Kemi Tornion ammattikorkeakoulu

Tietoturvakartoitus ISO/IEC 27001-standardin mukaan

Hannele Saari

Kaupan ja kulttuurin toimialan opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
Tradenomi

TORNIO 2013

TIIVISTELMÄ

KEMI-TORNION AMMATTIKORKEAKOULU, Kaupan ja kulttuurin toimiala

Koulutusohjelma:	Tietojenkäsittelyn koulutusohjelma
Opinnäytetyön tekijä(t):	Hannele Saari
Opinnäytetyön nimi:	Tietoturvakartoitus ISO/IEC 27001-standardin mukaan
Sivuja (joista liitesivuja):	42 (3)
Päiväys:	30.4.2013
Opinnäytetyön ohjaaja(t):	Juha Meriläinen

Opinnäytetyössä perehdytään ISO/IEC 27001-standardin tietoturvavaatimuksiin. Haetaan vastausta kysymykseen, mikä on esimerkkiyrityksen henkilöstön tietoturva-osaamisen taso tällä hetkellä. Tarkoituksena on tutkia, tarvitaanko lisäkoulutusta ja pohtia osaamisen ylläpitoon erilaisia vaihtoehtoja.

Teoreettisena viitekehyksenä on ISO/IEC 27001-standardi ja siihen liittyen informaatioteknologia, turvallisuus, tietoturvallisuuden hallintajärjestelmät ja vaatimukset. Tutkimuksessa on käyty läpi tietoturvan hallintajärjestelmään liittyviä asioita, termejä ja määritelmiä.

Opinnäytetyössä kartoitetaan esimerkkiyrityksen henkilöstön tietoturvaosaamista kyselyn avulla. Kyselyn analysoinnin jälkeen käydään läpi riskienhallintaa, käytännön ohjeita ja tietoturvaan liittyvää lainsäädäntöä.

Kyselyn tuloksena selvisi, että tietoturva-asioissa ei ole ollut ongelmia, mutta koska osalla esimerkkiyrityksen työntekijöistä oli jonkin verran epätietoisuutta tietoturva-politiikan sisällöstä, kannattaa ottaa tavaksi kerrata tietoturva-asioita aina säännöllisin väliajoin.

Asiasanat: ISO/IEC 27001-standardi, tietoturvallisuus, tietoturvallisuuden hallintajärjestelmä, riskianalyysi.

ABSTRACT

KEMI-TORNIO UNIVERSITY OF APPLIED SCIENCES, Business and culture

Degree programme:	Business information technology bachelor´s thesis
Author(s):	Hannele Saari
Thesis title:	Information security survey by ISO/IEC 27001 standard
Pages (of which appendixes):	43 (2)
Date:	23.4.2013
Thesis instructor(s):	Juha Meriläinen

This thesis studies the requirements of the ISO/IEC 27001 standard. The objective of this study is to examine the personnel's current level knowledge in terms of information security. The objective is to find out if further training is needed and to consider the options for maintaining know-how.

The theoretical framework is the ISO/IEC 27001 standard and information technology, security, information security management system and requirements. This study reviews issues, terms and expression of the information security management.

The thesis examines employees' current knowledge level of information security issues in the case organization through a questionnaire survey. After analyzing the questionnaires, the thesis discusses risk management, presents practical instructions, and deals with the current legislation concerning information security.

The results of the questionnaire survey indicate that there have been no problems with information security so far. There have been some uncertainties about the content of the information security policy, and therefore it would be recommendable to take a habit to raise information security policy for general discussion in the case organization once in a while.

Keywords: ISO/IEC 27001-standard, Information Security, Information Security Management System, risk analysis.

SISÄLLYS

1 JOHDANTO

Tämän opinnäytetyön aiheena on perehtyä ISO/IEC 27001-standardiin, tehdä tietoturvakartoitus pk-yritykselle ja tutkia tietoturvallisuuden hallintajärjestelmän toteuttamista ja kouluttamista henkilökunnalle.

Tässä opinnäytetyössä lähdetään liikkeelle tietoturvakyselyllä, joka osoitetaan koko esimerkkiyrityksen henkilökunnalle. Yleensä tietoturva-asiat koulutetaan työsuhteen alkaessa muun perehdytyksen mukana. Koska siinä vaiheessa on paljon uusia työsopimukseen liittyviä asioita, uusia henkilöitä ja uusia työtehtäviä opeteltavana, tietoturva-asiat jäävät usein muiden asioiden vuoksi taka-alalle. Työtoverit tulevat tutuksi, työohjeet opetellaan ulkoa, mutta tietoturva-asiat jäävät yrityksen verkon yhteisille sivuille odottamaan omatoimista kertausta, jota ei ehkä koskaan tulekaan.

Esimerkkiyrityksenä opinnäytetyössäni on 17 henkilöä työllistävä ICT-alan yritys Suomessa. Tarkoituksena on tehdä tämän kokoiselle yritykselle sopiva tietoturvakartoitus ISO/IEC 27001-standardin mukaisesti, jotta yritys voisi myöhemmin harkita, lähteekö hakemaan ISO/IEC 27001-standardia. Lisäksi etsitään uusia tapoja pitää yllä henkilökunnan tietoturvaosaamista. Tietoturva koskee aina koko yrityksen henkilöstöä, vastuuta ei voi siirtää pelkästään hallinnolle tai tietoturvasta vastaavalle henkilölle.

Jotta saavutetaan opinnäytetyön tavoitteet, tulee löytää vastaukset seuraaviin kysymyksiin:

- Miten tietoturva liittyy liiketoimintaan?
- Onko tietoturvavaatimukset ymmärretty?
- Ovatko tietoturvatavoitteet ja tietoturvapolitiikka määritetty?
- Mikä on henkilöstön tietoturvaosaamisen taso tällä hetkellä?

Teoreettisena viitekehyksenä on ISO/IEC 27001-standardi ja siihen liittyen informaatioteknologia, turvallisuus, tietoturvallisuuden hallintajärjestelmät ja vaatimukset. Olen myös perehtynyt oppimateriaalin lisäksi tietoturvakirjallisuuteen. Näkökulma, jonka haluan tuoda tässä tutkimuksessa esiin, on kirjailija Petteri Järvisen: ”Odota odottamatonta” (Järvinen 2012, 25).

Opinnäytetyöhön kuuluu teoria- ja tutkimusosuus. Teoriaosuudessa käydään läpi tietoturvapolitiikkaa, riskienhallintaa ja sitä, miten olennaista on tietoturva liiketoiminnan kannalta. Tässä vaiheessa käydään läpi myös standardin sisältöä, prosessikuvauksia ja käsitteiden määrittelyä. Tutkimusosassa kartoitetaan henkilöstön tietoturvaosaamista ja vastausten analysointia sekä etsitään menetelmiä, joiden avulla tietoturvaosaaminen saadaan luontevasti mukaan jokapäiväiseen työhön.

Tutkimusmenetelmä on laadullinen eli kvalitatiivinen. Opinnäytetyössä käytetään aineistoanalyysejä, joiden avulla perehdytään teoreettiseen viitekehykseen ja kyselylomakkeita, joita käytetään henkilöstön tietoturvatietämyksen kartoittamiseen sekä havainnointia esimerkkiyrityksen työpisteissä.

2 TIETOTURVALLISUUSPOLITIIKKA

2.1 Tietoturva ja -suoja

Tämän opinnäytteen tavoitteena on pohtia, miksi yrityksellä pitäisi olla tietoturvallisuuspolitiikka. Kyllähän kaikki tietävät, että työpaikan asioista ei puhuta vieraille, ei tutuille eikä entisille työtovereille. Jokaisen tulisi miettiä, miten vastaa, kun entinen työtoveri tulee vastaan kaupassa ja kyselee kuulumisia. Pitäisi aina harkita, millä tarkkuudella voi kertoa nykyisestä työpaikasta. Kannattaa myös harkita sitä, voiko kertoa, ovatko kaikki entiset työtoverit vielä töissä.

Tällaisessa tapauksessa tulisi olla jo selkeästi mielessä oman yrityksen tietoturvakäytäntö. Työpaikasta riippuu, mitä asioita voi kertoa ulkopuolisille. Jos ei ole varma, on parasta antaa ympäripyöreä vastaus ja vaihtaa puheenaihetta. Yrityksen tietoturvapolitiikka voi määritellä, mihin kysymyksiin voit vastata.

Tietoturva ja tietosuoja ovat eri asioita. Tietosuoja eli yksityisyyden suoja perustuu lakiin, käytäntöön ja hyviin tapoihin. Sillä tarkoitetaan ihmisten henkilötietojen ja henkilökohtaiseen toimintaa liittyvien tietojen keräämisen ja käsittelyn rajoittamista siten, ettei henkilön yksityisyys vaarannu. Tietoturva on kokonaisuus, johon liittyvät tietokoneiden ja muiden tiedonkäsittelylaitteiden fyysinen turvallisuus sekä tiedonkäsittelijöiden osaaminen. Tähän kokonaisuuteen kuuluu olennaisesti myös dokumenttien ja viestien turvaaminen. (Tirronen 2003, hakupäivä 3.4.2013.)

Tietoturvallisuus on oleellinen osa yrityksen toiminnan ja palvelun laatua sekä päivittäistä tietojen käsittelyä. On pystyttävä siihen, että tietoturvallisuuden perusvaatimukset säilyvät. Näitä ovat saatavuus, eheys ja luottamuksellisuus. Tietojen turvaaminen edellyttää jatkuvaa seurantaa, suunnittelua, varautumista erilaisiin tilanteisiin sekä sovittujen käytäntöjen noudattamista, ohjeiden ajanmukaisuutta ja koulutusta. (Laaksonen, Nevasalo & Tomula 2006, 58.)

2.2 Julkinen tietoturvapolitiikka

Yrityksen tulee laatia julkinen tietoturvapolitiikka eli määritellä tietoturvapolitiikka-asiakirja ja sen soveltamisohjeet. Vastuu yrityksen toimivuudesta on aina ylimmällä johdolla ja johdon on osattava arvioida oman yrityksensä kehittyminen ja tietoturva-edellytykset. Ensimmäisenä tulisi pohtia sitä, miten liiketoiminnan tavoitteet ja tietoturvatavoitteet voidaan yhtenäistää niin, että nämä tavoitteet ovat linjassa organisaation muitten tavoitteiden kanssa. (Laaksonen ym. 2006, 58.)

Liiketoiminnan ja tietoturvallisuuden tavoitteiden harmonisointi vaikuttaa mm. resurssien jakamiseen, toiminnan mittaamiseen sekä seurantaan. Esimerkiksi resurssien käyttöä voidaan tehostaa siten, että laajennetaan laatuorganisaation tehtäväkenttää tietoturva-asioihin ja yhdistetään muihin prosesseihin tietoturvallisuuden elementtejä ja kontrolleja. Tietoturvaan ei pidä panostaa niin paljon, että sen kustannukset vievät mahdollisuuden yrityksen tuloksen tekemisestä. Yrityksen johto hyväksyy tietoturvapolitiikan ja se annetaan tiedoksi kaikille työntekijöille. Myös lainsäädäntö tulee muistaa tietoturvapolitiikkaa laadittaessa. (Laaksonen ym. 2006, 118.)

Tietojärjestelmiä hankittaessa on vaikeaa hinnoitella ja mitata tarkkaa tietoturvan osuutta. Hinnoittelua ja mittaamista vaikeuttaa se, että uhkien määrää ja vakavuutta ei etukäteen tarkkaan tiedetä. Hankinnassa on kuitenkin tärkeää se, että tietoturvaratkaisut ovat helppokäyttöisiä. Monesti tietoturvasta vastaavat henkilöt ajattelevat, että tietoturvaratkaisujen käyttö on itsestään selvää, mutta näin ei ole. Kannattaa käyttää tietoturvaratkaisuista sitä kieltä, mitä johto ja muu henkilökunta käyttää. (Lagus 2013, 14.)

Yrityksen pohtiessa sitä, kuinka laaja järjestelmä tulee rakentaa tietoturvallisuuden hallinnointiin, tulisi hakea vastaukset seuraaviin kysymyksiin:

- Minkälaista tietoa yrityksessä käsitellään? Voiko siitä joku hyötyä taloudellisesti?
- Vaatiiko tiedon tuottamisen suuria taloudellisia tai muunlaisia ponnisteluja? Kuinka helposti sama tieto tuotetaan uudelleen tarvittaessa? Onko siitä sen jälkeen enää mitään hyötyä?
- Kuka voisi olla kiinnostunut yrityksen tiedoista? Miten tietoon pyritään käsiksi?

- Miten tietoja voidaan viedä yrityksestä ulos? Millä tavoin se tapahtuisi?
- Kuinka laajaa ja monimuotoista on organisaation toiminta ja johtamisjärjestelmä?
- Voidaanko tietoturvajohtaminen yhdistää nykyiseen johtamisjärjestelmään?
- Miten yrityksessä vastataan ulkopuolelta tuleviin tietoturvavaatimuksiin?
- Onko yrityksellä tietoa velvoittavasta yleisestä lainsäädännöstä tai erityisestä säännöstelystä, joka koskee liiketoimintaa ja sen tietoturvavelvoitteita tai -oikeuksia? (Laaksonen ym. 2006, 118,119.)

