sama asia kuin laiton lataaminen Internetistä sekä näytettiin PowerPointilla tehty animaatio esimerkkiin liittyen. Internetin käyttö työpaikalla on sallittua, mutta koulutuksessa ohjeistettiin välttämään mm. keskustelupalstoja. Koulutuksessa tuotiin myös esille, miksi tietyt Internet-sivut eivät aukea sekä ohjeistettiin miten toimitaan, jos joku työn kannalta oleellinen sivu ei aukea. Internetin käyttöön liittyvien asioiden kouluttaminen tietoturvan osalta koettiin tarpeelliseksi, mutta kuitenkin kaikkiin muihin osa-alueisiin verrattuna ei niin tarpeelliseksi (katso kuvio 6).

4.3.6 Sähköposti

Kolmanneksi viimeisenä koulutuksessa käytiin läpi sähköpostin tietoturvallista käyttöä sekä informoitiin Normet Groupin asettamia rajoitteita. Ensiksi käytiin läpi suuruusrajat tiedostoille sekä miksi näin on. Tiedostojen suuruudet aiheuttivat kiivasta keskustelua, koska työhön liittyy suurien tiedostojen lähettämistä. Seuraavaksi koulutettaville näytettiin lista vaarallisiksi luokitelluista tiedostopäätteistä. Lista on myös liitetty käyttäjäohjeeseen ja jokainen voi halutessaan tulostaa sen työpisteelle jo ennen kuin epäilyttävä tiedostopääte tulee vastaan. Lisäksi neuvottiin, minne ottaa yhteyttä, jos sähköpostin liitetiedosto ei tule perille.

Koska jokaisella Normet Groupissa työskentelevällä toimihenkilöllä on oma sähköpostiosoite, niin työsähköpostin käyttöä myös ohjeistettiin. Työsähköposti on tarkoitettu lähinnä työasioiden hoitamiseen. Kuitenkin muissa yhteyksissä on tärkeä muistaa, kuinka osoitetta käyttää, sillä yrityksen nimi on osoitteessa mainittu. Esimerkiksi harrastusten yhteydessä mainittu työsähköpostiosoite voi joutua ns.

sähköpostiosoitteiden testaajien kohteeksi eli osoitteeseen lähetetään roskapostia ja näin testataan toimiiko osoite. Roskaposti sisältää usein viruksia. Roskaposti myös kuormittaa suodattimia.

Sähköposti-osio sisälsi paljon tärkeää asiaa, sillä sähköposti on olennainen osa työntekoa. Salasanasta muistutettiin vielä. Työsähköpostin salasanan tulee olla eri kuin henkilökohtaisen sähköpostin. Osiossa ohjeistettiin myös loma-ajan sähköpostiin liittyviä asioita. Loma-ajan ja muutenkin työsähköpostin lähettäminen henkilökohtaiseen sähköpostiin on kielletty. Loma-aikana on käytettävä Out of Office -toimintoa tai muuta vaihtoehtoista toimintoa. Kuitenkaan missään tapauksessa ei saa antaa omia käyttäjätunnuksia työkaverille. Loma-ajan sähköpostivaihtoehdoista pyydettiin keskustelemaan oman esimiehen kanssa.

Työsähköpostiin kirjautumista muualta kuin työkoneelta pitäisi myös välttää. Jos kuitenkin jostain syystä joutuu kirjautumaan, niin ohjeistettiin tyhjentämään selaimen välimuisti. Ohje välimuistin tyhjentämiseen löytyy ohje käyttäjäohjeiden liitteistä. Myös yksityisen sähköpostin käyttöä työkoneelta ohjeistettiin siten, että varsinkin liitetiedostojen aukaisemista työkoneella kannattaa harkita. Sähköpostiin liittyvien asioiden kouluttaminen koettiin kaikkein hyödyllisimmäksi osioksi. Kuvion (kuvio 6) mukaan keskiarvo on yli kolme ja puoli.

4.3.7 Tiedon siirtäminen ja matkapuhelimen käyttö

Koska Normet Groupin työntekijöillä on käytössää matkapuhelimia, ohjeistettiin myös niiden tietoturvallista käyttöä sekä tiedostojen siirtämiseen liittyviä tietoturva-asioita. Toiseksi viimeinen osa oli nimeltään tiedon siirtäminen ja matkapuhelimen käyttö. Erilaisten tiedonsiirtolaitteiden käyttöä ohjeistettiin välttämään työkoneella. Kuitenkin esimerkiksi muistitikkujen käyttö joissain tilanteissa on välttämätöntä, joten koulutettaville ohjeistettiin, mihin asioihin muistitikkua käyttäessä tulee kiinnittää huomiota. Salaisen tiedon siirtämiseen ohjeistettiin käyttämään työnantajan tarjoamaa ohjelmaa. Ohjelman käyttöön on myös ohjeistus, joka on liitetty käyttäjäohjeisiin.