2.3 Jatkuvuus- ja toipumissuunnittelu

Tietoturvaa uhkaavia tilanteita voi olla monenlaisia ja ne voivat johtua monista eri syistä. Tästä syystä nämä uhkaavat ja odottamattomat tilanteet on selvitettävä, jotta ne voidaan estää tulevaisuudessa. Odottamattomissa tilanteissa pitäisi saada työt jatkumaan mahdollisimman nopeasti, tarvittaessa muilla ratkaisuilla, mikäli tietokonejärjestelmät lakkaavat toimimasta. Jos tilanne on sellainen, että osa koneista ja järjestelmistä toimii, voidaan näitä tilanteita varten varautua myös varalaitteilla ja -järjestelmillä. Siksi yrityksen tulisi tietoturvapolitiikkaa laatiessa huomioida yrityksen jatkuvuussuunnittelu sekä toipumissuunnittelu.

Jatkuvuussuunnittelun tarkoitus on taata toimintojen jatkuminen normaalioloissa, häiriötilanteissa, poikkeustilanteissa ja poikkeusolojen aikana. Jatkuvuussuunnittelu on prosessi jonka tavoitteena on ennalta varautua mahdollisiin ongelmatilanteisiin. (Iivari & Laaksonen 2009, 227.)

Jatkuvuussuunnitelman käyttöönottoa harjoitellaan kouluttautumalla koko henkilökunnan kanssa ja on tärkeää päivittää ja ylläpitää suunnitelmaa säännöllisin väliajoin. Suunnitelmassa tunnistetaan liiketoiminnan kriittiset prosessit ja niihin liittyvät riippuvuudet. Pitää myös varmistaa työntekijöiden turvallisuus: pelastus, hälytys, suojaaminen ja turvaaminen. Liiketoiminnan palauttaminen normaaliksi pitäisi tapahtua mahdollisimman pian. (Marsh, hakupäivä 1.4.2013.)

Toipumissuunnittelussa kuvataan toimenpiteet vahingon jälkeen, jotta voidaan palauttaa normaali tilanne mahdollisimman pian ja pitää aiheutuneet vahingot mahdollisimman

pienenä. Toipumissuunnitelmaa voidaan tarvita silloin, kun olot ovat sekavat, resursseja ei ole riittävästi ja eikä välttämättä ole vielä edes selvillä, minkälainen on kokonaistilanne. Tällaisia häiriöitä voivat olla mm. pitkittynyt lakko, laaja mellakointi, luonnon aiheuttama poikkeustila, kuten tulva tai hurrikaani, tulipalo, keskeisen järjestelmän äkillinen tuhoutuminen tai jokin muu yritystä koskeva merkittävä ongelma. (Laaksonen ym. 2006, 234.)

2.4 Tiedon elinkaari ja luokittelu

Tiedon tuottajan tai tuojan tulisi vastata tiedon elinkaaresta, eli päättää, kuinka kauan tieto on käyttökelpoista. Ensin tieto tulee taloon, sitten se jaetaan käyttöä varten. Lopuksi tieto arkistoidaan tai tuhotaan. Tietoa luokitellaan siksi, että kaikkea ei tarvitsisi suojata. Luokittelussa voidaan käyttää perusjakoa kahteen, joko sisäiseen tai ulkoiseen tietoon. Sisäistä tietoa on se, jota käyttävät vain ne, jotka tarvitsevat sitä työssään, sekä tieto, joka on vapaasti yrityksen työntekijöiden käytössä. Julkista tietoa voi luovuttaa yrityksen ulkopuolelle ja se on sellaista tietoa, joka on saatavissa vaikkapa lehdistä, esitteistä ja yrityksen kotisivuilta. Yrityksen tietoja sisältäviin dokumentteihin pitäisi aina merkitä tiedon luokka sekä päivämäärä ja tiedon omistaja. Jokaisen tietoa käyttävän tulisi tietää, miten tietoa hallinnoidaan. (Heljaste, Korkiamäki, Laukkala, Mustonen, Peltonen & Vesterinen 2008, 57.)

Luokittelussa ei ole yhtä ainoaa oikeaa tapaa, poikkeuksena ovat viranomaiset, jotka käyttävät tiettyjä luokkia eri tiedoille. Luokittelusta ei pidä tehdä kovin monimutkaista, luokkia tulisi olla korkeintaan neljä. Lisäksi luokitelluille tiedoille tulisi olla omat käsittelysäännöt, joiden mukaan tietoja käsitellään. Tietojen luokittelu voi olla taulukon muodossa (taulukko 1), tärkeysluokat julkinen, sisäinen, luottamuksellinen, salainen. Käsittelysäännöt voivat koskea merkintää, tiedonjakelua, tiedon salausta, lähetystä sähköpostilla, tietojen tallennusta ja tietojen tallennusta siirrettävälle muistivälineille. (Laaksonen ym. 2006, 29.)

Taulukko 1. Tietojen luokittelu ja käsittelysäännöt (Laaksonen ym. 2006, 157).

Tiedon tärkeysluokka/ käsittelysääntö	Julkinen	Sisäinen	Luottamuksellinen	Salainen
Merkintä	Julkinen vähintään etusivulla	Sisäinen vähintään etusivulla	Luottamuksellinen vähintään etusivulla	Salainen jokaisella sivulla
Tiedonjakelu	Kaikille halukkaille	Kaikille yrityksen työntekijöille	Rajoitetulle määrälle yrityksen työntekijöitä	Erittäin rajoitetulle määrälle yrityksen työntekijöitä
Tiedon salaus	Ei pakollista	Ei pakollista	Pakollista, jos menee yrityksen ulkopuolelle	Aina pakollista
Lähetys sähköpostilla	Sallittu	Sallittu	Sallittu salattuna	Sallittu salattuna
Tietojen tallennus	Ei rajoituksia	Yrityksen keskitetyissä järjestelmissä	Yrityksen keskitetyissä järjestelmissä, asianmukaiset käyttöoikeudet	Yrityksen keskitetyissä järjestelmissä, asianmukaiset käyttöoikeudet ja tiedon salaus
Tietojen tallennus siirrettävälle muistivälineelle	Sallittu	Sallittu, salaus suositeltava	Sallittu salattuna	Sallittu salattuna

Merkintä laitetaan kaikissa tärkeysluokissa dokumentin etusivulle, lisäksi salaisessa laitetaan merkintä dokumentin jokaiselle sivulle. Julkiset tiedot voidaan jakaa kaikille halukkaille, sisäiset yrityksen sisälle, luottamukselliset rajoitetulle määrälle yrityksen työntekijöitä ja salatut erittäin rajoitetulle määrälle yrityksen työntekijöitä. Tiedon salaus ei ole pakollista julkisilla ja sisäisillä tiedoilla, mutta pakollista, jos luottamuksellinen

tieto menee yrityksen ulkopuolella. Salainen tieto kulkee aina salattuna. Sähköpostilla voi lähettää julkisia ja sisäisiä viestejä, mutta luottamukselliset ja salaiset viestit tulee lähettää aina salattuina. (Laaksonen ym. 2006, 157.)

Tietojen tallennuksessa ei ole rajoituksia julkisen tiedon kanssa, mutta sisäisiä tietoja saa tallentaa vain yrityksen keskitetyissä tietojärjestelmissä. Luottamuksellisia tietoja tulee tallentaa vain yrityksen keskitetyissä tietojärjestelmissä, joissa on asianmukaiset käyttöoikeudet, salaiset tiedot voidaan tallentaa yrityksen keskitetyissä tietojärjestelmissä, joissa on asianmukaiset käyttöoikeudet ja tieto tulee salata. Tietojen tallennus siirrettävälle muistivälineelle on julkisen tiedon kohdalla sallittua, sisäistä tietoa suositellaan salattavaksi, luottamuksellista tietoa voidaan siirtää salattuna, samoin salaista tietoa voidaan siirtää vain salattuna. (Laaksonen ym. 2006, 157.)

Tietojen luokittelu ei ole aina pysyvää, sillä luokka saattaa muuttua tiedon elinkaaren aikana. Esimerkiksi tilinpäätöstiedot ovat salaisia, kunnes muuttuvat julkisiksi julkistuksen jälkeen. (Laaksonen ym. 2006, 158.)

3 ISO/IEC 27001-STANDARDI

3.1 Yleistä

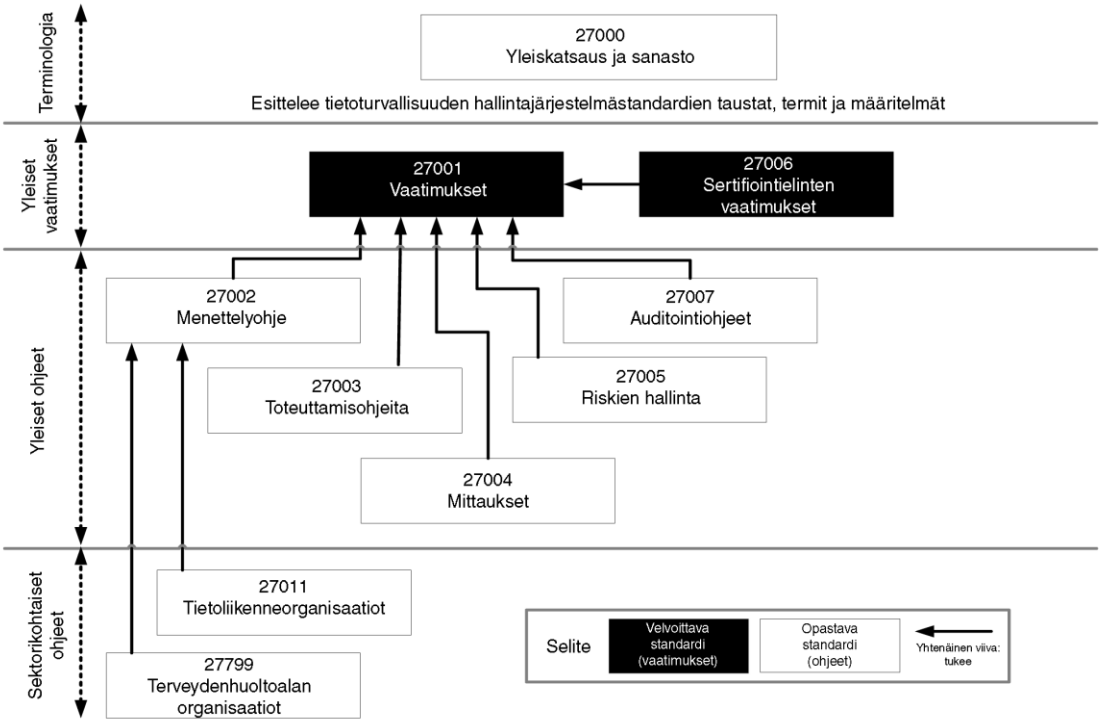
ISO/IEC 27001-standardi on kansainvälinen ja se on laadittu malliksi tietoturvallisuuden hallintajärjestelmän kehittämiselle, käyttämiselle, valvomiselle, katselmoinnille, ylläpitämiselle ja parantamiselle (Suomen standardisoimisliitto 2012, 6).

ISO/IEC 27001-standardi kattaa kaiken tyyppiset organisaatiot sekä määrittelee ne vaatimukset, jotka koskevat dokumentoidun tietoturvallisuuden hallintajärjestelmän luomista, toteuttamista, käyttämistä, valvontaa, katselmointia, ylläpitoa ja parantamista ottaen huomioon organisaation yleiset liiketoimintariskit. Tietoturvallisuuden hallintajärjestelmä luodaan siksi, että voidaan taata riittävä ja asianmukaisesti mitoitettu tietoturvamekanismien valinta. (Suomen standardisoimisliitto 2012, 10.)

Tämän kansainvälisen standardin sisältämät vaatimukset ovat yleisiä ja on tarkoitettu, että ne soveltuvat kaikille organisaatioille niiden tyypistä, koosta tai luonteesta riippumatta. Jos kuitenkin jokin turvamekanismeista jätetään pois, vetoamista tämän kansainvälisen standardin vaatimusten mukaisuuteen ei voida hyväksyä. (Suomen standardisoimisliitto 2012, 10.)

ISO/IEC 27001-standardi korvaa aiemman BS 7799 -standardin ja se toimii tietoturvajohtamisjärjestelmien standardina ja on järjestetty uudelleen yhdenmukaiseksi muiden kansainvälisten standardien kanssa. Uutena lisättynä ohjausmenettelynä on esimerkiksi keskittyminen tietoturvallisuuden hallintaan liittyvien vaarojen johtamiseen. ISO/IEC 27001-standardi on linjassa muiden, kuten laatujohtamisjärjestelmä ISO/IEC 9001-standardin ja ympäristöjärjestelmä ISO/IEC 14001-standardin kanssa. (DNV Business Assurance, hakupäivä 5.4.2013.)

ISO/IEC 27001-standardi ei ole yksittäinen, vaan kuuluu ISO/IEC 27000-standardiperheeseen. Osa standardeista on jo julkaistu ja osa on edelleen valmisteilla (kuva 1).



Kuva 1. ISO/IEC 27000 viitekehys (Suomen standardisoimisliitto SFS ry, hakupäivä 5.2.2013.)

Standardiperheeseen kuuluvat seuraavat ISO/IEC -standardit: ISO/IEC 27000, joka esittelee tietoturvallisuuden hallintajärjestelmästandardien taustat, termit ja määritelmät. ISO/IEC 27001 sisältää vaatimukset ja ISO/IEC 27006 sisältää puolestaan sertifioinnin vaatimukset. ISO/IEC 27002 käsittää menettelyohjeen, ISO/IEC 27003 toteuttamisohjeet ja ISO/IEC 27004 mittaukset. Tietoturvariskienhallintaan liittyy standardi ISO/IEC 27005 ja se sisältää järjestelmällisen riskienanalysointiprosessin, jonka viidellä askelmalla voidaan tuottaa riskien käsittelysuunnitelma. ISO/IEC 27007 sisältää auditointiohjeet. Sektorikohtaisia ohjeita ovat ISO/IEC 27011 tietoliikenneorganisaatioille ja ISO/IEC 27799 terveydenhuoltoalan organisaatioille. (Suomen standardisoimisliitto SFS ry, hakupäivä 5.2.2013.)

ISO/IEC 27001-standarin vaatimuksia ovat:

- linjata tietoturvallisuuden hallinta liiketoiminnan määräystenmukaisuuden ja riskien vähennystavoitteiden kanssa

- suojella tietojen luottamuksellisuutta, eheyttä ja saatavuutta
- olla hallinnollinen eikä tekninen standardi
- keskittyä tietotekniikan lisäksi liiketoiminnan prosesseihin
- löytää, hallinnoida ja vähentää tietoihin liittyviä riskejä.
  (Suomen standardisoimisliitto SFS ry, hakupäivä 5.2.2013.)

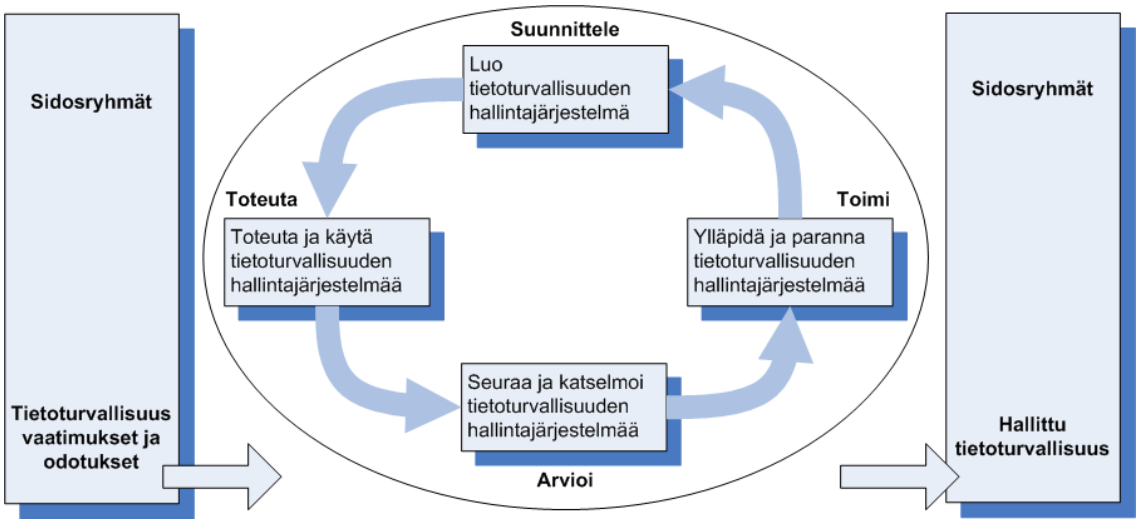
3.2 Prosessimainen toimintamalli

ISO/IEC 27001-standardissa omaksutaan prosessimainen toimintamalli organisaation tietoturvajärjestelmää kehitettäessä, toteutettaessa, käytettäessä, valvottaessa, katselmoitaessa, ylläpidettäessä ja parannettaessa. Jotta yritys voi toimia vakuuttavasti, sen tulee tunnistaa ja johtaa monia eri toimintoja. Sellainen toiminta, jossa käytetään ja johdetaan resursseja sitten, että se mahdollistaa panosten muuttamisen tuotoiksi, voidaan käsittää prosesseiksi. Tietoturvallisuuden hallinnan prosessimainen toimintamalli kannustaa käyttäjiä painottamaan seuraavien asioiden tärkeyttä:

- tietoturvavaatimusten ymmärtämistä ja tietoturvapolitiikan ja tietoturvavelvoitteiden määrittämistä
- turvamekanismien luontia ja käyttöä tietoturvariskien hallintaan
- tietoturvallisuuden hallintajärjestelmän valvontaa
- objektiiviseen mittaamiseen perustuvaa jatkuvaa parantamista. (Suomen standardisoimisliitto 2012, 8.)

PDCA-malli on monenlaisia ongelmia ratkaiseva prosessi. Sitä voidaan käyttää päivittäisessä projektin hallinnassa, toimittajien suhteitten jatkuvassa kehittämisessä, henkilöstön johtamisessa, uusien tuotteiden kehittämisessä sekä prosessin tutkimisessa. (Aaronscreations 2013, hakupäivä 7.4.2013.)

PDCA-mallia eli Suunnittele-Toteuta-Arvioi-Toimi -mallia voidaan soveltaa kaikkien tietoturvallisuuden hallintajärjestelmien prosessien rakenteeseen (kuva 2). (Suomen standardisoimisliitto 2012, 8.)



Kuva 2. PDCA-malli sovellettuna tietoturvallisuuden hallintajärjestelmän prosesseihin (Suomen standardisoimisliitto SFS ry, hakupäivä 5.2.2013)

Sidosryhmillä on turvallisuusvaatimuksia ja -odotuksia. PDCA-malli toimii jatkuvana prosessina, joka turvaa hallitun tietoturvallisuuden:

P = Plan, suunnittele. Luodaan tietoturvallisuuden hallintajärjestelmä.
D = Do, toteuta. Toteutetaan ja käytetään tietoturvallisuuden hallintajärjestelmää.
C = Check, arvioi. Seurataan ja katselmoidaan tietoturvallisuuden hallintajärjestelmää.
A = Act, toimi. Ylläpidetään ja parannetaan tietoturvallisuuden hallintajärjestelmää. (Suomen standardisoimisliitto SFS ry, hakupäivä 5.2.2013)

ISO/IEC 27001-standardi vaatii hallintoa

- tarkastelemaan organisaation tietoturvallisuusriskejä järjestelmällisesti, ottamalla huomioon uhkat, haavoittuvuudet ja vaikutukset
- suunnittelemaan ja toteuttamaan yhdenmukaiset ja kattavat tietoturvallisuuskontrollit ja riskien käsittelyohjeet jotta riskit, joita on mahdoton hyväksyä, saadaan käsiteltyä
- omaksumaan ylikaartuvan hallintoprosessin varmistaakseen tietoturvallisuuskontrollien jatkuvuuden tulevaisuudessa. (Suomen standardisoimisliitto SFS ry, hakupäivä 5.2.2013.)

3.3 Termit ja määritelmät

Seuraavaksi luetellaan ISO/IEC 27001-standardiin liittyviä termejä ja määritelmiä, joita käytettäessä tiedetään, että kaikki standardia käyttävät puhuvat asioista samoilla nimillä. Seuraavan luettelon määritelmät on poimittu ISO/IEC 27001-standardista:

- Suojattava kohde
  Mikä tahansa, jolla on arvoa organisaatiolle. (Suomen standardisoimisliitto 2012, 10.)

- Käytettävyys
  Ominaisuus, että tieto on saatavilla ja käyttökelpoinen. (Suomen standardisoimisliitto 2012, 10.)

- Luottamuksellisuus
  Ominaisuus, että tietoa ei luovuteta luvattomalle henkilöille, tahoille tai prosesseille. (Suomen standardisoimisliitto 2012, 10.)

- Tietoturvallisuus
  Tiedon luottamuksellisuus, eheys ja käytettävyys säilytetään. Näiden lisäksi tähän voi sisältyä muita ominaisuuksia, kuten aitous, vastuullisuus, kiistämättömyys ja luotettavuus. (Suomen standardisoimisliitto 2012, 12.)

- Tietoturvatapahtuma
  Tunnistettu järjestelmän, palvelun tai verkon tila, joka viittaa mahdolliseen tietoturvapolitiikan murtamiseen tai turvatakuiden pettämiseen, tai aikaisemmin tuntematon, odottamaton tilanne, jolla saattaisi olla merkitystä turvallisuudelle. (Suomen standardisoimisliitto 2012, 12.)

- Tietoturvahäiriö
  Epätoivottu tai odottamaton tietoturvatapahtuma, joka todennäköisesti vaarantaa liiketoiminnot ja on uhkana tietoturvallisuudelle. (Suomen standardisoimisliitto 2012, 12.)

- Tietoturvallisuuden hallintajärjestelmä (ISMS, Information Security Management System)

  Osa yleistä toimintajärjestelmää, joka liiketoimintariskien arviointiin perustuen luodaan ja toteutetaan. Sitä käytetään, valvotaan, katselmoidaan, ylläpidetään ja parannetaan ja sen tavoitteena on hyvä tietoturvallisuus. Hallintajärjestelmä sisältää myös organisaatiorakenteen, käytetyt politiikat, suunnittelutoimenpiteet, vastuut, menettelytavat, menetelmät, prosessit sekä resurssit. (Suomen standardisoimisliitto 2012, 12.)

- Eheys

  Suojattavien kohteiden oikeellisuus ja täydellisyys turvataan. (Suomen standardisoimisliitto 2012, 12.)

- Jäännösriski

  Riski joka jää jäljelle riskien käsittelyn jälkeen. (Suomen standardisoimisliitto 2012, 12.)

- Riskien hyväksyntä

  Päätetään, että riski otetaan. (Suomen standardisoimisliitto 2012, 12.)

- Riskianalyysi

  Riskianalyysissä tietoja käytetään systemaattisesti riskien tunnistamiseen sekä niiden vaikutuksen arviointiin. (Suomen standardisoimisliitto 2012, 12.)

- Riskien arviointi

  Kattaa riskianalyysin ja riskien vaikutuksen arvioinnin. (Suomen standardisoimisliitto 2012, 12.)

- Riskien vaikutusten arviointi

  Tässä prosessissa tunnistettujen riskien vaikutusta verrataan annettuihin kriteereihin ja tavoitteena on riskin merkityksellisyyden arviointi. (Suomen standardisoimisliitto 2012, 12.)

- Riskien hallinta
  Toimenpiteet, joilla koordinoidusti johdetaan ja ohjataan organisaation riskien käsittelyä. (Suomen standardisoimisliitto 2012, 14.)

- Riskien käsittely
  Tässä prosessissa valitaan ja toteutetaan riskejä muuttavia toimenpiteitä. (Suomen standardisoimisliitto 2012, 14.)

- Soveltamissuunnitelma (SoA)
  Tässä dokumentissa kuvataan organisaation tietoturvallisuuden hallintajärjestelmän kannalta olennaiset ja siihen soveltuvat valvontatavoitteet ja turvamekanismit. (ISO/IEC 27001.)

3.4 Tietoturvallisuuden hallintajärjestelmä

ISO/IEC 27001-standardin mukaan yrityksen tulee luoda, toteuttaa, käyttää, valvoa, katselmoida, ylläpitää ja kehittää dokumentoitua tietoturvallisuuden hallintajärjestelmää, joka tukee yrityksen liiketoimintaa. Hallintajärjestelmän luomiseksi tulee määritellä hallintajärjestelmän rajat ja kattavuus, unohtamatta liiketoiminnan erityispiirteitä. Samalla tulee määritellä puitteet tavoitteiden asettamiselle ja luoda yleinen suunta ja periaatteet. Tulee muistaa myös liiketoimintaan liittyvät sekä lakisääteiset että hallinnolliset vaatimukset ja sopimuksiin liittyvät tietoturvavelvoitteet. Kaikki nämä asiat tulisi olla johdon hyväksymiä ja samassa linjassa yrityksen riskienhallintastrategian kanssa. (Suomen standardisoimisliitto 2012, 14.)