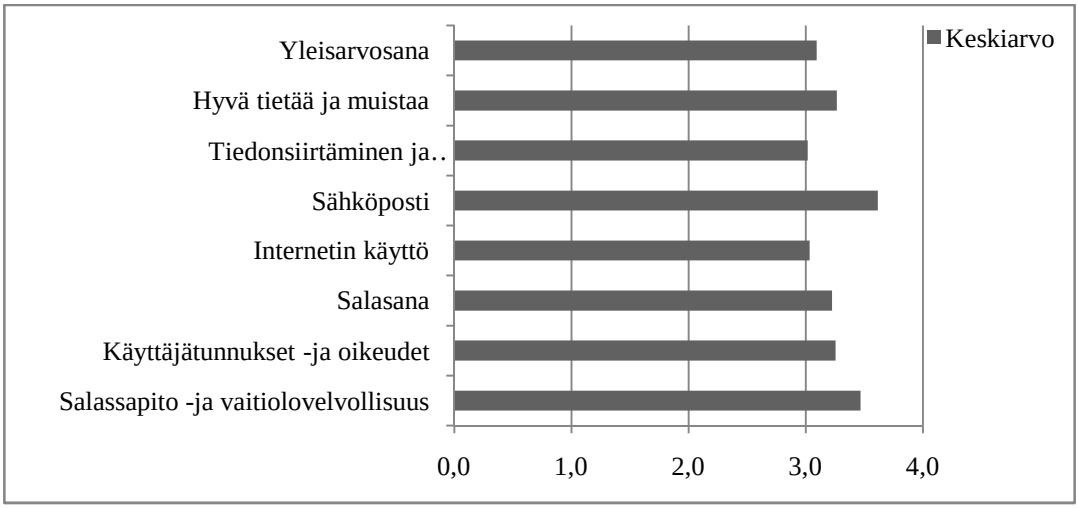
Matkapuhelimen käyttäjiä ohjeistettiin pitämään Bluetooth sekä Wlan -hakua pois päältä, koska mobiilivirukset yrittävät tunkeutua puhelimeen näiden kautta. Myös multimediaviestien (MMS) avaamisessa ohjeistettiin varovaisuuteen. Ohjeistuksien jälkeen kerrottiin, mitä mobiilivirukset voivat aiheuttaa. Puhelimen katoamisen sekä hajoamisen varalta ohjeistettiin ottamaan varmuuskopioita puhelimesta, erityisesti ennen matkaa. Kuvion (kuvio 6) mukaan tiedon siirtämistä ja matkapuhelimen käyttö -osio koettiin muihin osioihin verrattuna vähiten hyödylliseksi koulutuksissa.

4.3.8 Hyvä tietää ja muistaa

Viimeisessä osassa eli hyvä tietää ja muistaa, muistutettiin tietosuojaan liittyvistä asioista, luottamuksellisten asiakirjojen hävittämisestä sekä säilyttämisestä. Tässä osassa painotettiin myös tietokoneen ulkopuolella olevia uhkia, joita tulee ottaa huomioon. Myös tiedostojen käsittelyyn ja nimeämiseen esitettiin esimerkki. Koulutettavia muistutettiin katsomaan mm. Word tai Excel -taulukon ominaisuudet ennen lähettämistä. Asiakirjan ominaisuuksissa näkyy otsikkorivillä ensimmäiseksi asiakirjaan tallennettu otsikko. Tämä on hyvä tarkistaa, varsinkin, jos käyttää samaa pohjaa useasti ja eri asiakkaille. Kuitenkin suositeltavaa on tulostaa asiakirja PDF -muotoon.

Osion yhteydessä syntyi keskustelua paljon vierailijoiden liikkumisesta yrityksen tiloissa, lähinnä nykyisistä käytännöistä sekä myös parannusehdotuksia tulevaisuutta varten. Koulutettavia pyydettiin kirjaamaan myös lopuksi jaettavaan palautelomakkeeseen kommentteja sekä kehitysideoita.

Alla olevan kuvion (kuvio 7) mukaan hyvä tietää ja muistaa -osio koettiin hyödylliseksi. Koulutuksien keskiarvo on yli kolme.



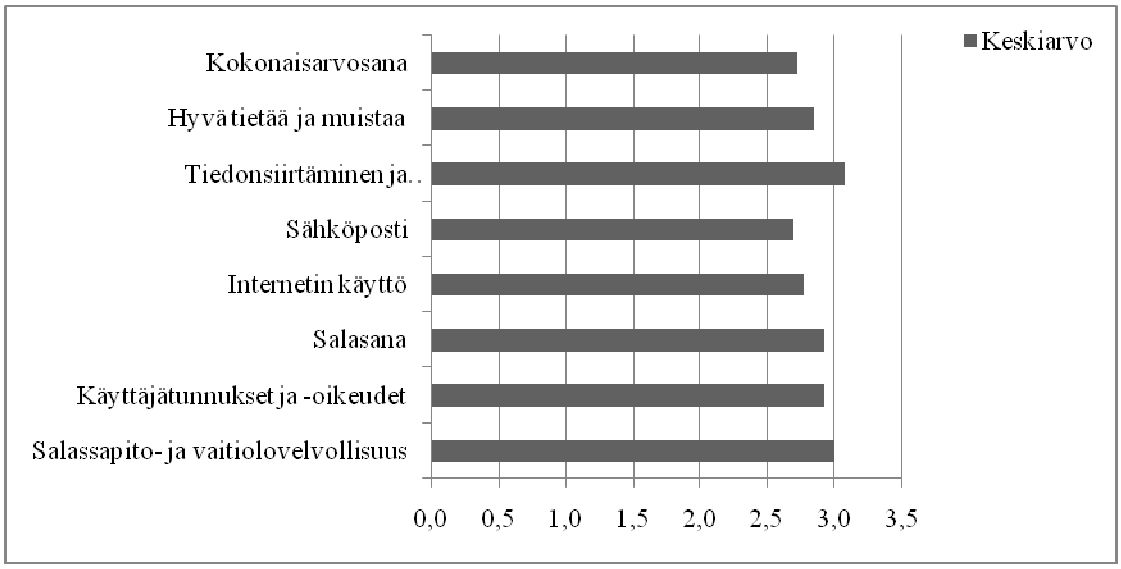
KUVIO 6. Yhteenveto toimihenkilöiden koulutuksista (n=106)