Hallintajärjestelmän ylimmällä tasolla ovat dokumentoituina seuraavat asiat:

- toiminnan uhkakartoitus
- riskienhallintasuunnitelma
- tietoturvapolitiikka
- tietoturvakäytännöt, joilla normaalisti suojataan tietojenkäsittely, verkot, työasemat, sähkönsaanti ja tilat

- tietoturvallisuuden perusohjeistus ja lisäohjeistusturvallisuuden kehittämissuunnitelma
- tietoturvallisuuden raportointi johdolle
- jatkuvuussuunnitelma
- toipumissuunnitelma
- poikkeusolojen tietojenkäsittelyn valmiussuunnitelmat
- toimintaan liittyvät tietoturvaprosessit
- auditointisuunnitelma. (Valtionvarainministeriö, hakupäivä 20.2.2013.)

Tietoturvan toteuttamiseen tarvitaan ohjeistus. Tietoturvaohjeiden tuottamisen ja ylläpidon prosessissa tulisi olla seuraavat vaiheet, kun havaitaan asia tai tapahtuma, joka edellyttää ohjeen laatimista:

- Ensin tarkastetaan, onko asiasta jo ohje. Olemassa oleva ohje päivitetään tarvittaessa.
- Jos ohjetta ei ole, laaditaan luonnos, joka käsitellään tietohallinnossa.
- Luonnos annetaan lausunnolle ja käsitellään turvallisuus- ja valmiusasianryhmässä.
- Jos ohjeen asia on niin laaja, että vaatii johtoryhmäkäsittelyn, niin hyväksytetään ohje johtoryhmässä ennen sen voimaan tuloa.
- Tietohallinto julkaisee ja tiedottaa ohjeen.
- Ohjeen kouluttaminen suunnitellaan hallinnon kanssa.
- Ohjeistus koulutetaan.
- Tarkastellaan ohjeet vuosittain ja tehdään tarvittavat päivitykset.
- Tiedotetaan toimenpiteistä ja parannuksista henkilökunnalle ja sidosryhmille yksityiskohtaisesti. (Valtionvarainministeriö, hakupäivä 20.2.2013.)

Kun ollaan arvioimassa tietoturvallisuuden hallintajärjestelmää, pitää tunnistaa, onko ohjeistus riittävä ja onko se sisällöltään kattava suhteessa organisaation toimintaan. Ohjeille määritellään omistaja, joka vastaa niiden ylläpidosta. (Valtionvarainministeriö, hakupäivä 20.2.2013.)

3.5 Johdon vastuu

Johdon tulee sitoutua tietoturvallisuuden hallintajärjestelmän luomiseen, käyttöönottoon, käyttöön, valvontaan, katselmointiin, ylläpitoon ja parantamiseen. Johdon vastuulla on määritellä tietoturvapolitiikka, ja varmistaa, että tietoturvatavoitteet asetetaan ja -suunnitelmat laaditaan. Johdon tulee määritellä roolit ja vastuuhenkilöt, sekä viestiä koko organisaatiolle, miten tärkeää on noudattaa annettua tietoturvapolitiikkaa ja -tavoitteita ja niihin liittyviä lakisäätteisten velvoitteiden noudattamista. Johto sitoutuu myös vastaamaan, että käytössä on riittävät resurssit hallintajärjestelmän kehittämiseen, toteuttamiseen, käyttöön ja ylläpitoon, sekä päättämään riskien hyväksymiskriteerit ja hyväksyttävät riskitasot. Johdon vastuulle kuuluu myös varmistaa, että auditoinnit ja johdon katselmukset tulevat suoritetuiksi. (Suomen standardisoimisliitto 2012, 24.)

3.6 Tietoturvallisuuden hallintajärjestelmän sisäiset auditoinnit

Sisäisiä auditointeja tulee järjestää suunnitellun aikataulun mukaisesti, jotta voidaan määritellä, ovatko tietoturvallisuuden hallintajärjestelmän valvontavelvoitteet, turvamekanismit, prosessit ja menettelytavat

- ISO/IEC 27001-standardin ja soveltuvan lainsäädännön mukaisia
- tietoturvavaatimusten mukaisia
- toteutettuina ja ylläpidettyinä sekä toimivat odotusten mukaisesti. (Suomen standardisoimisliitto 2012, 26.)

Auditointiohjelma tulee suunnitella siten, että otetaan huomioon auditoitavien prosessien ja alueiden tila ja tärkeys sekä aiempien auditointien tulokset. Auditointien kriteerit, laajuus, suoritustaajuus ja menettelyt tulee määritellä tarkkaan. Auditoijat eivät saa auditoida omaa työtään. Vastuuhenkilön tulee varmistaa, että havaittujen poikkeamien ja niiden syiden poistamisen toimenpiteet suoritetaan ilman aiheetonta viivettä. Seurantatoimenpiteisiin kuuluu suoritettujen toimenpiteiden toteaminen ja niiden tuloksista raportoiminen. (Suomen standardisoimisliitto 2012, 26.)

3.7 Tietoturvallisuuden hallintajärjestelmän johdon katselmus

Johdon tulisi katselmoida tietoturvallisuuden hallintajärjestelmä ennalta suunnitelluin väliajoin, vähintään kuitenkin kerran vuodessa. Tällä katselmoinnilla varmistetaan hallintajärjestelmän soveltuvuus, asianmukaisuus ja vaikuttavuus. Katselmuksen tulokset tulee dokumentoida selkeästi. Katselmuksen lähtötietojen tulee sisältää mm. sidosryhmien antamaa palautetta, tehokkuusmittausten tuloksista, aiempien johdon katselmusten seurantatoimenpiteistä sekä parantamissuosituksista. Katselmusten tulosten tulee sisältää päätökset ja toimenpiteet jotka liittyvät mm. tietoturvallisuuden hallintajärjestelmän vaikuttavuuden parantamiseen, riskien arviointi- ja käsittelysuunnitelman päivittämiseen tietoturvallisuuden menettelyjen ja toimintatapojen muuttamiseen, kun ne koskevat esim. liiketoiminnan vaatimuksia, turvallisuusvaatimuksia, lakisääteisiä tai hallinnollisia vaatimuksia, resurssitarpeita sekä turvamekanismien tehokkuuden mittaamistavan parantamista. (Suomen standardisoimisliitto 2012, 26, 28.)

3.8 Tietoturvallisuuden hallintojärjestelmän parantaminen

Yrityksen tulisi jatkuvasti parantaa tietoturvallisuuden hallintajärjestelmän vaikuttavuutta käyttämällä tietoturvatavoitteita, auditointien tuloksia, tapahtumien analysointia, korjaavia ja ehkäiseviä toimenpiteitä sekä johdon katselmuksia. Jotta tietoturvallisuuden hallintajärjestelmän poikkeamat eivät toistuisi, pitäisi laatia toimenpiteiden dokumentoitu menettely, joissa tunnistetaan poikkeamat, selitetään poikkeamien syyt, arvioidaan, mitä toimenpiteitä tarvitaan poikkeamien toistumisen estämiseksi, miten määritetään tarvittavat korjaavat toimenpiteet ja suoritettujen korjaavien toimenpiteiden katselmointi. Lisäksi tulee määritellä ehkäisevät toimenpiteet, ja näiden tärkeysjärjestys tulee päättää riskien arvioinnin tulosten perusteella. (Suomen standardisoimisliitto 2012, 30.)

4 TIETOTURVAKARTOITUS

4.1 Kysely

Tämän tutkimuksen keskeinen osa on esimerkkiyritykselle tehtävä tietoturvakartoituskysely. Hakiessani tietoa kyselylomakkeen suunnitteluun löysin valmiin kyselypohjan Internetistä, VTT:n pk-yritysten riskienhallinnan työvälinesarja – Henkilöstön tietoisuus ja toimintatavat. Kyselyssä on viisi osaa, joista ensimmäinen ja viides sopivat kaikille vastattaviksi ja osat 2, 3 ja 4 sopivat esimiesten vastattaviksi. Kysymykset ovat kokonaisuudessaan ja ”kyllä” -vastauksineen (%) liitteessä 1.

Kyselyn vastaajat saivat viikon vastausaikaa. Kyselyn vastausprosentiksi tuli 82, erikseen laskettuna esimiesten vastausprosentti oli 100. Tämän lisäksi kukaan vastaajista ei vastannut pelkästään yhdellä tavalla (kyllä, ei tai ei kuulu meille), joten jokainen vastaaja oli perehtynyt kysymyksiin.

Osan 1 kysymyksiin vastasivat kaikki vastaajat. Tässä osassa kartoitettiin vastaajien tietoisuutta tietoriskeistä. Vajaa puolet (43 %) vastaajista kertoi, että heitä oli koulutettu liiketoiminnan ja tuotekehityksen luottamuksellisuuteen ja tietosuojaan liittyviin kysymyksiin. Suurin osa (86 %) vastaajista tunsi yrityksen vastuun tietojen luottamuksellisuudesta ja tietoturvasta. Lähes kaksi kolmasosaa (64 %) vastaajista tiesivät, millaisten tietojen suojaaminen on tärkeää ja muutama vastaaja määrä vastaajista (71 %) pitivät selvänä, mitä yrityksen asioista voi kertoa ulkopuolisille. Noin puolet (57 %) vastaajista tiesivät, että yrityksellä on olemassa tietoturvaperiaatteet ja niiden mukaan laaditut ohjeet. Lähes kaksi kolmasosaa (64 %) vastaajista vastasivat, että on olemassa ohjeet myös suullista viestintää ja paperidokumenttien käsittelyä sekä jakamista varten. Tasan puolet (50 %) vastaajista tiesivät, että henkilöstö on koulutettu tunnistamaan tietoriskejä ja noudattamaan yrityksen turvakäytäntöjä. Vajaa kolmannes (29 %) vastaajista vastasivat, että tietoturva-asioita varten on olemassa menettely ja tietojen luokitteluohjeet sekä käytännöt ovat osa yrityksen arkipäivää. Vajaa puolet (43 %) vastaajista kertoivat allekirjoittaneensa tietojen käyttösäännöt. Lähes kaksi kolmasosaa (64 %) vastaajista tiesivät, minne voi ilmoittaa havaitsemistaan tietoturvarikkeistä ja -puutteista.

Osaan 2 vastasivat esimiehet. Tässä osassa aiheena oli uudet työntekijät. Uusien työntekijöiden taustat tarkistetaan ennen työsuhteen alkua, näin ei vastannut kukaan (0 %). Sen sijaan kaikki vastasivat (100 %) tietoturva-asioiden olevan mukana uusien työntekijöiden perehdyttämisessä ja uusille sekä väliaikaisille työntekijöille selvitetään yrityksen tietoturvapolitiikan ja vaitiolositoumuksen merkitys. Kaksi kolmasosaa (67 %) vastasivat, että työntekijät allekirjoittavat erillisen sitoumuksen tietojen ja järjestelmien käytöstä sekä tietojen palauttamisesta työsuhteen jälkeen.

Osaan 3 vastasivat edelleen vain esimiehet aiheesta työsuhteen päättyminen. Kaksi kolmasosaa vastaajista (67 %) vastasivat, että on suunniteltu toimenpiteet, joilla varmistetaan tietoturvallisuus työsuhteiden päättyessä ja esimiehillä on tieto henkilön irtisanoutumistilanteessa kaikista käyttäjätunnuksista ja käyttöoikeuksista, joiden voimassaolo voidaan poistaa. Kaikki esimiehet (100 %) huolehtivat siitä, että kaikki työntekijän käytössä olleet työ-, tallennusvälineet sekä yritystä koskevat asiakirjat palautetaan yritykselle. Sen sijaan vain kolmannes (33 %) esimiehistä vastasivat, että on varauduttu työntekijöiden riitaisaan irtisanoutumiseen tai irtisanomiseen.

Osaan 4 vastasivat esimiehet. Tässä osassa kartoitettiin henkilöstön toimintatapoja. Kaikki esimiehet (100 %) vastasivat, että työntekijät käsittelevät työhönsä liittyviä, luottamuksellisia tietoja tarkoituksenmukaisesti ja että yrityksen keskeiset tiedot on suojattu mm. rajaamalla niiden saatavuus ja määrittelemällä niiden käyttöoikeudet. Kaksi kolmasosaa (67 %) vastasivat, että yrityksen keskeiset tietojen ja dokumenttien myynti tai luovutus on minimoitu sekä yrityksen sisäiset valvontajärjestelmät ovat asianmukaiset ja luottamuksellisten tietojen säilyttämiseen on riittävästi lukittuja tiloja. Myös työntekijöiden omien töiden tekeminen työpaikalla on valvottua. Sama määrä vastaajia (67 %) vastasivat, että puhelinkäyttäytymisohjeet ovat olemassa ja varahenkilöjärjestelyistä on huolehdittu. Kaikki vastaajat (100 %) tiesivät jätepaperin keräyksen ja käsittelyn hoituvan hallitusti. Kolmasosa vastaajista (33 %) vastasivat, että tulipalon varalta on harjoiteltu.

Osan 5 kysymyksiin vastasivat jälleen kaikki vastaajat. Tässä viimeisessä osassa kartoitettiin tietojärjestelmien ja tietokoneiden käyttö. Melkein neljä viidesosaa vastaajista (79 %) vastasivat, että henkilöstöllä on riittävä perusosaaminen järjestelmien käyttöön.

Kaikki vastaajat (100 %) saavat häiriö- ja virhetilanteissa apua ja neuvontaa. Melkein kaikki (93 %) vastaajat kertoivat, että jokainen työntekijä käyttää työssään vain omaa käyttäjätunnustaan, sama määrä vastaajia tiesi Internetin käytön olevan ohjeistettu. Turvallisen salasanan muodostaminen on varmistettu ja sähköpostin käyttö on ohjeistettu, näin vastasivat yli kaksi kolmasosaa (71 %) vastaajista. Hieman suurempi määrä vastaajista (79 %) vastasivat, että on estetty mahdollisuus muilta työntekijöiltä lukea tai muuttaa käyttäjän tietoja huomaamatta. Puolelle (50 %) vastaajista oli selvää, että virustorjuntamenettelyt on ohjeistettu työ- ja kotikoneiden osalta. Suurin osa (86 %) vastaajista tiesivät virusohjelmien ja muiden vastaavien ohjelmien päivittyvän automaattisesti. Luottamuksellisia tietoja salakirjoitetaan, kun käytetään kannettavia laitteita, näin ei vastannut kukaan (0 %). Melkein kaikki (93 %) vastaajista tiesivät, ettei yrityksen verkkoon tai laitteisiin saa asentaa ulkopuolisia ohjelmia tai laitteita.

4.2 Analysointi

Kyselyn vastausprosentti oli erinomainen, 82. Tästä voidaan päätellä, että työntekijöitä kiinnostaa yrityksen tietoturva-asiat ja he ovat innokkaasti mukana kertomassa oman näkemyksensä asiassa. Tämä kertoo myös siitä, että kyselyn jälkeen mahdollisesti tuleviin jatkotoimenpiteisiin riittänee myös kiinnostusta.

Miten odottamattomaan on varauduttu esimerkkiyrityksessä, nähdään nopeasti vastauksista. Kaikki vastaajat eivät ole varautuneet odottamattomaan, sen huomaa runsaista ”ei” -vastauksista. Miten tietoturva liittyy liiketoimintaan, oli myös yksi johdantokappaleessa esitetyistä kysymyksistä. Kyselyn vastausten perusteella suurin osa henkilökunnasta on sitä mieltä, että henkilökunnalle ei ole koulutettu nykyaikaisen liiketoiminnan ja tuotekehityksen luottamuksellisuuteen ja tietosuojaan liittyviä yleispiirteitä. Tämä oli kyselyn ensimmäinen kysymys ja ”kyllä”-vastausten osuus oli vain 43 %.

Seuraavaksi kysyttiin, onko tietoturvavaatimukset ymmärretty ja ovatko tietoturvatavoitteet ja tietoturvapolitiikka määritetty. Kun kysymykseen ”kyllä”-vastauksia oli 57 %, on yli puolet henkilökunnasta sitä mieltä, että yritykselle on määritelty tietoturvaperiaatteet ja niiden toteuttamiseksi on tehty ohjeetkin. ”Ei”-vastausten lukumäärä antaa ymmärtää, että nämä ohjeet eivät ole kaikilla tiedossa.

Kyselyn vastausten perusteella ainoastaan yksi koko henkilökunnalle osoitettu kysymys sai myönteisen vastauksen. Kysymys oli 5. osan toinen kysymys: ”Saavatko työntekijät häiriö- ja virhetilanteissa apua ja neuvontaa”. Myönteinen vastaus tälle kysymykselle tarkoittaa sitä, että jokainen voi luottaa saavansa apua, kun sitä tarvitsee. Mutta jos ei tiedä, mitä kaikkia asioita tietoturvaan liittyy, ei osaa kysyä tarvittaessa apua.

Jokainen esimies vastasi myönteisesti 2. osan kakkoskohtaan ”Ovatko tietoturva-asiat mukana uusien työntekijöiden perehdyttämisessä”. Tietoturva-asiat käydään siis läpi perehdytysvaiheessa. Kaikki esimiehet olivat myös sitä mieltä, että työntekijät käsittelevät työhönsä liittyviä luottamuksellisia tietoja tarkoituksenmukaisesti. Mitään ongelmia ei siis ole ollut henkilökunnan tietojenkäsittelyn kanssa, eli esimiesten mukaan henkilökunta tietää, miten asioita käsitellään. Tässä lienee syy siihen, että muuhun tietoturvakoulutukseen ei ole ollut tarvetta. Kaikki vastaajat vastasivat kuitenkin vain 86 prosenttisesti kyllä, kun kysyttiin, tuntevatko he vastuun tietojen luottamuksellisesta ja tietoturvasta. Tästä voidaan vetää se johtopäätös, että perehdytystilanteessa tapahtuva tietoturvakoulutus pitäisi kerrata säännöllisin väliajoin. Kaikki asiat eivät ole jääneet perehdytyksestä mieleen ja sen ajankohdastakin saattaa olla kulunut jo useampi vuosi.

Tietoturvaosaaminen tuntuu epävarmalta ehkä juuri siksi, että asioita ei ole ehditty kertaamaan säännöllisin väliajoin, eikä työtehtävien muuttuessa ole välttämättä painotettu erikseen juuri siihen työhön liittyviä tietoturvanäkökohtia. Kuitenkin tärkeimmät asiakkaisiin liittyvät tietoturvaohjeet on sisällytetty työohjeisiin jo lainsäädännön vuoksi. Olemme siis saaneet vastauksen kysymykseen, mikä on henkilökunnan tietoturvaosaamisen taso tällä hetkellä.

Yhtä kaikille osoitettua kysymystä lukuun ottamatta kaikkiin kysymyksiin saatiin ”kyllä”-vastausten lisäksi ”ei”-vastauksia, joten kannattaisi alkaa suunnitella tietoturva-asioiden kertausta. Jos osa työntekijöistä on ollut jo vuosia työsuhteessa ja tietoturvaperehdytys on ollut muun perehdytyksen yhteydessä, ei ole ihme, jos jotkut asiat tai termit ovat jo unohtuneet. Pitäisi pohtia sitä, minkälainen lisäkoulutus olisi riittävän tehokasta ja silti mieleenpainuvaa.

4.3 Jatkotoimenpiteet

Tietoturvakoulutukseen sopivat monenlaiset opetusmenetelmät. Itsenäisen työskentelyn opetusmenetelmien elementteinä ovat yksilöllisyys ja eriytyvät työtavat ja esimerkkinä voisi olla tietokoneella tapahtuva opetus, jonka lähtökohtana on yksilöllisyys ja yksilöllisen etenemisen mahdollistava oppimateriaali ja ohjaus. Yhteistoiminnalliseen työskentelyyn pohjautuvista menetelmistä ovat esimerkkeinä ryhmätyö ja aivoriihi. Esittävistä opetusmenetelmistä luento on tyypillinen esimerkki. Oppimisen näkökulmasta hyvään lopputulokseen voi päästä useallakin eri menetelmällä. (Oulun yliopisto 2007, hakupäivä 1.4.2013.)

Paperiohjeet saattavat jäädä pöydälle ja Internetin selaaminen on helpompaa pienen tauon tullessa ajankohtaiseksi. Esimerkkiyrityksessä Internet avautuu aina intranetin etusivulle. Tälle sivulle voisi laittaa esimerkiksi joka kerta kirjautuessa vaihtuvan ”tietoturva-aforismin”. Mielekkäämpää on, jos tietoturvasääntöjä laitetaan vaikkapa runomuotoon, mitä hauskempi runo, sitä parempi. Kun tähän vielä määritellään arvottavaksi aina erilainen sääntö tai ohje, tulevat kaikki asiat jo lyhyen ajan sisällä käytyä läpi ja siirtyvät pikkuhiljaa pitkäkestoiseen muistiin kertauksen avulla. Vaihtuvan ohjeen voisi sijoittaa sivun kulmaan niin, että se näkyy mutta ei häiritse.

Jos jollakin henkilöllä yrityksen sisällä riittää aikaa laittaa tietoturva-asioita vaikkapa sarjakuvamuotoon, ovat tämän tyyppiset asiat helppo lukea esimerkiksi työpisteen seinältä. Tästä aiheesta voisi teettää ryhmätyön, vaikkapa piirustuskilpailun ”odota odottamatonta” ja palkintona voisi olla pullakahvit. Pääasia on, että saadaan henkilökunta pohtimaan omaan työhön liittyviä tietoturva-asioita.

On olemassa myös valmiita Internetkyselyjä, joita voi tietyin väliajoin käydä tekemässä ja arvioimassa niiden perusteella omia tietoturvataitoja. Näistäkin voisi laittaa linkkejä intranetin etusivulle. Mutta pelkkä teoria ei kuitenkaan jää niin helposti mieleen kuin itse tekeminen. Toivottavasti ainoa keino tekemällä oppimisesta ei ole virheistä oppiminen. Käytännön opetusta voi antaa myös ennaltaehkäisevästi.

Otetaan esimerkiksi ensiapukoulutus. Ensiavun oppiminen on tärkeää ja usein kursseilla saadaan teoriaopetuksen lisäksi tehdä käytännön harjoituksia. Asia on vakava ja harjoi-

teltavat haavojen sitomiset ja elvytystehtävät on tehtävä huolella. Kurssin lopuksi pidetään koe, jossa katsotaan, miten oppi meni perille ja voiko kurssilaiselle antaa ensiapukortin. Kurssin jälkeen on hyvä mieli siitä, että on oppinut asioita, joilla saattaa pelastaa hengen. Voisimme käyttää samantapaista menetelmää tietoturvakoulutuksessa. Vaikkapa näin, että ensin kouluttaja käy läpi luento-osuuden, joka on oman yrityksen tietoturvallisuusohjeiden mukainen. Sen jälkeen tehdään ryhmittäin pieniä harjoituksia, joissa ratkaistaan tietoturvaongelmia ja pohditaan, miten nämä ongelmat olisi voitu välttää. Jokainen osallistuu harjoituksiin ja pohtii miten ongelmat liittyvät omaan työhön ja miettivät muita omaan työhönsä liittyviä tietoturvariskejä. Opetustilaisuuden jälkeen suoritetaan pieni koe, jossa jälleen katsotaan, onko kurssilainen ymmärtänyt asian. Mikään ei estä antamasta tietoturvadiplomia kurssin päätteeksi. Ja kun tekemällä on harjoiteltu, on oppi jäänyt paremmin mieleen kuin pelkillä diaesityksillä.

Osasto- tai kuukausipalavereja voisi myös täydentää tietoturva-asioilla. Sen lisäksi, että käydään läpi tapahtuneet ja tulevat asiat, voitaisiin pitää pieni parin minuutin tietoisku palaverin alussa. Jotta asia olisi mielekäs ja kiinnostaisi kaikkia osallistujia, näihin pieniin puheenvuoroihin voisi vuorotellen osallistua jokainen työntekijä yksin tai työparin kanssa. Tilanteita sattuu ja tapahtuu jatkuvasti, niitä ei tarvitse keksiä. Riittää, kun kertoo sattuneen tapauksen tai mitä olisi voinut sattua ja miten siitä selvittiin tai mitä siitä aiheutui. Kun valmistelee pienenkin puheenvuoron tutusta aiheesta, jää asia paremmin mieleen kaikille osallistujille kuin jos sen vain lukisi paperista itsekseen. Tietoturva-asioiden puhumisesta tehdään tapa, asiat eivät tunnu enää niin vierailta ja jokainen voi osallistua asioiden kehittämiseen turvallisempaan suuntaan.

5 RISKIEN HALLINTA

5.1 Riskien arviointi

Tietoturvapolitiikan nojalla voidaan tehdä erilaisia tietoturvaohjeita riippuen siitä, mitkä ohjeet ovat yrityksessä tarpeen. Ohjeiden laatimiseen kannattaa kerätä laaja työntekijäjoukko, sillä he ovat yrityksessä usein parhaita asiantuntijoita sanomaan, mitä tarvitaan ja miten suunniteltu ohjeistus toimisi. Kun työntekijät osallistuvat ohjeiden suunnitteluun ja arviointiin, voidaan välttää muutosvastarintaa ohjeiden käyttöönoton yhteydessä. (Heljaste ym. 2008, 13.)

Kun käynnistetään riskien arviointi, on hyvä kartoittaa, mitä suojattavaa yrityksellä on. Tässä vaiheessa yritys voi käyttää apunaan asiantuntijoita, mutta yleensä yrityksen sisällä on riittävä tieto siitä, mitä tarvitsee suojata. Riskejä arvioitaessa on yksinkertaista tehdä taulukko, johon riskit sijoitetaan sen mukaan, miten todennäköiseksi ne arvioidaan ja miten suurta vahinkoa tulisi yritykselle, jos riski toteutuisi. Esille nousseet riskit laitetaan siihen järjestykseen, jossa niihin on järkevää ja mahdollista varautua. (Heljaste ym. 2008, 14, 15.)