Kokonaisuudessaan tietoturvakoulutus koettiin hyödylliseksi. Sähköposti sekä salassapito- ja vaitiolovelvollisuus -osiot koettiin muihin verrattuna kaikista hyödyllisimmäksi. Suurin osa työhön liittyvistä asioista hoidetaan sähköpostin kautta. Tiedonsiirtäminen ja matkapuhelimen käyttö sekä Internetin käyttö -osiot koettiin muita vähemmän hyödyllisiksi. Tämä johtuu siitä, että pienellä osalla työntekijöitä on matkapuhelin työpuolesta käytössään.

4.3.9 Englanninkielisen koulutuksen toteutuminen ja palaute

Englanninkielinen koulutus toteutettiin käyttäen työnantajan tarjoamaa WebEx -puhelinkonferenssiohjelmaa. Koulutus käytännössä toteutui puhelimen ja tietokoneen avulla. Kaikki osallistujat saivat linkin ja salasanan kirjautuakseen koulutukseen. Ohjelman kautta näytölle sai näkymään englanniksi PowerPoint -esityksen. Koulutus noudatti samanlaista kaavaa kuin suomenkielinen koulutuskin. Poikkeuksena oli kysymysten kysely -osio, joka jäi tekemättä Web toteutuksen takia. Yhden puhelimen ympärillä oli useita henkilöitä kuulemassa koulutusta, joten kyselyosio ei olisi palvellut sen tarkoitusta. Englanninkielinen koulutus sisälsi myös koulutuksen tarkoituksen ja tavoitteiden esittelyn sekä johdanto osion, jossa kerrottiin lyhyt selitys termille tietoturva sekä tietoturvan uhat. Osa-alueiden otsikot olivat samat kuin suomenkielisessä koulutuksessa.

Kouluttaminen puhelinkonferenssiohjelman kautta tehtiin ensi kertaa yrityksen historiassa. Palautteiden kautta kävi ilmi, että tällainen koulutusmuoto oli haasteellinen myös kuulijoille. Yhteys oli välillä heikko ja koulutettavien oli vaikea ymmärtää, mitä kouluttaja sanoi. Englanninkielisestä koulutuksesta ei ehditty pitää testikoulutusta kuten suomenkielisestä koulutuksesta, koska työntekijöillä oli tiukka aikataulu työnsä puolesta. Onneksi kuitenkin pieni osa ulkomailla työskentelevistä saatiin koulutettua. Alla olevassa taulukossa on englanninkielisten koulutusten keskiarvot.



KUVIO 7. Yhteenveto englanninkielisistä koulutuksista (n=33)

Tiedon siirtäminen ja matkapuhelimen käyttö sekä salassapito- ja vaitiolovelvollisuus koettiin kaikista hyödyllisimmäksi. Ulkomaan yhtiöissä työskentelevät joutuvat liikkumaan paljon työnsä puolesta ja heillä on myös käytössään matkapuhelin. Tämän vuoksi tietoturvakoulutuksen osio tiedon siirtäminen ja matkapuhelimen käyttö koettiin hyödylliseksi.

4.3.10 Tuotannon henkilökunnan koulutus ja palaute

Tuotannon työntekijöiden koulutuksessa käytiin kuusi osa-aluetta läpi. Osien pääotsikot olivat myös käyttäjäohjeen pohjalta. Pääotsikoita olivat: sähköposti, käyttäjätunnukset - ja oikeudet, salasana, Internetin käyttö, sähköposti sekä hyvä tietää ja muistaa. Koulutuksen sisältö määriteltiin toimeksiantajan tarpeiden mukaan. Kou-

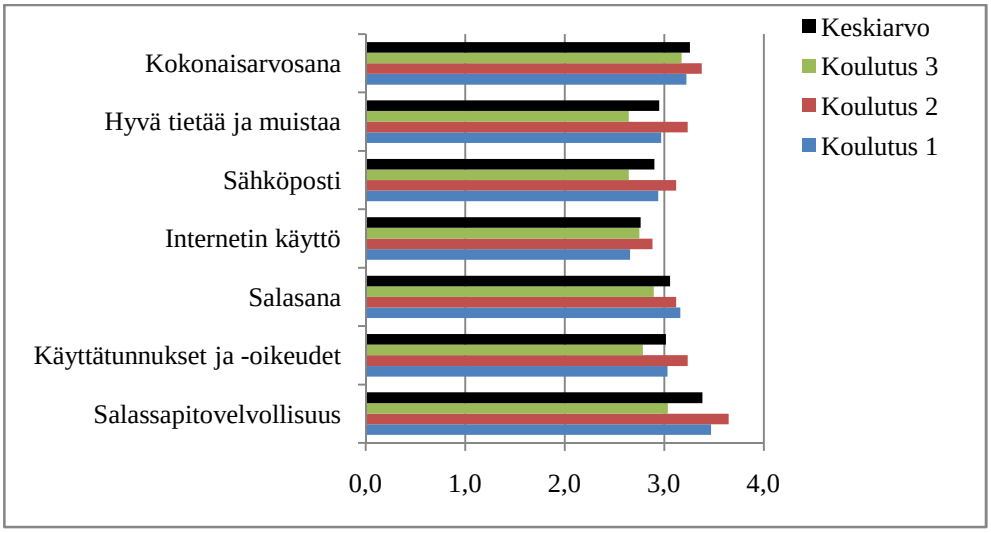
lutus alkoi esittelyllä sekä koulutuksen tavoitteiden ja tarkoituksen kertomisella. Tämän jälkeen siirryttiin johdantoon. Johdannossa koulutettaville esitettiin kysymys: mitä termi tietoturva tuo mieleen? Kommentteja kysymykseen pyydettiin suullisesti. Kommenttien jälkeen esitettiin tiivis määritelmä termille tietoturva. Koulutus eteni tietoturvauhkiin, jonka jälkeen näytettiin, mitä asioita koulutuksessa tullaan käymään läpi.