Suojattavien kohteiden rajaamisessa kannattaa olla huolellinen, sillä liian korkeasta tietoturvallisuudesta ei tule maksaa ylihintaa, eikä rima saa olla liian alhaallakaan (Rautvuori 2011, 30). Kaikkia tietoturvauhkia ei koskaan voida tietää etukäteen, minkä vuoksi järjestelmällisyyden tulisi korostua tietoturvatyössä (Lagus 2013, 10).

5.2 Riskianalyysi

Kaikki riskit eivät löydy yhdellä menetelmällä. Riskianalyysiä tehtäessä voisi käyttää toisia täydentäviä menetelmiä, yksi karkean tason tunnistusmenetelmä, yksi teknisen järjestelmän tarkkailuun ja yksi menetelmä ihmisten työtehtävien tarkasteluun. Riskianalyysissä kannattaa hyödyntää usean ihmisen tietoja ja ottaa mukaan riskianalyysipalavereihin henkilöitä, jotka tuntevat saman kohteen eri näkökulmista. Olisi myös hyvä ottaa heti mukaan henkilö, jolla on valtuudet päättää korjaavista toi-

menpiteistä. Kun ottaa yhden selkeän kokonaisuuden kerrallaan analysoitavaksi, saadaan tarkastelu käytyä läpi kohtuuajassa. Jokainen palaveri valmistellaan tekemällä etukäteisselvityksiä ja kokoamalla mukaan tarvittavat asiakirjat. Palavereissa kannattaa luoda selkeä yhteinen käsitys tarkasteltavasta kohteesta, vaikkapa kaavioilla ja taulukoilla. Kun ketään ei syyllistetä kokouksissa, löytyvät syyt helpommin. Avoimuus on välttämätöntä, sillä pienessä yrityksessä riskit saattavat liittyä yhden henkilön tekemiin tai tekemättä jättämiin toimenpiteisiin. (VTT, hakupäivä 3.4.2013.)

Löytyneistä riskeistä tulee tunnistaa, mitkä ovat suurimmat ja tärkeimmät torjua. Riskit priorisoidaan selvittämällä niiden suuruus, tämä määräytyy mahdollisten vahinkojen suuruuden ja vahingon todennäköisyyden perusteella. Riskianalyysissäkin dokumentointi on tärkeää. Tärkeintä riskianalyysissä on sopia siitä, miten toimitaan että saadaan tunnistetut riskit hallintaan ja aloittaa toimenpiteiden seuranta. Analyysi pitää myös muistaa päivittää, kun kohde muuttuu, joka tapauksessa katsaus riskeihin määräajoin on tarpeellista, jotta asiat pysyvät hallinnassa. (VTT, hakupäivä 3.4.2013.)

Riskianalyysia tehdessä tulee ymmärtää erilaiset uhkien aiheuttajat, joita ovat mm. oma henkilöstö, ulkopuoliset toimijat, järjestelmien ja laitteiden tekniset virheet tai vaurioitumien sekä onnettomuudet. Riskianalyysin tekoon on olemassa paljon työkaluja. Hyvä esimerkki on Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTI -julkaisu, joka on verkossa saatavilla ilmaiseksi. Voimassa olevat VAHTI-ohjeet löytyvät verkosta www.vm.fi/vahti. (Iivari ym. 2009, 119.)

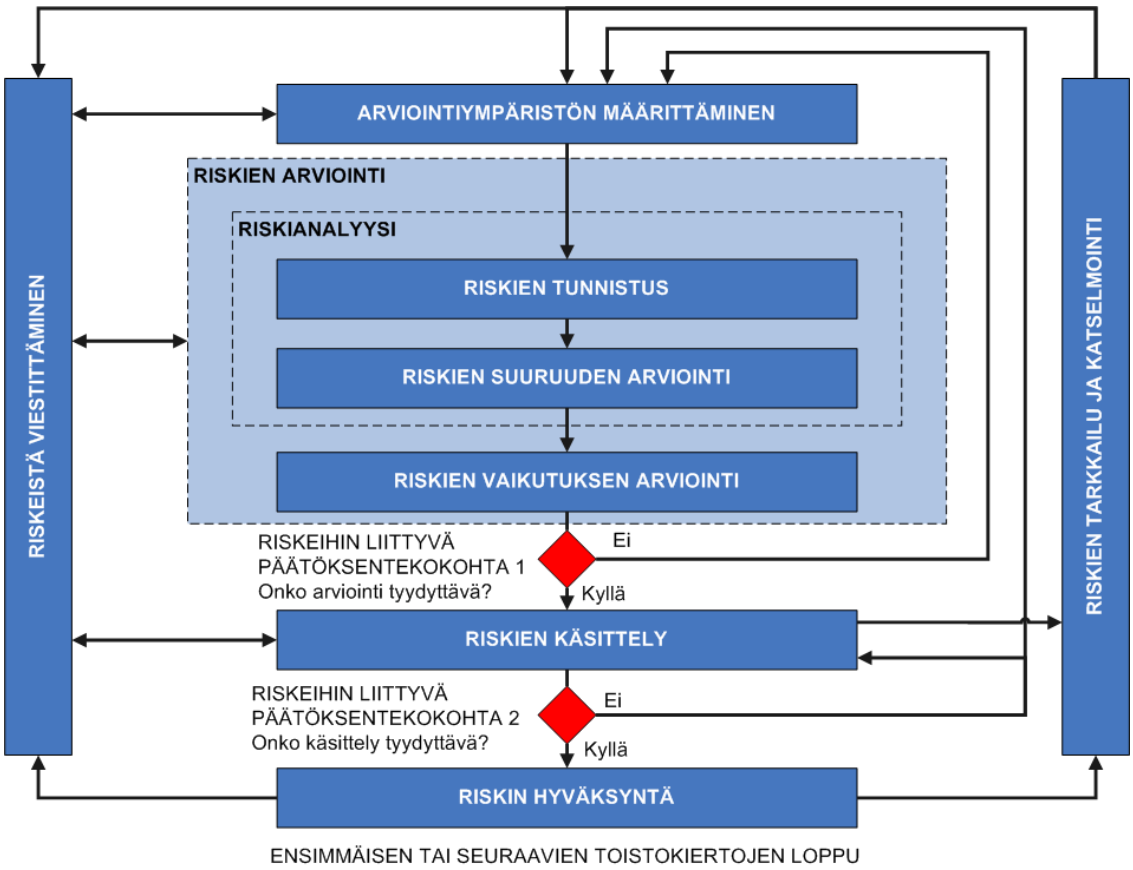
Kaikkia riskejä ei tarvitse poistaa. On olemassa riskejä, joiden kanssa tulee toimeen, kunhan sen vain tiedostaa. Muutaman euron riskiin ei kannata tuhlata tuhansia euroja. Joitakin riskejä varten voi varautua halutessaan vapaaehtoisella vakuutuksella ja osa vakuutuksista onkin lakisääteisiä.

Tietoturvariskien lisäksi tulee muistaa myös seuraavat riskit:

- Liikeriski on liikevoiton saamiseksi otettava tietoinen riski ja ne ovat olennainen osa liiketoimintaa.
- Henkilöriskejä ovat esim. ammattiosaamisen väheneminen, tahattomat inhimilliset virheet, tietovuodot tai varkaudet.

- Sopimus- ja vastuuriskit voidaan välttää tekemällä asianmukainen sopimuskumppanin kanssa. Pahimmassa tapauksessa yritykset eivät tee sopimuksia lainkaan.
- Tietoriskit, dokumentteja siirrellään ja käsitellään monimutkaisissa verkostoissa.
- Keskeytysriskit, pieni yritys kestää vain pieniä häiriöitä. Tulipalo on monilla aloilla merkittävä riski.
- Rikosriski, suurin osa yrityksiin kohdistuneista rikoksista on ennalta suunniteltuja. Poistetaan rikoksentekomahdollisuus ja lisätään kiinnijäämisriskejä. (VTT 2009, hakupäivä 8.3.2013.)

Standardiperheeseen kuuluva ISO/IEC 27005-standardi sisältää ohjeita tietoturvan riskien hallinnasta ja se on yhteensopiva työkalu ISO/IEC 27001-standardin mukaisen tietoturvallisuuden hallintajärjestelmän vaatimuksiin (kuva 3).



Kuva 3. Tietoturvariskien hallintaprosessi ISO/IEC 27005-standardi. (Suomen standardisoimisliitto SFS ry, hakupäivä 5.2.2013.)

Arviointiympäristön määrittämisen jälkeen voidaan siirtyä riskien tunnistukseen, riskien suuruuden arviointiin ja riskien vaikutusten arviointiin. Tämän vaiheen jälkeen on ensimmäinen päätöksentekokohta, jossa kysytään onko arviointi tyydyttävä. Jos vastaus on kielteinen, palataan takaisin arviointiympäristön määrittämiseen ja lähdetään samaa reittiä eteenpäin. Jos taas arviointi on tyydyttävä, päästään eteenpäin riskien arviointiin. Tästä seuraava vaihe on toinen riskeihin liittyvä päätöksentekokohta. Jos käsittely ei ole tyydyttävä, palataan takaisin arviointiympäristön määrittämiseen. Jos taas vastaus on myönteinen eli käsittely on tyydyttävä, päästään riskin hyväksyntään. Kaikista vaiheista voidaan siirtyä riskeistä viestittämiseen sekä riskien tarkkailuun ja katselmointiin. (Suomen standardisoimisliitto SFS ry, hakupäivä 15.3.2013.)

Jo pelkästään riskienhallintaan ja riskianalyysin tekoon saa apua erilaisilta kursseilta ja kouluttajilta, mutta tietoa löytyy myös Internetistä. Suomenkielistä materiaalia on olemassa, mutta jos yrityksen toisena virallisena kielenä on englanti tai englanninkieli käy muuten yrityksen koulutuskieleksi, niin lisää riskienkartoitustyövälineitä löytyy mm. HSE Guidance -sivuilta (HSE Guidance, hakupäivä 20.3.2013). Erilaisia oppaita ISO/IEC 27001-standardista ja riskienhallinnasta löytyy myös It Governance -sivuilta (IT Governance Ltd, hakupäivä 2.4.2014).

6 KÄYTÄNNÖN OHJEITA

Tietoturvan suurimpia vihollisia eivät ole hakkerit eivätkä vieraat valtiot, vaan käyttäjien oma kiire, osaamattomuus ja huolimattomuus (Järvinen 2012, 19). Tietoturva mielletään tekniseksi asiaksi, jota insinöörit hoitaa, mutta tämä on väärä käsitys. Puhutaan, että psykologian osuus on 80 prosenttia ja tekniikan vain 20 prosenttia. Tietoturvallisuus ja käyttömukavuus ovat keskenään ristiriidassa, sillä asioista voidaan tehdä joko tietoturvallisia tai helppokäyttöisiä, mutta ei molempia yhtä aikaa. (Järvinen 2012, 24.)

Jos yrityksellä ei ole vielä julkista tietoturvapolitiikkaa, niin tulisi pohtia miettiä, miten työntekijä voi ottaa ensimmäisen askelen tietoturvallisempaa työpistettä kohti. Ensisijaisesti työntekijän kannattaa lähteä liikkeelle työaseman tietoturvasta. Jos työaseman tietoturva on huolimattomissa käsissä, ei ole suurta väliä muistakaan tietoturva-asioista. Tästä voidaan lähteä liikkeelle:

- Tulee seurata tietoturvallisuuteen liittyviä tiedotteita ja tutustua ohjeisiin.
- Ei saa jättää vierasta yksin tai valvomatta työhuoneeseen tai muihin yrityksen tiloihin.
- Ei pidä antaa vieraan käyttää konetta, ellei ole varma hänen henkilöllisyydestään.
- Pitää noudattaa ”puhtaan pöydän” periaatetta, eikä jättää keskeneräistä työtä näytölle, eikä salaisia papereita pöydälle.
- Tietoja käsitellään aina huolellisesti.
- Salasanaa ei luovuteta toisten käyttöön.
- Käytetään pitkiä ja vaikeita salasanoja, joissa on isoja kirjaimia, pieniä kirjaimia, numeroita ja erikoismerkkejä. Vaihdetaan salasana riittävän usein.
- Kone lukitaan aina, kun poistutaan työpisteestä.
- Tuntemattomilta tulleisiin sähköposteihin pitää suhtautua varauksella. Tiedon alkuperä tulee selvittää ennen käyttöä ja vieraista lähteistä tulleiden liitetiedostojen avaamista pitää välttää.
- Työhön kuulumattomia ohjelmia ei pidä asentaa työkoneelle.
- Jos kone on yhteiskäytössä, pitää muistaa aina käytön jälkeen tyhjentää selaimen välimuisti, historia ja evästeet.

- Tulosteet tulee hakea tulostimelta heti tulostuksen jälkeen.
- Arkaluontoiset tulosteet laitetaan käytön jälkeen silppuriin.
- Työpäivän päättyessä kirjaudutaan ulos koneelta ja sammutetaan se.
- Kannettava tietokone tai puhelin ovat valvonnassa koko ajan
- Tietoturvallisuuteen liittyvistä ongelmista ilmoitetaan välittömästi tietoturvavastaavalle tai esimiehelle. (Lappia 2010, hakupäivä 12.3.2013.)