Koulutus jatkui salassapito - ja vaitiolovelvollisuuden määrittelyyn. Tässä osiossa painotettiin erityisesti, että jokaisella Normet Groupin työntekijällä on salassapito - ja vaitiolovelvollisuus ilman erillistä sopimusta. Salassapito - ja vaitiolovelvollisuus on osa työsopimusta. Erityisesti muistutettiin koulutettavia miettimään, mitä puhuu, kenelle puhuu ja missä puhuu. Painoarvo oli myös velvollisuuden rikkomisen seurauksista, joita pahimmillaan voivat olla irtisanominen tai vankeusrangaistus.

Käyttäjätunnus ja -oikeus -osiota sekä salasana -osiota käytiin tiiviimmin läpi kuin toimihenkilöiden koulutuksessa. Tuotannon työntekijöillä ei ole henkilökohtaisia käyttäjätunnuksia ja salasanoja vaan tunnukset ja salasanat ovat koontipaikkakohtaiset. Kuitenkin käsitteet selitettiin sekä painotettiin, etteivät käyttäjätunnus ja salasana saa olla näkyvillä tai kirjoitettuna mihinkään. Koulutuksessa muistutettiin myös, että esimerkiksi salasanan muodostamiseen liittyviä ohjeita voi hyödyntää henkilökohtaisessa tietokoneen käytössä. Internetin käyttö ja sähköposti -osioissa noudatettiin samaa kaavaa kuin toimihenkilöidenkin koulutuksessa.

Tuotannon koulutuksien tärkein osio oli hyvä tietää ja muistaa, jossa käsiteltiin asiakirjojen käsittelyyn sekä ulkopuolisiin tietoturvauhkiin liittyviä asioita. Osaalueen aikana keskusteltiin, millaisia asiakirjoja he päivittäin käsittelevät, kuinka niitä tulisi säilöä sekä hävittää. Myös tuotannon puolella liikkuvilta, tuntemattomilta henkilöiltä, tulisi kysyä, millä asialla he ovat.

Kuvio (kuvio 8) kertoo tuotannon työntekijöiden palautteen tietoturvakoulutuksista.



KUVIO 8. Yhteenveto tuotannon työntekijöiden koulutuksista (n=77)

Hyödyllisimmäksi koettiin salassapito - ja vaitiolovelvollisuus. On erittäin positiivista huomata, että kyseinen osa-alue koettiin hyödylliseksi. Yritykselle on erittäin tärkeää, että mm. liikesalaisuudet sekä muut yrityksen salassa pidettävät tiedot eivät leviä yrityksen ulkopuolelle. Lama-aikana ihmiset ovat yhä uteliaampia yrityksen taloudellisesta tilanteesta, joten tärkeää, että julkistamaton tieto ei leviä. Näin vältetään erilaisten huhu-puheiden liikkeelle lähtöä. Vähiten hyödylliseksi koettiin Internetin käyttö. Tämä johtuu siitä, että kaikilta heidän työkoneiltaan ei ole pääsyä Internetiin.

5 POHDINTA

5.1 Yleistä työn merkityksestä

Tietoturvasta keskustellessa yhä useammin tulee esille tietokoneisiin liittyvät tietoturva-asiat, lähinnä virustorjuntaohjelmat. Harvemmin puhutaan tietoturvan muista osa-alueista, kuten laitteistojen turvallisuudesta ja uhkista. Yrityksissä työ tapahtuu pääsääntöisesti tietokoneiden avulla, joten on luonnollista, että tietoturva-käsite liitetään yhä useammin tietokoneisiin. Myös ulkopuolelta tuleva mainonta tietoturvan osalta on lähinnä tietoturvaohjelmiin liittyvää. Opinnäytetyön tietoturvamateriaali muodostui suurilta osin tietokoneen kanssa toimimiseen, koska lähes kaikki tieto siirretään sen kautta. Kuitenkin materiaalissa haluttiin myös tuoda esille muita tietoturvaan liittyviä osa-alueita, jotta jokainen ymmärtäisi, mitä kaikkea tietoturvaan liittyy. Yrityksen tietohallinnon osasto huolehtii teknisesti tietoturvasta tietoturvaohjelmilla, varmuuskopioilla ja suojatuilla yhteyksillä. Ohjelmien ja erilaisten suojauksien ylläpitäjät eivät kuitenkaan voi varmistaa kokonaan tiedon säilymistä. Esimerkiksi, jos työntekijä lajittelee luottamukselliset asiakirjat väärin ja tieto pääse vääriin käsiin sitä kautta tai tietokone on jätetty lukitsematta ja ulkopuolinen pääsee yrityksen tiedostoihin käsiksi suoraan tietokoneelta. Näin jokaisen työntekijän päivittäinen toimiminen vaikuttaa tiedon säilymiseen.

Opinnäytetyötä tehdessä tutustuttiin myös tietoturvatutkimuksiin. Tutkimustulokset osoittivat, että tietoturvakoulutukselle on tarvetta yrityksissä. Tietoturvaa tulisi myös kehittää erilaisilla suunnitelmilla esimerkiksi miten voidaan välttyä riskien toteutumiselta tai miten toimitaan, jos riski toteutuu. Tutkimuksissa nousi esille myös tietoturvan tekninen puoli. Yritykset luottavat tietoturvan teknisiin ratkaisuihin ja muut osa-alueet jäävät usein ilman huomiota. Tulokset tukevat hyvin tämän opinnäytetyön tarkoitusta eli tietoturvatietoisuuden lisäämistä organisaation sisällä.

5.2 Yhteenveto käyttäjäohjeista ja tietoturvakoulutuksista

Materiaalista tehtiin perustietoturvapaketti, jossa otettiin huomioon myös erilaisissa työtehtävissä työskentelevien tietoturvatarpeita. Esimerkiksi kaikilla ei ole työn puolesta matkapuhelinta ja kaikki eivät joudu matkustamaan, mutta käyttäjäohjeissa oli mainittu kyseisiin asioihin liittyviä tietoturvaohjeita. Yrityksessä ei ole aikai-

semmin pidetty vastaavanlaisia koulutuksia, joten ihan perusasioiden kertaus sekä uusien asioiden esiin tuominen oli paikallaan. Materiaali haluttiin pitää myös yksinkertaisena ymmärtää, jotta tietoturvaan liittyvät asiat tulevat oikein ymmärretyksi. Tietoturvan käyttäjäohjeet tarjoavat myös uudelle työntekijälle peruskertauksen sekä tietoiskun tietoturva-asioista. Tietoturva-asioiden huomioiminen luo myös vastuuntuntoisen kuvan yrityksestä. Käyttäjäohje antaa myös lisätietoa yrityksessä käytössä olevista ohjelmista sekä kuinka niitä käytetään tai kuinka salasana vaihdetaan. Toimeksiantaja ei halunnut henkilökunnalle järjestettävän ennakkokyselyä tietoturva-asioista vaan, materiaalia muokattiin koulutuksissa esiin tulleiden asioiden mukaan. Näin materiaali pystyttiin pitämään kaikkia palvelevana.

Käyttäjäohjeilla pyritään välttämään tahattomia ja tahallisia tietoturvarikkomuksia. Ohjeiden avulla yritys myös varmistaa, että tietoturvarikkomuksen kohdalla työntekijä ei voi vedota tietämättömyyteen. Tietoturvan käyttäjäohje on myös koulutuksien kautta työntekijöiden tiedossa. Jos ei ole osallistunut koulutukseen, on tietoturvaan liittyvä materiaali saatavilla dokumentinhallintajärjestelmässä sekä ohjeisiin on lähetetty jokaiselle työntekijälle linkki.

Työntekijöille lähetetyssä kutsussa (liite 5) kerrottiin jo koulutuksen perustarkoitus eli lisätä henkilökunnan tietoturvatietoutta sekä tietoturvallista käyttäytymistä päivittäisessä työssään. Koulutuksien palautteiden mukaan, koulutus oli tarpeellinen eli se koettiin hyödylliseksi. Iisalmessa työskentelevien koulutusten kesken ei ollut merkittäviä eroja. Koulutuskohtaiset keskiarvot koulutuksen kokonaisarvosanasta olivat 2,8–3,1 välillä. Arviointi tapahtui asteikolla 1–4 (1=välttävä, 2=tyydyttävä, 3= hyvä ja 4=erinomainen).

Koulutuksien aikana syntyneet keskustelut osoittivat, että työntekijät joutuvat miettimään työssään tietoturva-asioita. Keskustelun syntyminen toi myös erilaisia näkökulmia sekä käytännön esimerkkejä tietoturva-asioihin. Koulutuksien tärkeimmiksi asioiksi nousivat salassapito- ja vaitiolovelvollisuus sekä sähköposti. Koulutettavien joukossa oli myös yksi uusi työntekijä. Palautteita ei nimetty, joten hänen henkilökohtaista arviotaan koulutuksesta ei ole saatavilla. Koulutusryhmä, jossa hän oli, arvioi koulutuksen eri osa-alueita 3,0–3,8 keskiarvoilla. Tämän perusteella koulutus on ollut hyödyllinen.

Tuotannon työntekijöitä oli vaikeampi saada keskustelemaan tietoturvaan liittyvistä asioista verrattuna toimihenkilöihin. Koulutuksien tärkeimmäksi asiaksi nousi salassapito- ja vaitiolovelvollisuus, jonka keskiarvot olivat 3,0–3,6 välillä. Internetin käyttöön liittyvät ohjeistukset koettiin vähiten tärkeäksi. Koulutuksien keskiarvot vaihtelivat 2,7–2,9 välillä. Tähän vaikuttaa, että kaikissa tuotannon tietokoneissa ei ole pääsyä Internetiin ja työntekijöiden työtehtävät eivät vaadi Internet-yhteyttä. Kolmen koulutuksen kokonaisarvosanan keskiarvot olivat 3,2–3,4 välillä.