Vaikka olisi kuinka varovainen, myös ajattelemattomuudesta johtuvia virheitä sattuu. Tahattomia tietovuotoja tapahtuu lähes joka alalla. Sähköiset välineet helpottavat työtä, mutta napin painallukset takana voi ollakin salassa pidettävää. Tietojen luvaton käyttö on muuttunut helpommaksi kuin aikaisemmin, toisaalta käyttäjälokien avulla siitä jää myös nykyään helpommin kiinni kuin aiemmin. Vaara saattaa vaania myös siinä, kun käyttää omia välineitä työasioiden hoitamisessa. Työnantajan vanhaan kannettavaan verrattuna oma älypuhelin on helpompi ja nopeampi käyttää, mutta tietoturvaltaan se ei välttämättä ole yhtä varma. (Castrén 2011, 27.)

Facebookissa omien työasioiden kertominen voi tuoda ongelmia. Jos työntekijä kommentoi työnantajaansa julkisesti, tasapainoilee hän silloin sananvapautensa ja työlainsäädännön lojaalisuusvelvoitteen välillä. Omien asioiden julkituominen ajattelemattomasti voi johtaa jopa kunnianloukkaukseen. (Castrén 2011, 28.)

Perinteisesti yrityksillä on käytössä tietoturvapalvelin, joka hoitaa turvaohjelmien asennukset, päivitykset ja asetukset keskitetysti verkon kautta. Raportointi ja valvonta takaavat, että kokonaiskuva tietoturvasta on koko ajan saatavilla ja tietoturva toimii. Vaihtoehtona yrityksellä on hankkia pilviturvapalvelut, eikä silloin tarvita omaa tietoturvapalvelinta, vaan kaikki tiedot kulkevat Internetin kautta salattuna. (Hämäläinen 2012, 41.)

Virustorjunta on ollut turvana jo yli kymmenen vuoden ajan. Torjuntaohjelmia myydään uuden tietokoneen mukana, mutta perinteinen virustorjunta on tulossa tiensä päähän. Petteri Järvisen mukaan virustorjunta alkaa muistuttaa hernepyssyä. (Järvinen 2012, 16.)

Torjuntaohjelmat havaitsevat ainoastaan tunnettuja viruksia, eivätkä riittävän ovelasti tehdyt virukset paljastu. Viime aikoina myös torjuntaohjelmien ongelmat ovat lisääntyneet. Ne toimivat pääkäyttäjän oikeuksilla ja pienilläkin virheillä voi näin olla vakavat seuraukset. Pitkällä tähtäimellä ainoa turvallinen ratkaisu on siirtää tiedostoja ja sovelluksia pilvipalveluihin. Sekään tie ei ole ongelmaton, mutta riskit eivät pysy enää samoina vaan vaihtuvat uusiin. (Järvinen 2012, 16.)

7 LAINSÄÄDÄNTÖ

Yritysjohdon tulisi tietää, ovatko sen valitsemat tietoturvakäytännöt oikeat. Tietoturvallisuuden perusteet pitäisi olla tiedossa. Vaikka asiat perustuvat standardiin, joskus on hieman epäselvää mihin nämä asiat perustuvat ja pohditaan sitä, kuka oikein päättää sen miten toimitaan. Eivät tietoturvaedellytykset ole sattumanvaraisia. Laki on kaikille sana.

Suomessa ei ole olemassa yhtä erillistä tietoturvalakia, johon olisi keskitetty kaikki tietoturvavelvoitteet. Lainsäätäjä on nähnyt parempana vaihtoehtona sen, että tietoturvavelvoitteet ovat osana muun lain sisältöä. (Laaksonen ym. 2006, 27.)

Seuraavaan listaan on poimittu tietoturvallisuuteen liittyvää säädösperustaa:

1. Perustuslaki 10§ (Laaksonen ym. 2006, 28).
2. Laki viranomaisten toiminnan julkisuudesta, julkisuuslaki (621/1999) (Laaksonen ym. 2006, 29).
3. Henkilötietolaki (523/1999) (Laaksonen ym. 2006, 31).
4. Laki kansainvälisistä tietoturvavelvoitteista (588/2004) (Laaksonen ym. 2006, 47).
5. Laki yksityisyyden suojasta työelämässä (759/2004) (Laaksonen ym. 2006, 49).
6. Sähköisen viestinnän tietosuojalaki (516/2004) (Laaksonen ym. 2006, 54).
7. Laki tietoyhteiskunnan palvelujen tarjoamisesta (458/2002) (Laaksonen ym. 2006, 77).
8. Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003) (Laaksonen ym. 2006, 78).
9. Laki sähköisestä allekirjoituksesta (617/2009) (Laaksonen ym. 2006, 79).
10. Viestintämarkkinalaki (393/2003) (Laaksonen ym. 2006, 80).

Tietoturvallisuuteen liittyviin ja muihin lakeihin voi tarkemmin tutustua Finlexin sivustolla, http://www.finlex.fi. Tältä sivustolta löytyy aina ajantasainen lainsäädäntö sekä mm. tietosuojalautakunnan viimeisimmät päätökset. (Finlex 2013, hakupäivä 1.4.2013.)

8 POHDINTA

Tässä opinnäytetyössä on käyty läpi esimerkkiyrityksen tietoturvakartoitus, ISO/IEC 27001-standardin vaatimuksia ja yleisesti tietoturvaan liittyviä asioita. Tämä kyseinen standardi on hyvä valinta siksi, että se on jo kansainvälisesti ja kansallisesti tunnettu ja se sopii yhteen muiden samaan ISO/IEC 27000-standardiperheeseen kuuluvien osien kanssa.

Opinnäytetyön lähtökohtana oli tutkia, kuinka hyvin esimerkkiyrityksen henkilökunnalla ovat tietoturva-asiat mukana jokapäiväisessä työnteossa. Kyselyn pohjaksi valittiin ISO/IEC 27001-standardi ja asiaa tutkimalla löytyi valmis kyselypohja pk-yritysten riskienhallinnan työvälinesarjasta. Kyselyn vastausprosentti oli 82 ja kysymykset liittyivät suoraan opinnäytetyön kannalta merkityksellisiin kysymyksiin. Johdannossa esitettiin kysymyksiä tietoturvan merkityksestä, vaatimuksista ja tavoitteista sekä tietoturvapolitiikasta ja henkilökunnan tietoturvaosaamisesta. Näihin kysymyksiin olemme saaneet vastaukset neljännessä luvussa. Tietoturvatavoitteet ja politiikka on yrityksessä määritetty, mutta käytännössä näiden asioiden omaksumisessa on hieman puutteita. Toisaalta kaikki osaavat hakea apua ongelmiin, joten tulos on siltä osalta positiivinen. Kun kaikki esimiehet olivat sitä mieltä, että työntekijät käsittelevät työhönsä liittyviä luottamuksellisia tietoja tarkoituksenmukaisesti, ei tietoturvallisuusasioiden kanssa ole ollut ongelmia. Havaintojeni mukaan asiakkaisiin liittyvät tietoturva-asiat kuuluvat kiinteästi mukaan työohjeisiin, joten ilman erillisiä tietoturvaohjeitakin päivittäinen rutiini sujuu niin kuin pitää. Mutta myös odottamattomiin tilanteisiin pitäisi osata varautua.

Tästä lähtökohdasta on hyvä lähteä etsimään sopivaa koulutusmenetelmää. Työtilanteet ja -kiireet huomioon ottaen voidaan valita, käytetäänkö itsenäisiä tietokoneella olevia harjoituksia, tehdäänkö palaverien ohessa ryhmätöitä, laitetaanko aivoriihi rakentamaan ratkaisuja vai pidetäänkö tietoturvallisuusluentoja. Tietoturvakyselyn suuri vastausprosentti mielestäni kertoo siitä, että henkilökunta on kiinnostunut omasta työstään ja valmis osallistumaan tietoturva-asioiden kehittämiseen sekä ottamaan vastuuta oman työn tietoturvallisuudesta.

Kyselyn jälkeen seuraavana jatkotoimenpiteenä voisi olla riskianalyysi. Sen tekemiseen on monta tapaa ja omien resurssien ollessa riittämättömät, tähän työhön voi palkata

konsultin. Toisaalta paras tietämys löytyy oman yrityksen sisältä. Silloin kun aloitetaan riskein arviointi, on samassa yhteydessä hyvä päivittää tavallisia käytännön ohjeita. Kun on tiedossa mitkä riskit uhkaavat, niihin osataan varautua.

Tietoturvaan liittyvää yhtä ainoaa lakia ei ole olemassa. Sen vuoksi olen koonnut muutaman keskeisen lainkohdan mukaan tähän raporttiin. Lakeihin saattaa tulla muutoksia, siksi viimeisimmät tiedot kannattaa käydä etsimässä Finlexin sivuilta, joka on oikeusministeriön omistama oikeudellisen aineiston julkinen ja maksuton palvelu Internetissä.

Olen päässyt tekemään havaintoja esimerkkiyrityksen tehtäviin ja työtapoihin. Työn hektisyys ei anna useinkaan aikaa perehtyä omatoimisesti esimerkiksi verkkolevyillä oleviin yleisiin ohjeisiin ja jos kiireen keskelle tulee pienen tauon mahdollisuus, ei ensimmäisenä tule mieleen ohjeiden etsiminen. Tämän vuoksi jo työohjeisiin tulisi jouhevasti liittää jokaiseen työvaiheeseen liittyvät kaikki tietoturvaohjeet. Osa asiakkaisiin liittyvistä tietoturvaohjeista on jo ohjeissa mukana lainsäädännön perusteella. Pöydällä oleviin ohjeisiin voisi liittää vaikkapa taustapuolelle esimerkkitapauksia erilaisista tietoturva-asioista. Vanha viisaus ”kertaus on opintojen äiti” pitää paikkansa. Kun työn ohessa tulee muutaman sekunnin tauko, niin siinä papereita selaillessa voisi silmäillä vaikkapa kuukauden välein vaihtuvia erilaisia mielenkiintoisia tapauksia, joissa tietoturva on ollut uhattuna. Näin saisi tietoa, mitä näissä tilanteissa olisi pitänyt tehdä ennakkoon välttääkseen vahingon ja mitä sen jälkeen, kun vahinko on jo tapahtunut. Mitä lähempänä nämä esimerkit ovat omaa työtä, sitä paremmin ne jäävät mieleen.

Tämän tutkimustyön perusteella ei voida vielä lähteä esimerkkiyrityksessä hakemaan ISO/IEC 27001-standardin mukaista sertifiointia, sillä tähän tutkimukseen ei liittynyt sertifiointiin valmistautumiseen liittyviä toimenpiteitä. Kun esimerkkiyrityksessä saadaan tietoturvallisuuden termit ja perusasiat päivitettyä henkilökunnalle ja määriteltyä prosessien vastuuhenkilöt, voidaan lähteä miettimään sertifioinnin vaatimia resursseja. Silloin tulee ajankohtaiseksi harkita, riittääkö oma henkilökunta vai tarvitaanko konsulttia. Harkitaan samalla, kuinka monta henkilöä voidaan laittaa kursseille. Pohditaan, tarvitaanko lisää henkilökuntaa sertifioinnin vaatimiin tehtäviin. Jos sertifiointiin asti halutaan mennä, kannattaa asia ottaa puheeksi jo seuraavassa tietoturvakoulutuksessa. Näin päästään totuttautumaan ajatukseen sertifioinnista, tiedetään jo etukäteen mitä se tarkoittaa, eikä vastuu tule enää myöhemmin yllätyksenä asianosaisille.

Olen yrittänyt tehdä tästä opinnäytetyöstä selkeän ja käytännön ohjeita sisältävän raportin, joka on helppo lukea ja jossa ei ole lähdetty kertomaan liian pitkälle sertifiointiin johtavista asioista. Niiden asioiden vuoro mahdollisesti tulee myöhemmin jos yritysjohto katsoo, että henkilökunta on siihen valmis ja resurssit riittävät. Sertifiointiin liittyviin toimenpiteisiin ei kannata ryhtyä ennen kuin tarkkaan miettii siitä mahdollisesti saavutettavat hyödyt.

Tutkimustuloksista voi ottaa suuntaa siihen, mitä asioita kannattaa lähteä kertaamaan ensin. Liian monen asian yhtäaikainen kertaus saattaa johtaa siihen, että kiirehditään asiat läpi pintapuolisesti ja perustavaa laatua olevat asiat jäävät kunnolla läpikäymättä. Tärkeää on selvittää termit ja määritelmät, jotta kaikki tietävät, mistä puhutaan. Kun jokainen yrityksen henkilökunnasta tietää osaavansa tietoturvan perussäännöt, on niitä mahdollista soveltaa myös odottamattomiin tilanteisiin.