Englanninkielisten koulutusten haasteellisuus oli sen toteuttaminen WebEx-puhelinkonferenssiohjelman kautta, joka nousi myös esille palautteissa.. Koulutuksen seuraaminen oli hankalaa, joka osaksi johtui puhelinyhteydestä. Koulutuksen toteutus kasvotusten olisi ollut parempi vaihtoehto. Kokonaisarvosanan keskiarvot vaihtelivat kahden ja kolmen välillä.

Koulutus oli myös pakollinen, jotta saadaan mahdollisimman moni ottamaan osaa koulutukseen sekä haluttiin painottaa tietoturvakoulutuksen tärkeyttä. Tietoturva koulutusaiheena ei ole niitä mielenkiintoisimpia koulutusaiheita, joten osanottajat olisivat voineet jäädä vähäisiksi ilman koulutuspakkoa. Tietoturvaa ei välttämättä mielletä tärkeäksi.

5.3 Itsearviointi ja palaute

Kouluttajana toimiminen on haasteellinen tehtävä. Koulutusta suunniteltaessa tulee ottaa huomioon erilaisia tekijöitä mm. kuinka saada koulutettavat kiinnostumaan aiheesta sekä myös keskustelemaan. On mietittävä, minkä kokoiset koulutusryhmät ovat sopivat sekä kuinka pitkä koulutuksen tulee olla. Myös koulutuksen palautelomakkeen suunnittelu on tärkeä osa, jotta nähdään kuinka koulutus on sujunut ja miten koulutusta voi parantaa. Palautelomakkeessa on tärkeä miettiä arviointiasteikko, jotta palautteesta saadaan totuudenmukainen. Kouluttajaa arvioitiin esiintymisen ja asiantuntevuuden alueilta. Arviointi tapahtui myös asteikolla 1–4 (1=välttävä, 2=tyydyttävä, 3= hyvä ja 4=erinomainen), samoin kuin koulutuksien osa-alueiden arviointi. Esiintymisen sekä asiantuntevuuden arvosanojen keskiarvot olivat lähes samat eli yli kolmen. Koulutettavien mukaan kouluttaja on onnistunut omassa roolissaan.

Tuotoksen englanninkielisyys toi myös oman haasteensa. Englanninkielinen käyttäjäohjeisto ja tietoturvakoulutus lisäsivät englanninkielen suullista ja kirjallista osaamista. Työn kautta opin paljon uusia sanoja, joista on hyötyä tulevaisuudessa. Oikeiden termien löytäminen ja lauseiden muodostaminen lisäsivät työn haasteellisuutta. Kouluttaminen englanninkielellä oli aivan uusi kokemus. Testikoulutus olisi ollut myös tarpeen englanninkielisiä koulutuksia varten, joka ajanpuutteen takia jäi pitämättä. Sanojen ääntäminen ja puhuminen puhelimen kautta tuottivat ensimmäisessä koulutuksessa ongelmia. Aluksi ajatus kouluttamisesta puhelinkonferenssiohjelman kautta vaikutti helpolta, kun koulutettavat eivät ole konkreettisesti edessä. Ensimmäisen englanninkielisen koulutuksen jälkeen kuitenkin tuntui siltä, että on helpompi pitää koulutusta, kun koulutettavat ovat konkreettisesti edessä.

5.4 Kehitysideat

Tietoturvan käyttäjäohjeet on hyvä päivittää samassa yhteydessä, kun tietoturvapolitiikka päivitetään. Käyttäjäohjeet on kuitenkin hyvä käydä läpi vuosittain ja päivittää tarpeen mukaan. Koulutustilaisuuksia olisi myös hyvä järjestää jatkossa esimerkiksi kolmen vuoden välein. Materiaalin painottaminen uuden työntekijän tullessa on myös tärkeää, joten muiden asioiden perehdyttämisen yhteydessä neuvoa lukemaan tietoturvan käyttäjäohjeet yrityksen dokumenttienhallintajärjestelmästä.

Tietoturva on aiheeltaan laaja ja siitä löytyy paljon huomioitavia sekä kehitettäviä osa-alueita yrityksissä. Perusohjeistuksen pohjalta on hyvä miettiä osastokohtaisia tietoturva-asioita. Kuinka esimerkiksi taloushallinnon osastolla käsitellään erilaisia asiakirjoja ja mitkä asiat ovat arkaluontoisia.

Koulutuksen toteutusta voisi kehittää niin, että koulutus olisi jokaiselle osastolle erilainen. Koulutuksen sisällössä painottuisi osastolla huomioitavat tietoturva-asiat, koska jokaisella osastolla työtehtävät ovat erilaisia. Työtehtävien kautta tietoturvaan liittyvät asiat painottuvat erilailla. Osaston kesken on hyvä käydä läpi, minkälaisia asioita voi mainita esimerkiksi yhteistyökumppanille tai toisen osaston henkilölle.

LÄHTEET

Gollman, D. 1999. Computer Security. Englanti: John Wiley & Sons Ltd.