On olemassa muutamia valmiita opinnäytetöitä, jotka sivuavat tätä samaa aihetta. Tietoturvakartoituskyselyn vastaukset muodostivat pohjan tälle työlle ja se erottaa tämän työn muista. Vaikka kyselyn vastaukset saattaisivat olla samansuuntaisia muuallakin, ne ovat kuitenkin vain yhden yrityksen vastaukset. Raportti on tarkoituksella tehty niin yleisluonteisesti, että sitä voi käyttää hyödykseen muutkin yritykset. Sisällysluettelo on suunniteltu siten, että ensin kerrotaan yleisitä asioista, sitten käydään läpi kysely ja sen jälkeen jatkotoimenpiteet. Tämä järjestys lienee käytännöllinen joka organisaatiolle.

Havainnoinnista tuli tärkeä osa tätä opinnäytetyötä. Eri työpisteissä tapahtuneen havainnoinnin avulla ISO/IEC 27001-sertifiointi alkoi muuttua mielessäni mahdollisuudeksi, johon esimerkkiyritys voisi tarttua. Ilman havainnointia ja esimerkkiyritystä työ ei olisi ollut niin antoisaa. Kun tietää mitä oikeita työvaiheita on olemassa, pystyy näkemään, miten prosessit etenevät ja miten standardin luomat vaatimukset voitaisiin liittää niihin. Standardi ei jää enää pelkäksi teoriaksi vaan muuttuu ohjeiksi, joiden avulla vaatimusten mukaiseen suunnitteluun päästään konkreettisesti käsiksi.

Lyhyesti sanottuna tietoturvatyössä on hyvänä toimintatapana kolmevaiheinen malli, jossa laitetaan perusta kuntoon. Silloin on hyvä ottaa malliksi vaikkapa juuri ISO/IEC 27001-standardi, sillä tärkeintä on saada tietoturvatyöhön laaja kattavuus, jossa huoleh-

ditaan kaikista tietoturvan osa-alueista. Toisena vaiheena tietoturvassa vaikuttavat liikemaailman vaatimukset, jotka on erityisesti huomioitava silloin, jos IT-palveluita ulkoistetaan. Kolmantena vaiheena on jatkuva prosessi, johon päästään kahden ensimmäisen vaiheen kautta. Avainasemassa ovat riskihavainnot, sillä niiden pohjalta tehdään tarvittavia säätöjä. Säädöt perustuvat ihmisten, prosessien ja teknologian oikeaan suhteeseen. (Lagus, 2013 10.)

Tähän tutkimukseen on rajattu vain keskeiset asiat tietoturvakartoitukseen liittyvistä asioista. Jokaisen kohdan perusteellinen läpikäynti olisi vaatinut jopa kuukausia lisää aikaa. Tätä voi kuitenkin pitää muistilistana ja näiden perusasioiden jälkeen on helppo lähteä etsimään lisää tietoa. Kaiken tämän jälkeen jää vielä yksi asia: ”odota odottamatonta”.

LÄHTEET

Aaronscreations 2013. Hakupäivä 7.4.2013.
<http://www.chartitnow.com/PDCA_Plan_Do_Check_Act.html>

Castrén, Kirsi 2011. Työntekijä – tietoturvan heikoin lenkki? Tietosuoja 4/2011.

DNV Business Assurance Hakupäivä 5.4.2013
<http://www.dnvba.com/fi/Sertifointi/Hallinta-ja-johtamisjarjestelmat/Tietoturvallisuus/Pages/ISO-27001.aspx>

Finlex 2013, Hakupäivä 1.4.2013.
<http://www.finlex.fi/fi>

Heljaste, Juha-Matti & Korkiamäki, Jari & Laukkala, Heljo & Mustonen, Juha & Peltonen, Jere & Vesterinen, Panu 2008. Yrityksen turvallisuusopas. Helsinki: Gummerrus Kirjapaino Oy.

HSE Guidance. Risk management. Hakupäivä 10.3.2013.
<http://www.hse.gov.uk/risk/index.htm>

Hämäläinen, Pertti 2012. Täältä saat parhaan pilviturvan. Tietokone 8/2012.

Iivari, Mika & Laaksonen, Mika 2009. Liiketoiminnan jatkuvuussuunnittelu ja ICT-varautuminen. Helsinki: Tietosanoma Oy.

IT Governance Ltd. Hakupäivä 2.4.2014.
<.http://www.itgovernance.eu/c-46-information-security.asp>

Järvinen, Petteri 2012. Arjen tietoturva. Jyväskylä: Docendo.

Järvinen, Petteri 2012. Virustorjunta on hernepyssy. Tietokone 8/2012.

Kemi-Tornionjokilaakson koulutuskuntayhtymä, Lappia 2010. Tietoturva. Hakupäivä 12.3.2013.
<http://www.kkylappia.fi/Suomeksi/Paatoksenteko/Ohjeet_ja_ saannot/Tietoturva/Tyoaseman_tietoturva.iw3>

Laaksonen, Mika & Nevasalo, Terho & Tomula, Karri 2006. Yrityksen tietoturvakäsikirja. Helsinki: Edita Publishing Oy.

Lagus, Antti 2013. Varaudu uhkiin järjestelmällisesti. Tietosuoja 1/2013.

Mars. Hakupäivä 2.4.2013.
<http://www.portal.marsh.fi/fi/claimsdemo_fi.nsf/0/CD16EBBD17C96527C1257065002C5BCC/$FILE/jatkuvuussuunnittelu100903.pdf>

Oulun yliopisto 2007. Hakupäivä 1.4.2013
<http://www.oulu.fi/laatutyo/koulutukset/laatutyopaja_opiskelijoille/2_tyopaja/nayttelykavelymateriaalit.pdf>

Rautvuori 2011, 30Tietosuoja 3/2011 s.30.

Suomen standardisoimisliitto ry 2013. ISO 27000 standardiperhe. Hakupäivä 31.1.2013.
<http://www.sfs.fi/haku?137_o=1&searchterms=iso+2000&service=site>

Suomen standardisoimisliitto SFS 2012. ISO/IEC 27001:fi. Helsinki.

Tirronen, Helena 2003. Liiketoiminnan kehittäminen. Hakupäivä 3.4.2013.
<http://elearn.ncp.fi/materiaali/uimonenj/VirtAMK/tturva.html>

Valtionvarainministeriö 2009. Liite 3 Tietoturvallisuuden hallintajärjestelmä ja siihen kuuluvat tietoturvaohjeet. Hakupäivä 8.3.2013.
<https://www.vahtiohje.fi/web/guest/86>

Valtionvarainministeriö 2004. Pk-Yrityksen riskienhallinnan työvälinesarja. Hakupäivä 31.1.2013.
<http://www.pk-rh.com/pdf/henkiloston-tietoisuus-ja-toimintatavat-tietoriskien-hallinnassa.pdf>

VTT 2005. Riskianalyysi. Hakupäivä 3.4.2013.
<http://virtual.vtt.fi/virtual/riskianalyysit/indexe5b3.html>

LIITELUETTELO

Liite 1 1 (3)

Osa 1 kaikille: Henkilöstön tietoisuus tietoriskeistä

1. Onko henkilöstölle koulutettu nykyaikaisen liiketoiminnan ja tuotekehityksen luottamuksellisuuteen ja tietosuojaan liittyviä yleispiirteitä? (43 %)
2. Tunteeko henkilöstö yrityksen vastuut tietojen luottamuksellisuuden ja muun tietoturvallisuuden suhteen? (86 %)
3. Onko kaikille selvää, millaisten tietojen suojaaminen on tärkeää? (64 %)
4. Onko kaikille selvää, mitä yrityksen toiminnasta saa kertoa ulkopuolisille? (71 %)
5. Onko yritykselle määritelty tietoturvaperiaatteet ja laadittu niiden toteuttamiseksi ohjeet? (57 %)
6. Kattavatko ohjeet sähköisten tietojärjestelmien lisäksi suullisen viestinnän ja paperidokumenttien käsittelyn ja jakelun? (64 %)
7. Onko henkilöstö koulutettu tunnistamaan tietoriskejä ja noudattamaan yrityksen turvakäytäntöjä? (50 %)
8. Onko olemassa menettely tietoturva-asioiden käsittelyä varten? (29 %)
9. Onko jokainen työntekijä allekirjoittanut tietojen käyttösäännöt? (43 %)
10. Onko tietojen luokitteluohjeet ja käytännöt osa arkipäivän toimintaa? (29 %)
11. Tietääkö henkilöstö, minne ilmoittaa havaitsemistaan tietoturvarikkeistä tai käytännön puutteista? (64 %) (VTT 2004, hakupäivä 31.1.2013.)

Osa 2 esimiehille: Uudet työntekijät

1. Tarkistetaanko uusien työntekijöiden taustat ennen työsuhteen alkamista? (0 %)
2. Ovatko tietoturva-asiat mukana uusien työntekijöiden perehdyttämisessä? (100 %)
3. Selvitetäänkö myös uusille ja väliaikaisille työntekijöille yrityksen tietoturvapolitiikan ja vaitiolositoumuksen merkitys? (100 %)
4. Allekirjoittavatko työntekijät erillisen sitoumuksen tietojen ja järjestelmien käytöstä sekä tietojen palauttamisesta työsuhteen jälkeen? (67 %) (VTT 2004, hakupäivä 31.1.2013.)

Osa 3 esimiehille: Työsuhteen päättyminen

1. Onko suunniteltu toimenpiteet, joilla varmistetaan tietoturvallisuus työsuhteiden päättyessä? (67 %)
2. Onko henkilöstön irtisanoutumistilanteessa esimiehellä tieto kaikista henkilön käyttäjätunnuksista ja käyttöoikeuksista, joiden voimassaolo voidaan poistaa? (67 %)
3. Huolehditaanko, että kaikki työntekijän käytössä olleet työ-, tallennusvälineet sekä yritystä koskevat asiakirjat palautetaan yritykselle? (100 %)
4. Onko varauduttu työntekijöiden riitaisaan irtisanoutumiseen tai irtisanomiseen? (33 %)(V TT 2004, hakupäivä 31.1.2013.)

Osa 4 esimiehille: Henkilöstön toimintatavat

1. Käsittelevätkö työntekijät työhönsä liittyviä, luottamuksellisia tietoja tarkoituksenmukaisesti? (100 %)
2. Ovatko yrityksen keskeiset tiedot suojattu mm. rajaamalla niiden saatavuus ja määrittelemällä niiden käyttöoikeudet? (100 %)
3. Onko minimoitu mahdollisuus myydä tai luovuttaa yritykselle keskeisiä tietoja tai dokumentteja? (67 %)
4. Ovatko yrityksen sisäiset valvontajärjestelmät asianmukaiset (työnvalvonta, tilojen valvonta, tietojen käytön ja tietojärjestelmien valvonta)? (67 %)
5. Onko työntekijöiden omien töiden tekeminen työpaikalla hallittua (ajat, kulkuoikeudet, valvonta)? (67 %)
6. Onko luottamuksellisten tietojen säilyttämiseen riittävästi lukittuja tiloja? (67 %)
7. Hoidetaanko jätepaperin keräys ja käsittely hallitusti? (100 %)
8. Ovatko puhelinkäyttäytymisohjeet olemassa? (67 %)
9. Onko toiminta tulipalon varalta ohjeistettu ja harjoiteltu? (33 %)
10. Onko varahenkilöjärjestelyistä huolehdittu? (67 %) (VTT 2004, hakupäivä 31.12013.)

Osa 5 kaikille. Tietojärjestelmien ja tietokoneiden käyttö

1. Onko henkilöstöllä riittävä perusosaaminen järjestelmien käyttöön? (79 %)
2. Saavatko työntekijät häiriö- ja virhetilanteisiin apua ja neuvontaa? (100 %)

3. Käyttääkö jokainen työntekijä työssään vain omaa käyttäjätunnustaan? (93 %)
4. Onko varmistettu turvallisen salasanan muodostaminen? (71 %)
5. Onko estetty mahdollisuus muilta työntekijöiltä lukea tai muuttaa käyttäjän tietoja huomaamatta? (79 %)
6. Onko varmuuskopioiden ottamiseen ja palauttamiseen olemassa toimintaohjeet? (36 %)
7. Valvotaanko varmuuskopioiden ottamista? (29 %)
8. Onko Internetin käyttö ohjeistettu? (93 %)
9. Onko sähköpostin käyttö ohjeistettu? (71 %)
10. Onko virustentorjuntamenettelyt ohjeistettu työ- sekä kotikoneiden osalta? (50 %)
11. Ovatko virusohjelmien ja muiden vastaavien päivitykset automatisoitu? (86 %)
12. Salakirjoitetaanko kannettavilla laitteilla (tietokoneet, kämmentietokoneet yms.) olevat luottamukselliset tiedot? (0 %)
13. Onko käyttäjiä kielletty asentamasta yrityksen verkkoon tai työasemiin ulkopuolisia ohjelmistoja tai laitteita? (93 %) (VTT 2004, hakupäivä 31.1.2013.)