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Porvoo: WS Bookwell.

Helsilä, M. 2002. Käytännön henkilöstötyö. Tampere: Tammer-Paino Oy.

Juholin, E. 2008. Viestinnän vallankumous - Löydä uusi työyhteisöviestintä. Juva: WS Bookwell Oy.

Järvinen, A., Koivisto, T. & Poikela, E. 2000. Oppiminen työssä ja työyhteisössä. Juva: WS Bookwell Oy.

Järvinen, P. 2002. Tietoturva & Yksityisyys. Porvoo: WS Bookwell Oy.

Kerttula, E. 1999. Tietoverkkojen tietoturva. Helsinki: Edita.

Kleemola, M. & Tervo-Pellikka, R. 1998. Tietosuoja. Jyväskylä: Gummerus Kirjapaino Oy.

Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Helsinki: Edita Publishing Oy.

Van Bon, J., Kemmerling, G. & Pondman, D. 2002. IT Service Management - An Introduction. Australia: Van Haren Publishing.

Whitman, M. & Mattord, H. 2003. Principles of Information Security. Boston: Thomson Course Technology.

Painamattomat lähteet

A Frost & Sullivan White Paper. 2008. The (ISC)² Global Information Security Workforce Study. [Viitattu 23.1.2009] Saatavissa: https://www.isc2.org/uploadedFiles/Industry_Resources/2008_Global_WF_Study.pdf

Ernst & Young. 2008. Moving beyond compliance - Ernst & Young's 2008 Global Information Security Survey. [Viitattu: 29.1.2009] Saatavissa: http://www.ey.com/Publication/vwLUAssets/2008_Global_Information_Security_Survey/$file/2008GlobalInformationSecuritySurvey.pdf

Hallinnollinen näkökulma. 2002. TTKK. [Viitattu: 22.9.2009] Saatavissa: http://www.cs.tut.fi/kurssit/8306000/ha.html

Kajava, J. 2001. Johdatus tietoturvaan: perusluonne ja tasot. Oulun Yliopisto. [Viitattu: 30.1.2009] Saatavissa: http://www.ulapland.fi/files/20040114154859.pdf

Kyselytutkimus: Tietoturvan uhat tiedostettu. 2001. Digitoday. [Viitattu: 9.8.2009] Saatavissa: http://m.digitoday.fi/?page=showSingleNews&newsID=20019467

Tietoturvallisuuden hallinta suomalaisissa organisaatioissa 2007. 2007. Nixu Oy. [Viitattu: 23.1.2009] Saatavissa: http://www.nixu.com/news/tietoturvatutkimus2007/Tietoturvallisuuden_hallinta_suomalaisissa_organisaatioissa_2007.pdf

Omat työntekijät suurin tietoturvauhka. 2008. IT-Viikko. [Viitattu: 9.8.2009] Saatavissa: http://m.itviikko.fi/?page=showSingleNews&newsID=200826642

Sanasto. 2008. TIEKE Tietoyhteiskunnan kehittämiskeskus ry. [Viitattu: 22.9.2009] Saatavissa: http://www.tieke.fi/julkaisut/oppaat_yrityksille/sahkoisen_kaupankaynnin_aapinen/sanasto/

Valtion tietoturvasanasto VAHTI 8/2008. 2008. Valtiovarainministeriö. [Viitattu: 22.9.2009] Saatavissa: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20081211Valtio/Vahti_8_NETTI%2b_KANNET.pdf

Yrityksen tietoturvaopas: Toimiva tietoturva - avainkysymykset. 2009. Tietoturvaopas. [Viitattu: 22.9.2009] Saatavissa: http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/avainkysymykset.html

Yrityksen tietoturvaopas: Panosta henkilöstön osaamiseen. 2009. Tietoturvaopas. [Viitattu: 30.1.2009] Saatavissa: http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/henk_osaaminen.html

LIITE 3

TAULUKKO RISKEISTÄ JA MAHDOLLISISTA UHKISTA

RISKI/ UHKA	VARAUTUMI-NEN	SEURAUS	TOIMEN-PIDE	OTA YHTEYS
Henkilöstö - tietovuoto - luvaton järjestelmään tunkeutuminen - varkaus	Koulutus / Käyttäjäohjeet sekä niiden päivittäminen Käyttäjätunnuksien / -oikeuksien päättäminen	Tiedon pääseminen julkisuuteen Järjestelmähäiriö	Varoitus/ työsuhteen päättäminen Järjestelmän häiriön/vian etsiminen ja korjaaminen	Lähin esimies Service Desk IT Osasto
Virus/haitta-ohjelmat Tietoturva-ohjelmiston pettäminen Hakkerit / Krakkerit	Tietoturvaohjelmat Varmuuskopiointi Henkilöstön ohjeistus, tietoturvaohjelmat	Järjestelmän kaatuminen Tietovuoto	Uudelleen asennus varmuuskopi-oista	Service Desk IT Osasto
Varkaus Tulipalo / Lämpö-tilan liiallinen kohoaminen Vesivahinko/ Kosteus Sähköhäiriö	Kulkulupa, ovien lukitse-minen Paloturvallisuus-ohjeet Hälytyslaitteet Laitteet pois lattialta, ei vesiputkien lähelle laitteita Varavirta, säännöllinen varavirran toimivuustarkistus	Omaisuuden katoaminen Tärkeiden tietojen häviäminen Laitteiden rikkoutuminen, tulipalo Laiterikko, tulipalo	Rikosilmoitus Vian etsintä ja korjaus Avun hälyttäminen	Lähin esimies Poliisi IT Osasto Hätäkeskus IT Osasto Palokunta Lähin esimies Hätäkeskus

Hätätilanteissa soita aina hätäkeskukseen, 112.

Paloturvallisuusohjeet löytyvät ilmoitustaululta.

Tietoturvakoulutus

Arvioi osa-aluiden sisällön hyödyllisyyttä asteikolla 4 (erittäin hyödyllinen) - 1(ei hyödyllinen)

Koulutuksen osa-alueet:	4	3	2	1
• Salassapitovelvollisuus	☐	☐	☐	☐
• Käyttäjätunnukset ja -oikeudet	☐	☐	☐	☐
• Salasana	☐	☐	☐	☐
• Internetin käyttö	☐	☐	☐	☐
• Sähköposti	☐	☐	☐	☐
• Tiedon siirtäminen ja matkapuhelimen käyttö	☐	☐	☐	☐
• Hyvä tietää ja muistaa	☐	☐	☐	☐

Arvioi kouluttajaa 4 (erinomainen) - 1 (tyydyttävä)

• Esiintyminen	☐	☐	☐	☐
• Asiantuntevuus	☐	☐	☐	☐

Anna koulutukselle yleisarvosana väliltä 1-4. (4=erinomainen, 1=välttävä)

Laita kolme (3) tietoturvaan liittyvää asiaa oman työsi kannalta tärkeysjärjestykseen.

Vapaita kommentteja koulutuksesta, tarvittaessa jatka kääntöpuolelle.

Information Security Training

Assess utility of the training content, scale 4 (extremely useful) - 1 (non-useful)

Content of the training	4	3	2	1
• Introduction	☐	☐	☐	☐
• Confidentiality	☐	☐	☐	☐
• User names and rights	☐	☐	☐	☐
• Password	☐	☐	☐	☐
• Use of the Internet	☐	☐	☐	☐
• E-mail	☐	☐	☐	☐
• Transfer of the information and use of the mobile phone	☐	☐	☐	☐
• Good to know and good to remember	☐	☐	☐	☐

Give a general grade to training, scale 1 - 4. (4=excellent, 1=passable)

List three (3) things about information security, which are the most important for your work.

Free comments about training.

Tietoturvakoulutus

Arvioi osa-aluiden sisällön hyödyllisyyttä asteikolla 4 (erittäin hyödyllinen) - 1(ei hyödyllinen)

Koulutuksen osa-alueet:	4	3	2	1
• Salassapitovelvollisuus	☐	☐	☐	☐
• Käyttäjätunnukset ja -oikeudet	☐	☐	☐	☐
• Salasana	☐	☐	☐	☐
• Internetin käyttö	☐	☐	☐	☐
• Sähköposti	☐	☐	☐	☐
• Hyvä tietää ja muistaa	☐	☐	☐	☐

Arvioi kouluttajaa 4 (erinomainen) - 1 (tyydyttävä)

• Esiintyminen	☐	☐	☐	☐
• Asiantuntevuus	☐	☐	☐	☐

Anna koulutukselle yleisarvosana väliltä 1-4. (4=erinomainen, 1=välttävä)

Laita kolme (3) tietoturvaan liittyvää asiaa oman työsi kannalta tärkeysjärjestykseen.

Vapaita kommentteja koulutuksesta, tarvittaessa jatka kääntöpuolelle.

LIITE 5

”Hei!

Normet Groupin tietohallinto järjestää toukokuussa 2009 henkilöstölle suunnatun tietoturvakoulutuksen.

Koulutuksen tarkoituksena on lisätä henkilökunnan tietoturvatietoutta ja tietoturvallista käyttäytymistä päivittäisessä työssä.
Koulutus on pakollinen.

Liitteenä on ryhmäjako-taulukko. Jos aika ei sinulle käy, ota yhteys Jonna Kauppiseen ja sovi koulutuksesta toisen ryhmän mukana.

Jussi Ahomaa
Global IT Manager
Normet Group
mob.+358 40 483 4611
fixed +358 17 832 4266
jussi.ahomaa@normet.fi”

Jonna Kauppinen
Trainee
jonna.kauppinen@normet.fi

LIITE 5

Hi all,

Normet Group Oy arranges Information Security training for personnel during May-June 2009. For personnel working outside Finland the training will be arranged using teleconferencing system (WebEx). Training language is English.

The goal of the training is to increase information security awareness and behaviour of the personnel in daily work.

Inform Jonna Kauppinen (jonna.kauppinen@normet.fi) **which date and time You will be participating, and Jonna will send participating instructions.**

Here are the dates and times for training:

Wed 20 May 8.00-10.00 am
Wed 20 May 15.00-17.00 pm

Wed 27 May 8.00-10.00 am
Wed 27 May 15.00-17.00 pm

Tue 16 June 8.00-10.00 am
Tue 16 June 15.00-17.00 pm

Times are announced as Finnish time (GMT +02:00).

With Best regards,

Jussi Ahomaa
Global IT Manager
Normet Group
mob.+358 40 483 4611
fixed +358 17 832 4266
jussi.ahomaa@normet.fi

Jonna Kauppinen
Trainee
jonna.kauppinen@normet.fi